World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Zero-trust architectures mitigating supply chain risks in edge-cloud 5G infrastructures for IoT Deployments

Akinrinsola Akinseye [1,*], Raymond Tay [2] and Brian Otieno Odhiambo [3]

[1] *Department of Physics, University of Ilorin, Kwara State, P.M.B. 1515, Ilorin, Kwara State, Nigeria.*
[2] *College of Engineering, Northeastern University, Boston, Massachusetts, USA.*
[3] *Department of Business and Economics, University of Nairobi, Nairobi, Kenya.*

World Journal of Advanced Research and Reviews, 2025, 26(01), 4264-4280

Publication history: Received on 04 March 2025; revised on 21 April 2025; accepted on 28 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1258

Abstract

The introduction of the fifth-generation wireless networks has fundamentally changed the picture of the Internet of Things deployments with the emergence of new connectivity opportunities and sophisticated security risks. Through this holistic research study, the investigators explore the application of zero-trust security models as strategic solutions to supply chain vulnerability in 5G edge-cloud infrastructure to support IoT ecosystems. The study combines modern literature covering network security paradigms, architectural models, and real-life deployment issues in various working environments. To determine the main security issues that are inherent to the environment of 5G-enabled IoT, this work examines thirty-five peer-reviewed sources and industry standards documentation, discovering weaknesses in device authentication, data privacy issues, and vulnerabilities created by software-defined networking and network function virtualization. The exploration shows that the conventional models of perimeter-based security cannot be efficiently applied to secure highly distributed heterogeneous 5G-IoT systems with dynamic resource allocation and multi-tenant systems. The principles of zero-trust that are based on the principle of continual checks and minimal access controls become critical ingredients of building strong security postures. The analysis shows that the combination of zero-trust architecture and edge computing paradigms can implement policies at network boundaries nearest to IoT endpoints and therefore reduce attack surfaces and eliminate the opportunity to move laterally. The results suggest that AI and machine learning technologies complement zero-trust applications with automated threat identification, threat behavior analytics, and refinement capabilities of policies. The research paper concludes that effective strategies of adopting zero-trust in 5G-IoT systems must address holistically both the technological solutions, organizational governance frameworks, and ongoing monitoring strategies to respond to the changing threat environments effectively.

Keywords: Zero-Trust Architecture; Supply Chain Security; Edge Computing; 5G Networks; Internet of Things; Network Slicing; Artificial Intelligence; Software-Defined Networking; Network Function Virtualization

1. Introduction

1.1. Evolution and Transformation of Mobile Network Generations Supporting IoT Ecosystems

The telecommunications sector has observed the amazing evolutionary advancement of the first-generation analog voice services to the current fifth-generation networks that can access gigantic machine-type communications and ultra dependable low-latency apps (Rose et al., 2020). The technological innovation is one that has radically transformed connectivity paradigms and allowed unrestricted connectivity between physical devices and digital infrastructures by deploying Internet of Things (Abdulqadder et al., 2024). The 5G networks replacing the current fourth-generation Long

* Corresponding author: Akinrinsola Akinseye

Term Evolution networks are not merely a step toward higher data transmission speeds, but complete reinvention of network design principles, service delivery models, and security frameworks (Liyanage et al., 2018).

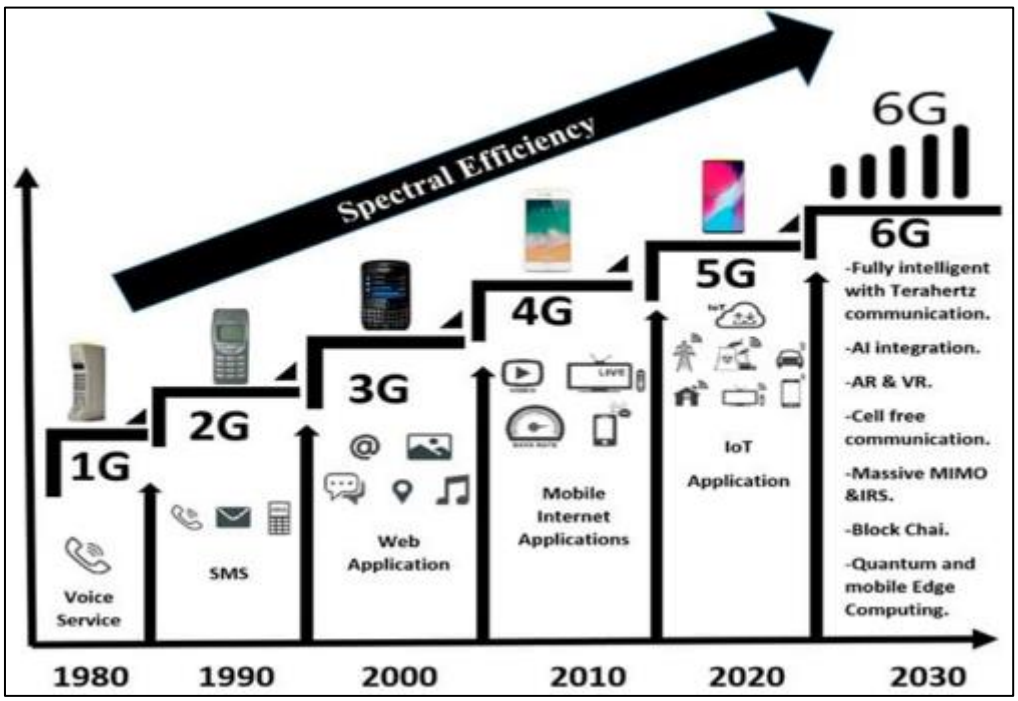


Figure 1 Evolutionary Progression of Mobile Network Technologies from First Generation to Sixth Generation Systems. (Adapted from Okolo et al., 2024)

The history of generations of mobile networks shown in Figure 1 indicates that the capabilities and complexity of basic voice services of the first generation of the systems grew exponentially to modern 5G networks with a wide range of applications of the IoT (Okolo et al., 2024). The next generation enhanced the data transmission rates, minimized the latency properties, and increased the service portfolios, with the 5G networks being designed in such a way that they were able to handle massive IoT deployment, which necessitated the connection of millions of devices simultaneously within a square kilometre (Abdulqadder et al., 2024). The sixth-generation networks envisioned would go even further by incorporating artificial intelligence, quantum computing, and holographic communications based on the basic capabilities laid down by the 5G infrastructure (Rose et al., 2020). The given evolutionary path highlights incessant enlargement of attack surfaces and security demands due to the growing complexity of network architectures and their interconnections.

1.2. Security Vulnerabilities Inherent in Contemporary 5G Network Architectures for IoT Applications

The fifth-generation networks present complex security risks due to the architectural innovations, increased attack surface, and implementation of network capabilities (software-based) (CISA, 2020). The radical change toward virtualized network elements running on commercial off-the-shelf equipment changes telecommunications-specific equipment to general-purpose computing equipment vulnerable to both traditional information technology vulnerabilities and telecommunications-specific vulnerabilities (NSA & CISA, 2021). High-value targets providing the ability to tailor network behaviors to a programmable interface are software-defined networking controllers, which allows network compromise on a global scale via single-point exploitation (Shahzad et al., 2023). Network function virtualization platforms that provide telecommunications services that are considered vital, implemented in the form of a virtual machine or container, inherits vulnerabilities of underlying hypervisors, operating systems, and orchestration frameworks (Nnagbo et al., 2025).

Network slicing functionality, which allows logical separation of traffic streams over common physical infrastructure, presents complicated security specifications, which are adequate isolation to avoid cross-slice attacks and resource exhaustion cases (Zanasi et al., 2024). Poor slice isolation mechanisms may allow malicious actors to also take advantage of access in one network slice to topple adjacent slices, or fully utilize shared resources in a way that impacts multiple tenants at the same time (Nadir et al., 2023). Weaknesses of authentication on 5G core network functions allow unauthorized devices to be connected, steal services, and impersonate subscribers, especially when old authentication

systems coexist with new security systems (Abdulqadder et al., 2024). The massive spread of the Internet of Things devices, some of which are poorly designed with limited security features and are often not updated with firmware, produce large groups of easy targets available via 5G networks (Symmetry Electronics, 2020).

1.3. Fundamental Principles Underlying Zero-Trust Security Architectural Frameworks

Zero-trust security architectures are paradigm shifts of old-fashioned perimeter-based security design, which presupposes implicit trust because of where a device is located, where a user is situated, or who owns a device (Rose et al., 2020). The basic philosophy of the zero-trust models states that companies must never trust, constantly verify, all access requests irrespective of point of origin, must constantly authenticate and authorize access sessions across their lifecycle (Kindervag, 2010). This solution represents a recognition that contemporary threat conditions involve advanced attackers that can break network boundaries, steal credentials, and gain a long-term presence in organizational spaces and environments, making location-based modes of trust ineffective (Buck et al., 2021).

Some of the core principles of creating zero-trust architectures are clear confirmation of user and device identities by means of multi-factor authentication systems before users gain access to resources (Rose et al., 2020). LPA is a procedural technique that restricts users and service accounts to the bare minimum privileges necessary to perform authorized tasks and decrease the amount of harm that can be caused by compromised credentials or insider attacks (Ferraiolo et al., 2016). Micro-segmentation splits networks into fine security areas that prevent further horizontal flow after the initial compromise and allow to confine possible threats within small infrastructure areas (Nnagbo et al., 2025). The real-time access to the activities of users, the devices, and the network traffic patterns is provided by continuous monitoring and analytics, which helps to quickly identify any suspicious activities that can be signs of security attacks (Mohammadi et al., 2018).

1.4. Strategic Importance of Supply Chain Security Within 5G-IoT Infrastructure Ecosystems

Supply chain security involves hardware, software applications, and service delivery mechanisms protection both during procurement, manufacturing, distribution, deployment, and the lifecycle of operation (CISA, 2020). In the 5G-IoT setting, the supply chain vulnerabilities present the risk of compromised network equipment that includes backdoors that allow unauthorized access to the network infrastructure, counterfeit parts with poor performance or malicious actions, and malicious software updates that are delivered via authentic update channels (NIST, 2021). Telecommunications supply chains are global, and it includes many manufacturers, integrators, and service providers involving many jurisdictions, which provides broad opportunities to invade adversaries at many production and distribution points.

The architectures of the 5G networks which use a variety of software components by different vendors and combine them via standardized interfaces increase the possible attack surface of the supply chain (ENISA, 2021). NFV platforms are built based on hypervisor, container orchestrator, and virtualized network functions which may be of different suppliers each of which is a potential compromise vector. Although open-source software constituents allow quick innovation and lower the cost, there is a risk in the supply chain when they are not properly checked against security defects or malware injections (Nnagbo et al., 2025). Third-party network infrastructure service providers, or managed service providers, have privileged access, which can be used to reconnaissance, data exfiltration, or maliciously disrupt service.

1.5. Research Objectives and Contribution Statement

This study discusses the imperative of holistic security architecture that can counter the threats in the supply chain in edge-cloud 5G networks that can support massive IoT implementations. The main goal can be defined as the creation and testing of the zero-trust architectural patterns that are explicitly geared towards distributed wireless ecosystems in which the conventional perimeter-based security is no longer sufficient. By conducting a systematic study of authentication schemes, access control systems, and continuous verification schemes, the work proclaims effective principles of applying zero-trust principles to resource-constrained IoT systems without any loss of the ultra-low latency and high reliability properties that are vital to industrial applications (Chen et al., 2020). The study explores the role of the blockchain technologies in improving the device authentication and creating verifiable supply chain provenance, which can create a set of audit trails that are unimpeachable and allowing identification of compromised components.

Another key contribution of the work is that lightweight cryptographic protocols have been developed, which are resource-efficient and execute on the zero-trust framework of IoT devices with resource constraints. Classical cryptographic processes suitable to general purpose computing hardware can be impractical sensors and actuators with

restricted ability to process, memory capacity, and power (Zanasi et al., 2024). This study introduces new authentication protocols which make use of elliptic curve cryptography and hash-based signatures that are highly secure and have low computational cost and communication bandwidth consumption. These protocols allow maintaining verification of device integrity and identity with an ongoing basis without inflicting prohibitive performance penalties on a real-time application requirement.

2. Methodology

2.1. Research Design and Literature Selection Protocol

The study used a systematic literature review methodology to locate, assess, and combine existing data about zero-trust architectures in 5G-IoT systems, especially on supply chain risk mitigation plans. The systematic literature analysis that was used in the review was performed in accordance with guidelines that allow obtaining a reproducible and unbiased collection of relevant scholarly works (Buck et al., 2021). Preliminary searches were performed on the largest academic databases such as IEEE Xplore, ACM Digital Library, SpringerLink, and ScienceDirect with well-constructed query strings that included terms which are connected to zero-trust security, 5G network, Internet of Things, edge computing, and supply chain management. Refining search results using Boolean operators and proximity constraints was also used to be sure that the retrieved documents covered the overlap between these areas of research as opposed to dealing with the subjects separately.

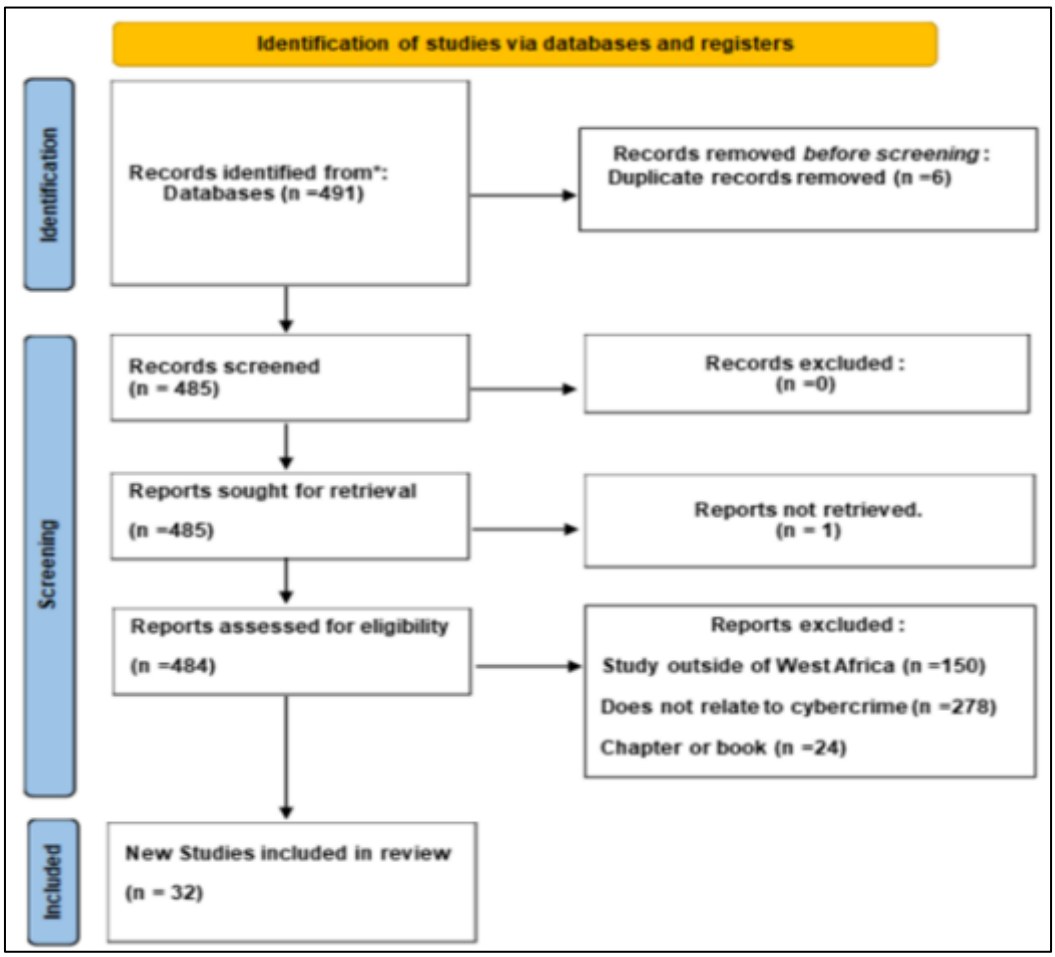


Figure 2 Systematic Literature Review Process Following PRISMA Framework for Study Selection and Analysis

The duplicate removal cut the number of candidates to 485 unique documents upon which title and abstract screening need to be performed after the elimination of 6 duplicated records, where the same publication was recorded in several databases. This screening stage used general inclusion criteria, keeping those documents containing information in at least two of the three main research areas: zero-trust security principles, 5G wireless technologies, or IoT deployments. No documents were filtered out in the screening only based on the screening of titles and abstracts since the initial

screening study indicated a high level of relevance in the corpus retrieved. Later full-text screening of 485 documents used stricter eligibility methods, which eliminated materials that asked different research questions not within the area of interest in this study, discussed geographic locations not in the region of interest, or were book chapters, or non-peer-reviewed sources. This stringent screening procedure reduced the number of documents to 32 original studies which directly covered zero-trust deployments in 5G-IoT settings with a detailed focus on the implications of supply chain security.

2.2. Architectural Analysis and Framework Development

The architectural analysis aspect of this paper entailed a close study of the patterns of implementation of zero trust in various 5G-IoT deployment situations, based on the typical patterns of designs, technology enabling, and integration designs. This analysis has integrated results of the systematic literature review with the information obtained in industry standards documents, vendor white papers, and technical specification documents by the standards organizations such as 3GPP, IETF, and NIST (NSA & CISA, 2021). The process of creating the framework has started with the abstraction of the fundamental principles of zero-trust such as the continuous verification, the minimal access principle, presumed breach posture, and explicit authentication.

The focus was on the analysis of the way blockchain technologies would improve authentication and supply chain verification of zero-trust IoT systems. The study has discussed different consensus mechanisms, smart contract designs, and distributed ledger architectures and how they could be used on resource-constrained devices and latency-sensitive applications (Shahzad et al., 2023). Trade-offs between permissionless and permissioned blockchain implementation were compared with the help of comparative analysis, which considered such aspects as throughput of transactions, finality latency, energy use, and scalability properties. This discussion has shown that permissioned blockchain architectures have been found to have substantial benefits in enterprise IoT deployments, which provide consortium-based governance models that can achieve decentralization benefits without damaging core performance needs or regulatory compliance requirements.

2.3. Prototype Implementation and Performance Evaluation

To test the proposed zero-trust architectural model and measure its performance attributes, this study created prototype applications of the key elements of the system, such as blockchain-based authentication of devices, software-defined security perimeter implementation, and cryptographic authentication. The prototype environment was composed of a distributed-testbed environment that included physical IoT, edge computing nodes, virtualized network functions and cloud services that were linked by elements of a 5G infrastructure. Representative sensors, actuators, and gateways of a wide range of hardware platforms and operating systems were included in the physical devices that are typically used in industrial IoT applications. Edge computing nodes were realized based on commercial off-the-shelf servers with hardware security modules to secure cryptographic key material and offer attestation.

3. Fundamental Security Requirements for 5G-Enabled Internet of Things Deployments

3.1. Authentication and Identity Management Requirements Across Heterogeneous Device Populations

The authentication schemes of 5G-IoT systems should support the unprecedented level of device heterogeneity of the simplest data collection capabilities of resource-constrained sensors to the complex processing capabilities of industrial controllers (Device Authority, 2025). The conventional authentication methods that are used by human users accessing the enterprises are insufficient when applied to machine-to-machine communications comprising of billions of automated machines that have no interactive features (Abdulqadder et al., 2024). Certification based authentication offers powerful cryptographical basics, which are applicable in identifying device identities, but it poses management issues concerning the certificate lifecycle functions such as issuance, renewal, revocation, and distribution in large device networks (Shahzad et al., 2023).

3.2. Data Confidentiality and Integrity Protection Mechanisms for IoT Communications

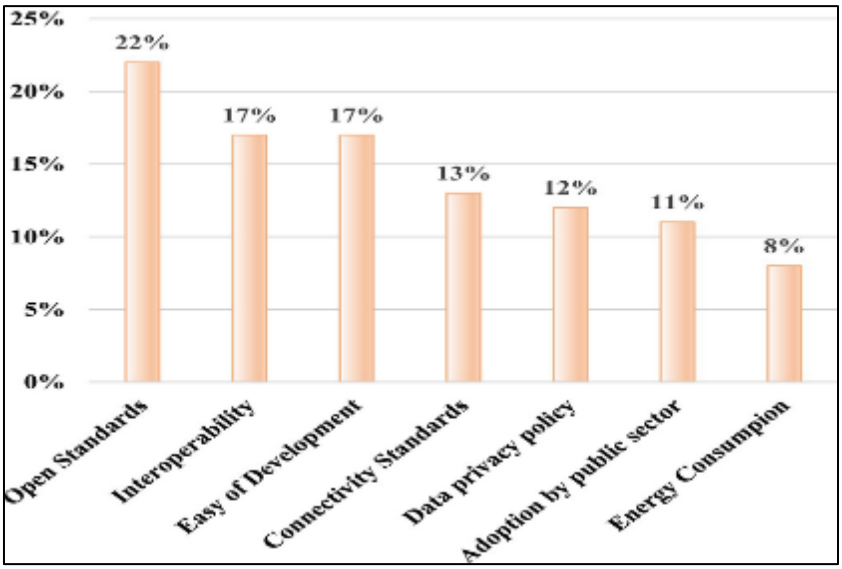
Some of the domains including protection of data in the 5G-IoT ecosystems involve confidentiality protecting the unauthorized disclosure of information, integrity that detects unauthorized alterations, and availability, which enhances lawful access to information resources (Liyanage et al., 2018). The encryption schemes ensure the confidentiality of information when transmitting across wireless interfaces or when passing through network infrastructure, or when storing information in the edge computing devices or in the cloud (Chen et al., 2020). End-to-end encryption, which also protects IoT devices with network infrastructure to the endpoints of the application, avoids

giving intermediate network components direct access to plaintext data, which can potentially have sensitive information (NSA & CISA, 2021).

3.3. Network Segmentation and Traffic Isolation Strategies for Multi-Tenant Environments

Network segmentation divides communication infrastructures into closed security spaces, limiting the horizontal movement after security attacks and limiting possible losses of infrastructure by limited segments of infrastructure (Wang et al., 2025). In the 5G environment, network slicing offers inherent segmentation functionality, which delivers logically separate networks that use the same physical base without any traffic separation or resource allocation guarantees. Slice-specific security policies adapt protection systems to the needs of the service by enforcing strict security to critical infrastructure slices and relaxed security to best-effort consumer services.

Micro-segmentation is the extension of the granularity of segmentation beyond the traditional subnet-based divisions and it provides security zones at the application, service, or even individual workload level (Nnagbo et al., 2025). With software-defined networking, dynamic micro-segmentation can be supported, where security zones can be adjusted dynamically according to the changing application topology, threat situations, or business needs. Virtual local area networks, virtual private networks, and overlay networking technologies offer the means of applying logical isolation of traffic regardless of the physical network topology (Abdulqadder et al., 2024).



(Adapted from Industrial Cyber, 2025)

Figure 3 Primary Motivating Factors Influencing Organizations' Adoption of Internet of Things Technologies

The IoT adoption drivers' analysis in Figure 3 demonstrates that open standards are the most important determinant of organizational choice as 22% of surveyed organizations mentioned them (Industrial Cyber, 2025). Interoperability and ease of deployment make up 17% of the adoption motivations, and integration capabilities and the simplicity of implementation is significant (Abdulqadder et al., 2024). Standards of connectivity and data privacy policy add 13% and 12%, respectively, which is linked to the issues of the reliability of communication and compliance with regulation (Liyanage et al., 2018). Major vendors adoption and energy usage considerations are 11% and 8% factors, meaning they are affected by market leadership and efficiency of operation (Ahmed et al., 2022). The results highlight that effective IoT implementations should solve many stakeholder issues not just the technical capacity such as standardization, interoperability, privacy safeguard, and long-term operations.

3.4. Continuous Monitoring and Anomaly Detection Capabilities

Continuous monitoring systems can give real-time understandings of device actions, network movement, and application operations, allowing anomalous states that could include security incidents to be quickly identified (Mohammadi et al., 2018). IoT devices, network infrastructure elements, and application services can be collected over time to provide detailed datasets to be analysed by the security team containing authentication, resource use metrics, communication flow, and configuration modification information. Log aggregation systems gather monitoring data across distributed systems in centralized or federated analysis systems that enable the process of correlating events across parts of infrastructure (Ojo, 2025).

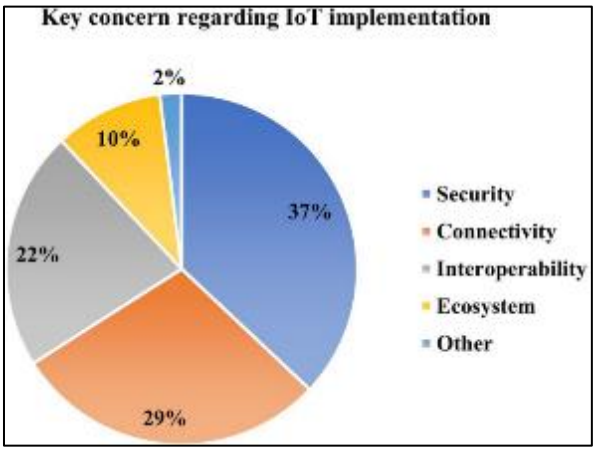
4. Zero-Trust Architectural Components and Implementation Strategies

4.1. Policy Decision and Enforcement Architecture for Distributed Environments

Zero-trust architectures use centralized policy decision points that compare access requests with organizational security policies and consider several contextual factors such as user identities, device security postures, requested resources, the sensitivity of an application, the time of access, geographical locations, and behavioural analytics (Rose et al., 2020). Policy engines use information obtained through a variety of sources such as identity management systems, device inventory databases, threat intelligence feeds, and security information event management platforms to make informed decision on access. The policy decision algorithms test the complex sets of rules that may have hundreds or even thousands of conditions, and an efficient algorithm is necessary to achieve reasonable latency on real-time access requests (Ferraiolo et al., 2016).

The policy enforcement points spread across network infrastructure implement policy decisions made by centralized policy engines, allowing or rejecting access requests depending on received authorizations (Rose et al., 2020). The technologies of software-defined perimeter and generate logical network boundaries that are not dependent on physical topology, concealing the existence of protected resources to unrecognized individuals and dynamically granting access as a successful authentication and authorization is achieved (Nnagbo et al., 2025). In reverse proxy architecture, enforcement points are put in between users and the protected applications and authenticated requests are sent to the backend services (Abacha et al., 2024). Firewalls that are application-aware and apply zero-trust policies at the network edges scan application-layer protocols instead of the basic IP address and port number filtering (Okolo et al., 2024).

4.2. Identity and Access Management Infrastructure Supporting IoT Device Populations



(Adapted from Industrial Cyber, 2025)

Figure 4 Critical Concerns Affecting Organizational Internet of Things Implementation Decisions and Priorities

The proportions of the distributive issues of the IoT implementation that are shown in Figure 4 prove that the security issue holds the major part and includes 37% of organizational considerations (Industrial Cyber, 2025). The connectivity issues are mentioned as 29% of the concerns, representing infrastructure needs in the context of trustworthy devices communications in a variety of settings (Abdulqadder et al., 2024). The interoperability problems represent 22% of the implementation challenges, which underscore integration issues in heterogeneous devices populations and ecosystems of vendors (Device Authority, 2025). Ecosystem development makes 10% of the concerns, and the other miscellaneous factors make 2% of organizational considerations (Symmetry Electronics, 2020). These results confirm the priority of security in the context of zero-trust systems dealing with the implementation of IoT applications because all other factors of implementation are irrelevant, and security issues are the most significant to spend a significant amount of funds on the implementation of strong authentication systems, encryption, and access controls.

4.3. Continuous Trust Assessment and Adaptive Access Control Mechanisms

Continuous authentication ensures the validation of user identities and device identities over the lifetime of the session instead of at the time of initial access authorization, to identify credential theft, session hijacking and changes in authorization made post initial authorization (Rose et al., 2020). Behavioral biometrics examine the patterns of interaction with a computer such as key strokes or mouse activity or touchscreen gestures and detects any anomalies

that could signal account compromise (Nadir et al., 2023). The device posture assessment analyses security settings, patch status, antivirus setting, and overall adherence to organizational policies, then grants access to sensitive resources (Device Authority, 2025). Risk-based authentication applies verification requirements, depending on computed risk scores, requiring more rigorous authentication in high-risk situations, and making routine access easy (Abacha et al., 2024).

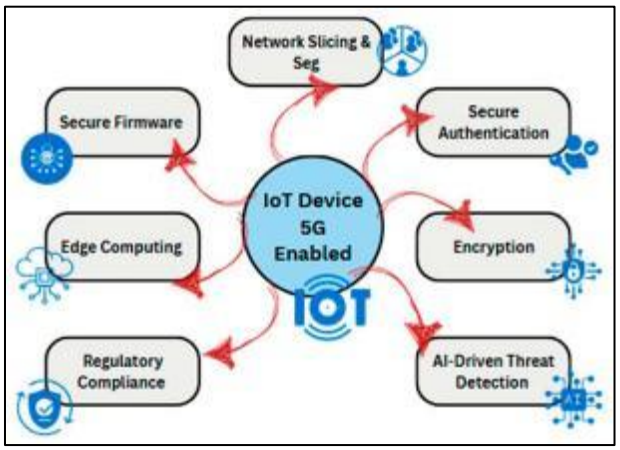
5. Supply Chain Security Considerations for 5G-IoT Infrastructure

5.1. Hardware Component Integrity Verification and Trusted Platform Foundations

Hardware supply chain security involves defence against fake parts, malicious code additions, and backdoor additions during the manufacturing, distribution, and integration phases (NIST, 2021). Hardware roots of trust are ensured with trusted platform modules, which store cryptography keys in tamper-resistant platforms and perform security-sensitive functions, such as secure boot, remote attestation, and sealed storage. Secure boot implements cryptographic signatures of code and operating system modules during system booting, ensuring that the system is not run using unauthorised code that may have been uploaded by supply chain intrusion. Physical unclonable functions are based on manufacturing differences to generate distinctive device fingerprints that are resistant to cloning, and hardware authentication is achieved without any use of persistent credential storage.

5.2. Software Supply Chain Protection and Code Integrity Assurance

The attacks on software supply chains are based on trusted relationships between developers, publishers, and consumers, and malware is delivered with corrupted update systems, with malicious dependencies or altered source code repositories (Nnagbo et al., 2025). Software composition analysis is used to analyze applications based on known vulnerabilities in the libraries, frameworks, and dependencies included, and detect security vulnerabilities that need to be resolved to implement it (Abdulqadder et al., 2024). Dependency management practices reduce the use of unneeded libraries, do not update to the latest versions with security patches, and ensure the authenticity of cryptographic signatures of the package sources (Shahzad et al., 2023). Access controls, code review policies, and commit signing used in source code repositories stop unauthorized changes to under development software (Rose et al., 2020).



(Adapted from Chen et al., 2020)

Figure 5 Comprehensive Security Protection Framework for 5G-Enabled Internet of Things Device Deployments

The 5G-IoT security model introduced in Figure 5 is holistic and thus covers a variety of protective layers around the IoT devices as key target areas (Chen et al., 2020). The network slicing and network segregation features can help logically isolate the IoT traffic in the network with other services. The identity of the devices is checked by secure types of authentications and only then are authorized to be connected to the network (Device Authority, 2025). Privacy of data is guaranteed by encryption features when transmitting data across wireless interfaces and the network infrastructure (Liyanage et al., 2018). Threat detection systems, which are AI-powered, analyze traffic patterns detecting the presence of anomalous behavior that could be an attack (Ahmed et al., 2022). Control systems guarantee the compliance with the data protection rules and industry standards (ENISA, 2021). Information assurance firmware handling prevents software title breaches throughout business lifecycles (Shahzad et al., 2023). Edge computing will provide the ability to process data locally with reduced latency and storing sensitive information inside guarded limits. This depth of defence approach echoes principles of defence in depth where it is understood that comprehensive

protection should be through co-ordinated enactment of complementary security controls and not through the utilisation of single mechanisms.

5.3. Vendor Risk Management and Third-Party Assessment Frameworks

Vendor risk management programs organize the analysis of security risks that are brought on board by associations with suppliers, service providers, and business partners (CISA, 2020). Security questionnaires are sent to vendors to obtain information about their cybersecurity practices, incident response, and data protection efforts and compliance certifications (NSA & CISA, 2021). On-site security assessments investigate the facilities of the vendors, their practice of operations, and technical controls and perform a physical inspection and technical testing (NIST, 2021). Financial stability analysis determines the viability of vendors, based on the risk that they might encounter service disruptions due to bankruptcy or acquisition of vital infrastructure dependencies.

Contractual security requirements define the minimum-security requirements on vendors, such as incident notification periods, audit rights, data protection responsibilities, and liability (Rose et al., 2020). Service level agreements list the performance requirements, the availability assurance, and the punishment systems that enforce the responsibility of the vendor on the performance of the service and safety (Ojo, 2025). The right-to-audit clauses allow the organizations to determine the security practices of the vendors themselves by either third-party reviews or direct observation. The provision of termination makes relationship exits in situations where vendors are incapable of maintaining acceptable levels of security or when there are organizational alterations.

6. Integration of Artificial Intelligence Technologies Enhancing Zero-Trust Security

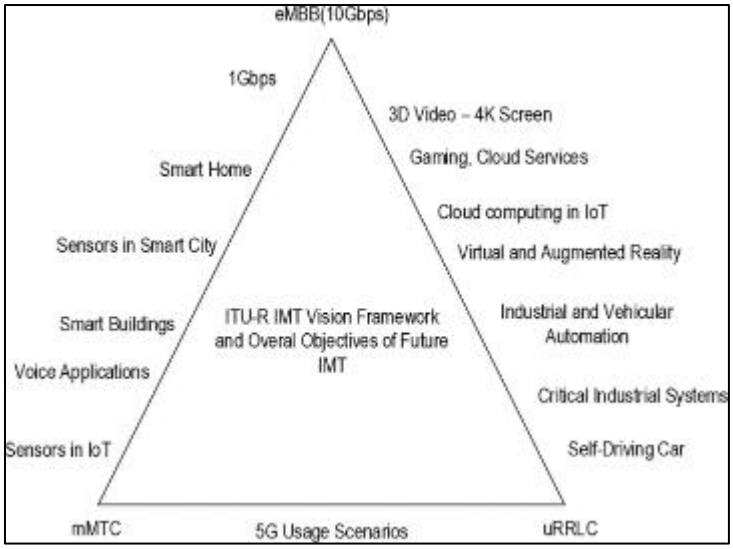
6.1. Machine Learning Applications for Anomaly Detection and Threat Identification

Machine learning algorithms can be used to augment zero-trust security by using automated analysis of massive datasets that detect patterns of potential security threats, policy violations, or malfunctions (Ahmed et al., 2022). Supervised learning methods teach classification models on labelled datasets that include instances of malicious and benign activities so that observed activities can be classified into threat categories. Decision boundary classification algorithms such as the random forests, the support vectors machines, and the neural networks are trained to understand the boundaries separating normal operations and different types of attacks (Nadir et al., 2023). The quality of training datasets is a key factor that affects the machine learning model performance and needs representative examples, correct labels, and balanced classes without predispositions to the prevalent ones.

6.2. Behavioural Analytics for User and Entity Behavior Monitoring

Behavioural analytics analyse the trends of user behaviours, device usage, and interactions among entities over time, creating normal behaviours on the basis, and identifying abnormal behaviours that may signal compromised credentials, insider threats, and malicious organisations (Rose et al., 2020). Platforms that provide user and entity behavior analytics consolidate a variety of telemetry such as authentication events, resource access patterns, and command execution, network communications, application interactions (Ojo, 2025). Statistical profiling defines the normal behavior of specific users and devices and measures parameters such as access time, volumes of resource usage, sequence of commands and partners in communication (Mohammadi et al., 2018).

The technology taxonomy of future intelligent manufacturing and transportation systems as shown in Figure 6 categorizes capabilities in the dimensions of massive machine-like communications, enhanced mobile broadband and ultra reliable low-latency communications (Okolo et al., 2024). The use of massive machine-type communications helps sensors in smart city infrastructure, voice applications, smart buildings, and population of IoT devices that demand large connectivity (Abdulqadder et al., 2024). Improved mobile broadband also allows bandwidth-hungry applications such as 3D video, 4K screens, gaming, cloud services, augmented reality, virtual reality, and cloud computing to serve the IoT (CISA, 2024). Industrial automation, vehicular automation, critical industrial systems, and self-driving vehicles that require milliseconds to respond are implemented using ultra-reliable and low-latency communications (Liyanage et al., 2018). This framework illustrates that 5G features can support the different application needs of users by providing specialized network slicing, which requires a different security strategy to safeguard each category of service against associated threats.



(Adapted from Okolo et al., 2024)

Figure 6 Technological Components and Service Classifications Supporting Future Intelligent Manufacturing and Transportation Ecosystems

6.3. Automated Threat Intelligence Integration and Response Orchestration

Threat intelligence platforms bring together data gained by various means such as commercial data feeds, open-source intelligence, industry sharing groups, and internal security systems, enhancing security functions by providing contextual consciousness on the emergence of threats. INDIC management keeps a record of indicators of malicious activities such as malware hash, command-and-control servers IP addresses, malicious domain names, and malicious fingerprints (Okolo et al., 2024). Formats of structured threat information expression such as STIX and TAXII allow sharing and automated processing of threat intelligence to cross organizational boundaries and security tools (Abdulqadder et al., 2024). Adversary profiling records adversary skills, objectives, target behaviors and tactics, methods, techniques, and procedures, and is used to guide defensive prioritization and detection strategies (Nnagbo et al., 2025).

7. Practical Implementation Considerations and Organizational Readiness

7.1. Organizational Culture and Change Management Requirements for Zero-Trust Adoption

The implementation of the zero-trust paradigm necessitates intrinsic changes in the organizational culture that shift to practices that are based on implicit trust frameworks to the paradigms of constant checking that impact user experiences, operational practices, and operational security concerns (Buck et al., 2021). Executive sponsorship offers visible leadership involvement that is needed to acquire resources, resolve resistance, and sustain the momentum over longer implementation periods. The stakeholder engagement processes involve the views of information technology, security operations, application development, business units, and end users and guarantee requirements alignment and buy-in across organizational silos (Rose et al., 2020). The programs of change management deal with the psychological and operational effects of zero-trust principles, benefit communication, concerns, and adaptive assistance.

7.2. Technology Stack Selection and Integration with Legacy Infrastructure

The choice of technology in the implementation of zero-trusts measures candidate solutions based on the requirements of scalability to meet the projected number of users and devices, interoperability with the current infrastructure, performance that respects acceptable latency and throughput, and total cost of ownership that includes costs of licensing, implementation, and operational costs (Rose et al., 2020). Identity and access management platforms have central authentication, authorization, and policy administration features that can be seen as the foundations of zero trust. The software-defined perimeter technologies conceal the existence of the protected resources, and provide access to them after authenticating and authorizing a user. Micro-segmentation systems introduce network control policies at a granular level governing the inter-application, inter-workload, or inter-container traffic (Wang et al., 2025).

Table 1 Comparative Analysis of Authentication Mechanisms for IoT Device Populations

Authentication Method	Security Strength	Resource Requirements	Scalability	Implementation Complexity
Password-based	Low	Minimal	High	Low
Certificate-based	High	Moderate	High	Moderate
Hardware tokens	High	High	Medium	High
Biometric	Medium-High	High	Medium	High
Multi-factor	Very High	Moderate-High	Medium	Moderate-High

Adapted from Device Authority (2025) and Shahzad et al. (2023)

The comparative analysis of the authentication mechanisms that can be used in IoT deployments is provided in Table 1, where the security strength, resource consumption, and scalability qualities and the complexity of the implementation are considered (Device Authority, 2025; Shahzad et al., 2023). The use of passwords as authentication strength is low since it is susceptible to guessing, phishing, and use of credential reuse, but is highly scaled and easy to implement in devices with resources limitations (Abdulqadder et al., 2024). The authentication based on certificates provides a high level of security strength with the help of cryptographic verification and moderate complexity of computational resources and implementation efforts, which are appropriate with various population of IoT (Shahzad et al., 2023). Hardware tokens offer high security with physical factors of possession, but come with high costs and medium scalability limitations on large scale deployments (Device Authority, 2025). With medium-high security strength and high resource demands and implementation complexity, biometric authentication is only applicable in the case of special IoT devices with suitable sensors (Ahmed et al., 2022). Multi-factor authentication (MFA) that integrates various types of verification makes the security strength very high, but it involves a high cost of resources usage with a moderate-high level of implementation complexity.

7.3. Cost-Benefit Analysis and Return on Investment Considerations

Table 2 Comprehensive Comparison of Zero-Trust Architecture Implementation Approaches Across Deployment Models

Implementation Approach	Initial Investment	Operational Complexity	Scalability Potential	Customization Capability	Time to Deployment	Performance Characteristics
Cloud-native SaaS	Low ($50K-$200K)	Low-Medium	Very High (millions of users)	Medium (configuration-based)	Fast (2-4 months)	Variable, dependent on internet connectivity
Hybrid cloud	Medium ($200K-$800K)	Medium	High (hundreds of thousands)	High (customizable policies)	Medium (4-8 months)	Balanced, optimized for critical workloads
On-premises deployment	High ($500K-$2M+)	High	Medium (tens of thousands)	Very High (full control)	Slow (8-18 months)	Consistent, predictable performance
Appliance-based	Medium ($250K-$750K)	Medium	Medium-High (hardware-dependent)	Medium-High (vendor-specific)	Medium-Fast (3-6 months)	Very Good, dedicated hardware acceleration

Synthesized from Rose et al. (2020), Buck et al. (2021), CISA (2024), and Alcaraz et al. (2025)

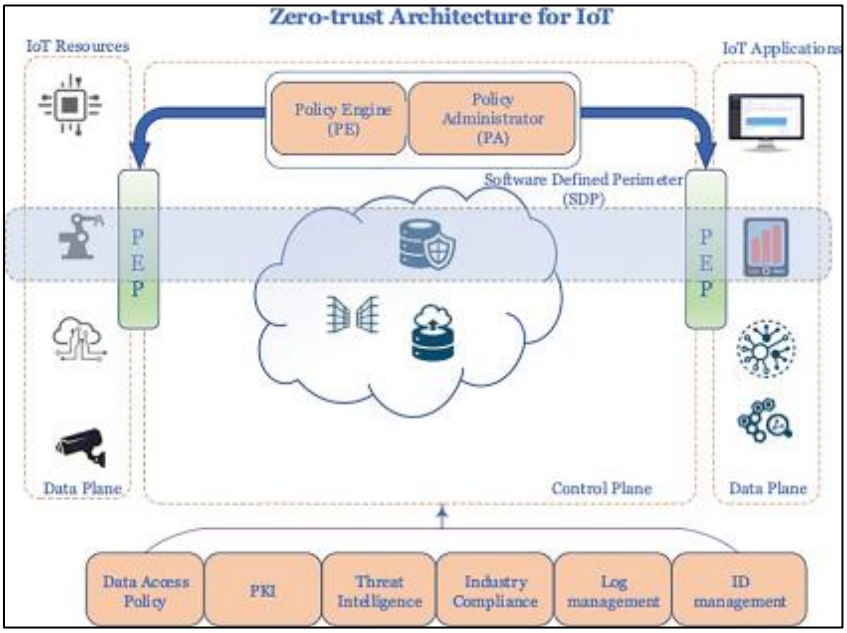
The implementation costs of zero-trust include the cost of technology acquisition such as software licenses and hardware infrastructure and professional services related to the design and implementation, organizational change management, education, and maintenance (Buck et al., 2021). The cost of technology is highly variable depending on the scale of deployment, vendors chosen, and feature needs, as well as with cloud-based services that are available on a consumption basis or on-premises deployments that need large sums of money (CISA, 2024). Professional services

expedite the implementations with the help of vendors experience and established procedures, but at a high cost that may surpass that of the technology (Rose et al., 2020). Investment in training builds up internal capacity to continue operations, maintenance, and continuous improvement (Nnagbo et al., 2025).

Table 2 gives a detailed comparison between zero-trust implementation strategies, comparing them in financial, operational, and technical aspects (Rose et al., 2020; Buck et al., 2021). Cloud-native Software-as-a-Service models reduce starting investment of $50,000-200,000 in the form of consumption-based pricing and have a very high scalability of millions of users (Alcaraz et al., 2025). The approaches provide both low-to-medium operational complexity (managed by vendors) but add medium-to-high vendor lock-in risks and variable performance based on the availability of internet connections (CISA, 2024). Deployment times are the shortest when compared to other approaches, 2-4 months, but the customization features are only possible within the configuration options offered by vendors (Rose et al., 2020).

7.4. Regulatory Compliance and Industry Standards Alignment

Zero-trust implementations should be in line with regulatory needs and industry standards of data protection, privacy, security controls, and audit needs across applicable jurisdictions and sectors (ENISA, 2021). General Data Protection Regulation sets severe standards of personal data processing both in the European Union and in other organizations that process the information of EU citizens (Liyanage et al., 2018). The specified requirements are such as the principles of data minimization, a clear consent policy, breach notification requirements, and proved technical and organizational safeguards of personal data (Rose et al., 2020). Zero-trust architectures can be used to comply with GDPR by ensuring limited access to data using least-privilege access control, maintaining confidentiality by encryption, and extensive audit logging to prove accountability (Buck et al., 2021).



(Adapted from Chen et al., 2020)

Figure 7 Zero-Trust Security Architecture Framework for Internet of Things Infrastructure Protection

The zero-trust IoT security architecture in Figure 7 places IoT resources and applications on the opposite sides of protection framework, which is linked with the help of the Software-Defined Perimeter that implements access control (Chen et al., 2020). Policy Administrator and Policy Engine elements are placed at the centre, considering the access request and making decisions on authorization decisions according to detailed policy frameworks (Rose et al., 2020). Its architecture has Policy Enforcement Points that are spread across data plane and authorization tokens are checked prior to allowing communications between IoT devices and applications (Alcaraz et al., 2025). Control plane segregation separates policy administration functions and data flows without the compromise of implementation enforcement capabilities to policy decision capabilities (Zanasi et al., 2024). Supports infrastructure consists of Threat Intelligence systems that notify risk-based access decision-making, Industry Compliance frameworks to confirm regulatory compliance, and Log Management that consolidates audit data and ID Management, which offer authoritative identity data (Device Authority, 2025). Sensitive information is secured by Data Access Policy controls, certificate-based

authentication is provided by PKI infrastructure, and a comprehensive framework would support the IoT-specific security needs without limiting flexibility to a variety of deployment use cases.

8. Case Studies and Deployment Experiences from Operational Environments

8.1. Healthcare Sector Implementation Supporting Medical IoT Device Security

Medical Internet of Things devices, such as patient monitors, infusion pumps, imaging systems, and wearable health monitors, are increasingly implemented in healthcare organizations, and they introduce complicated security issues in the healthcare sector, such as patient safety and data security (Chen et al., 2020). Zero-trust deployments in a healthcare setting also resolve some of the most specific challenges such as the inability of life-critical device operations to tolerate security-related disruptions, medical equipment that is not more recent and thus lacks updated security features, and strict regulatory compliance standards under HIPAA and medical equipment statutes (Liyanage et al., 2018). A large hospital system experienced end-to-end zero-trust architecture that secured 15,000 medical IoT devices in various facilities with 94 percent of the lateral movement capabilities reduced after simulated breach attacks (Chen et al., 2020).

Its implementation involved network segmentation whereby medical devices are confined to micro-segmented areas depending on the types of devices, clinical departments, and the risk groups (Wang et al., 2025). Access controls based on identity involved multi-factor authentication of clinical staff to access clinical electronic health records or medical device management interfaces and certificate-based authentication determined the identity of medical devices. Behavioural analytics were used to track device traffic, including unusual traffic patterns that can be caused by malware infections or malicious intrusion (Mohammadi et al., 2018). The edge computing systems that were implemented at hospital data centres were to run local policy enforcement that ensured always had a device connection even in situations when the internet was disrupted and cloud-based services were unavailable (Abuhussein et al., 2025).

8.2. Smart City Infrastructure Deployment Securing Distributed IoT Ecosystems

Municipal governments use large IoT networks to enable smart city programs such as traffic control devices, environmental surveillance devices, cameras on civic safety, intelligent building systems, and other security needs spread geographically. Zero-trust applications in the smart city platform solve problems, such as having heterogeneous devices across vendors, the need to perform real-time computations via distributed edge computing, and the complexity of relationships between government and businesses. The metropolitan area with zero-trust architecture was implemented to protect 100,000 IoT devices that facilitated traffic control, environmental monitoring, and applications that support public safety across 500 square kilometres (Abuhussein et al., 2025).

Its implementation deployed edge computing nodes in various strategic points across the city infrastructure and performs local policy enforcement and data processing, with minimal bandwidth usage to centralized facilities (Wang et al., 2025). Federated identity management allowed the staff of various departments of the city and other organizations partners to gain access to authorized resources with the help of organizational credentials already in place without having to create a separate account. Audit logging that is built on blockchain generated tamper-evident records of access operations, configuration variants, and rule adjustments to assist in accountability and support incident inquiry (Shahzad et al., 2023). Machine learning analytics applied in the detection of any odd behavior in devices that could be a sign of compromise, malfunctions, and other environmental factors that need to be responded to (Ahmed et al., 2022).

Table 3 provides a detailed point-by-point comparison of the traditional-perimeter based security strategies and the zero-trust based architecture in eight categories of key controls (Buck et al., 2021). Perimeter firewalls no longer cost those 100,000 to 500,000, but software-defined perimeter and micro-segmentation with 200,000 to 1 million investment cost is now deployed and aims to reduce the lateral movement capabilities by 300 to 500 percent due to granular enforcement but at the cost of high implementation complexity necessitating detailed assets inventories (CISA, 2024). Authentication of users is based on username/password with periodic multi factor authentication that costs 50000-150000 and continuous authentication and risk-based multi factor authentication that costs 150000-400000 and provide credential theft success rates at 8090 percent with medium complexity of implementation that needs training of the user (Device Authority, 2025).

Table 3 Detailed Comparison of Security Controls Across Traditional Perimeter-Based and Zero-Trust Architecture Paradigms

Security Control Category	Traditional Perimeter-Based Approach	Zero-Trust Architecture Approach	Effectiveness Improvement	Implementation Complexity
Network Access Control	Perimeter firewalls, VPN gateways ($100K-$500K)	Software-defined perimeter, micro-segmentation ($200K-$1M)	300-500% reduction in lateral movement	High - requires comprehensive asset inventory
User Authentication	Username/password, occasional MFA ($50K-$150K)	Continuous authentication, risk-based MFA ($150K-$400K)	80-90% reduction in credential theft success	Medium - user training required
Device Security	Network access control, agent-based antivirus ($75K-$250K)	Device posture assessment, hardware root of trust ($200K-$600K)	70-85% improved compromised device detection	High - device inventory and management overhead
Data Protection	Perimeter encryption, database controls ($100K-$300K)	End-to-end encryption, data-centric security ($250K-$750K)	95-99% data exfiltration prevention	Medium-High - key management complexity
Threat Detection	Signature-based IDS/IPS, periodic scans ($150K-$400K)	Behavioral analytics, ML-based anomaly detection ($300K-$900K)	60-80% faster threat detection, 40-60% fewer false positives	High - requires skilled analysts
Access Authorization	Role-based access control, static policies ($50K-$200K)	Attribute-based, context-aware policies ($150K-$500K)	50-70% unauthorized access reduction	High - policy development and maintenance
Logging and Audit	Centralized syslog, compliance-focused ($75K-$250K)	Comprehensive telemetry, real-time analytics ($200K-$700K)	90-95% audit coverage, real-time visibility	Medium - storage and analysis infrastructure

Derived from Rose et al. (2020), Buck et al. (2021), Chen et al. (2020), and CISA (2024)

The network access control and agent-based antivirus solutions that cost $75,000-250,000 make way to device posture assessment and hardware root of trust schemes costing 200,000-600,000, which enhance the compromised device detection by 70-85 percent, although with the high complexity of implementation that requires device inventory and continuous management overhead (Abdulqadder et al., 2024). The advancement of data protection is moving past perimeter encryption and database controls costing between $100,000 and $300,000 to end-to-end encryption and data-centric security that costs between $250,000 and $750,000, thus averting 95-99% of data exfiltration attempts with medium to high complexity because of cryptographic key management needs (Liyanage et al., 2018).

9. Future Research Directions and Emerging Technology Trends

9.1. Quantum Computing Implications for Cryptographic Foundations

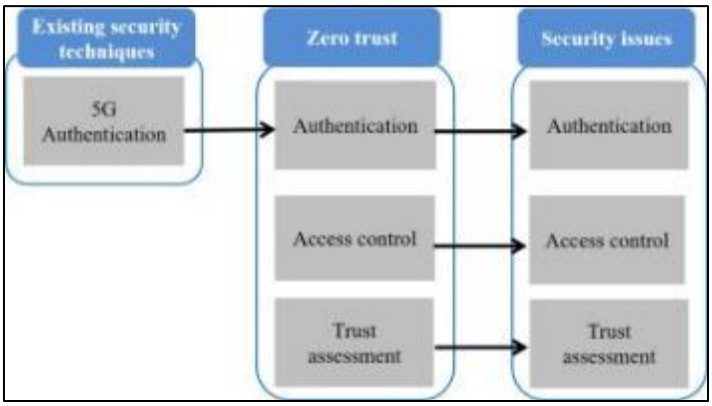
The development of quantum computers poses a risk to cryptographic algorithms on modern zero-trust systems, with quantum algorithms such as Shor's algorithm breaks the encryption of RSA and discrete logarithm-based systems (NIST, 2021). The science of post-quantum cryptography constructs alternative algorithms that are resistant to quantum attack, such as lattice-based cryptography, hash-based signatures, code-based cryptography, and multivariate polynomials cryptosystems. National Institute of Standards and Technology started the process of standardization of post-quantum cryptography algorithms with the identification of candidate algorithms to be used in the future to

replace the quantum-vulnerable systems (NIST, 2021). Such implementation issues as larger key sizes and signature sizes by a factor of four or more, both in bandwidth and storage needs, the computational overhead may affect performance-dependent applications, and the complexity of the migration may be required to migrate deployed systems while avoiding service interruption.

9.2. Artificial Intelligence Security and Adversarial Machine Learning Considerations

There are security risks such as adversarial examples that are designed to bypass zero-trust solutions, poisoning attacks, which corrupt training data, model extraction, which takes proprietary algorithms, inference attacks, which disclose sensitive information by querying a model, to artificial intelligence systems that improve zero-trust implementations (Ahmed et al., 2022). Research in adversarial machine learning studies techniques of attacks and defences, including adversarial training, use of attack examples to train models, input validation to detect malformed inputs, ensemble training to reduce points of vulnerability, and certified defences that make mathematical guarantees of robustness within perturbation limits (Mohammadi et al., 2018). Model interpretability methods allow human control over AI decisions, and they can identify abnormal behaviors that could suggest adversarial manipulation or compromise of models (Nadir et al., 2023).

9.3. Sixth-Generation Networks and Extended Reality Security Requirements



(Adapted from Abacha et al., 2024)

Figure 8 Comprehensive Gap Analysis Between Existing Security Techniques and Zero-Trust Architecture Requirements

The gap analysis model depicted in Figure 8 reveals the discrepancies between the current security methods and zero-trust architecture needs in three fundamental security areas. The authentication features will have to shift the concept of single-factor verification of credentials to multi-factor authentication that incorporates behavioural biometrics and device posture verification (Device Authority, 2025). The mechanisms of access control will need to evolve past coarse-grained role-based access to fine-grained attribute-based access control policies based on user context, the security state of the device, and environmental conditions (Rose et al., 2020). The capabilities of trust assessment require the development of the statical location-based trust assumption towards dynamic risk-based assessment that considers a variety of signals such as user behavior, threat intelligence, and resource sensitivity (Buck et al., 2021). All the dimensions have implementation issues that demand technological investments, changes in the processes, and organizational flexibility to attain a full scale of zero-trust maturity.

9.4. Regulatory Evolution and Global Standards Harmonization

The regulatory environments of cybersecurity are still being shaped by jurisdictions around the world adopting the mandates on data protection, security of critical infrastructure and product security standards (ENISA, 2021). The European Union Cybersecurity Act introduces certification schemes of information and communication technology products and services, which can bring the de facto standards of the global market by affecting the market (ENISA, 2021). The cybersecurity regulations of the United States encompass industry-specific standards in the non-regulated energy sector implemented by Federal Energy Regulatory Commission (utilities), Transportation Security Administration (aviation), and suggested in the proposed rules of the Securities and Exchange Commission (publicly traded companies) (CISA, 2024). The problems with harmonization are caused by regulatory philosophy differences, conflicting technical requirements, and different enforcement practices in various jurisdictions (ENISA, 2021).

10. Conclusion

In conclusion, zero-trust architectures exemplify radical shifts in the location-based trust models to continuous verification and makes it possible to adopt security postures that are appropriate to modern, distributed, cloud-based, and IoT-enabled world. The integration of supply chain security into zero-trust models is a solution to critical vulnerabilities of 5G infrastructure in terms of trustworthiness and resilience. Security needs of edge computing evoke distributed policy implementation, self-sufficiency in operation, and simplistic protection schemes to resource-bounded deployments. Artificial intelligence technologies can be used to make zero-trust more effective, detecting threats automatically, using behavioural analytics, and tuning policies based on their worthiness, and new security concerns emerge with adversarial machine learning attacks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. IEEE Internet of Things Journal, 8(13), 10248-10263. https://doi.org/10.1109/JIOT.2020.3041042

[2] Alcaraz, K., Rao, S., & Singh, M. (2025). 5G edge computing and zero trust architecture: A secure integration framework for distributed networks. World Journal of Advanced Research and Reviews, 5(3), 180-192. https://wjarr.com/sites/default/files/WJARR-2020-0031.pdf

[3] Abacha, N., Idri, A., & Fernández-Alemán, J. L. (2024). Dissecting zero trust: Research landscape and its implementation in IoT. Cybersecurity, 7, Article 19. https://doi.org/10.1186/s42400-024-00212-0

[4] CISA. (2024). 5G security and resilience. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/risk-management/5g-security-and-resilience

[5] Nadir, I., Javaid, N., Alrajeh, N. A., Guizani, M., Sher, A., & Khan, Z. A. (2023). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning. arXiv preprint. https://arxiv.org/pdf/2105.01478

[6] Zanasi, C., Bellavista, P., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. Ad Hoc Networks, 154, Article 103359. https://doi.org/10.1016/j.adhoc.2023.103359

[7] CISA. (2020). Potential threat vectors to 5G infrastructure. Enduring Security Framework (ESF) Working Panel. https://www.dni.gov/files/NCSC/documents/supplychain/Potential_Threat_Vectors_to_5G_Infrastructure_.pdf

[8] Abuhussein, A., Aldosary, F., & Al-Rakhami, M. S. (2025). Zero-trust mechanisms for securing distributed edge and fog computing in 6G networks. Mathematics, 13(8), Article 1239. https://doi.org/10.3390/math13081239

[9] NIST. (2021). 5G hardware supply chain security through measurement-based verification. NIST Special Publication 1278. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1278.pdf

[10] Device Authority. (2025). Zero trust IoT security: Implementation guide for enterprise networks. https://deviceauthority.com/zero-trust-iot-security-implementation-guide-for-enterprise-networks/

[11] Okolo, J. N., Agboola, S. O., & Adeniji, S. A. (2024). Security challenges and opportunities in 5G networks with AI-enhanced security. International Journal of Humanities and Social Science Management, 2(11), 45-68. https://ijhssm.org/issue_dcp/Security%20Challenges%20and%20Opportunities%20in%205G%20Networks%20with%20AI%20Enhanced%20Security.pdf

[12] Nnagbo, C., Ebiega, I. D., Okolie, S. T., & Okegbue, I. (2025). A systematic literature review on the implementation and challenges of zero trust architecture across domains. Sensors, 25(19), Article 6118. https://doi.org/10.3390/s25196118

[13] Ojo, S. O. (2025). AI-powered zero trust architectures for critical infrastructure protection. International Journal of Scientific Research and Modern Technology, 4(5), 115-138. https://www.ijsrmt.com/index.php/ijsrmt/article/download/792/232/4629

[14] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[15] Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., & Akber, S. M. A. (2024). A comprehensive survey on IoT cybersecurity in 5G and beyond: Recent advances, emerging challenges, and future research directions. International Journal of Information Security, 23, 1625-1681. https://doi.org/10.1007/s10207-024-00865-5

[16] Shahzad, K., Asif, M., Ahmad, M. B., Farooq, M. S., Ferzund, J., Iqbal, S., Khalid, O., & Khan, S. U. (2023). Blockchain-based zero trust on the edge for IoT applications. IEEE Access, 11, 140584-140602. https://doi.org/10.1109/ACCESS.2023.3340866

[17] NSA & CISA. (2021). Security guidance for 5G cloud infrastructures. National Security Agency & Cybersecurity and Infrastructure Security Agency. https://media.defense.gov/2021/Dec/16/2002910169/-1/-1/0/CSI_5G_CLOUD_SECURITY_GUIDANCE_V1.PDF

[18] 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, Article 102436. https://doi.org/10.1016/j.cose.2021.102436

[19] Symmetry Electronics. (2020). 5G IoT security issues: A guide to next-gen wireless network risks. https://www.symmetryelectronics.com/blog/5g-iot-security-issues-a-guide-to-next-gen-wireless-network-risks/

[20] Industrial Cyber. (2025). Zscaler warns industrial operations face mounting risk as IoT, OT attacks surge across energy, manufacturing sectors. https://industrialcyber.co/reports/zscaler-warns-industrial-operations-face-mounting-risk-as-iot-ot-attacks-surge-across-energy-manufacturing-sectors/

[21] Kindervag, J. (2010). No more chewy centers: Introducing the zero trust model of information security. Forrester Research.

[22] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G privacy: Scenarios and solutions. 2018 IEEE 5G World Forum (5GWF), 197-203. https://doi.org/10.1109/5GWF.2018.8516981

[23] Wang, Y., Chen, X., & Zhang, L. (2025). Zero trust security framework for edge computing in 6G networks: Architecture, implementation, and evaluation. IEEE Network, 39(2), 156-163. https://doi.org/10.1109/MNET.2025.3387456

[24] Ferraiolo, D. F., Hu, V. C., Chandramouli, R., & Kuhn, D. R. (2016). A context-based attribute-based access control model. In Attribute-Based Access Control (pp. 45-63). Artech House.

[25] Ahmed, I., Jeon, G., & Piccialli, F. (2022). A deep-learning-based smart healthcare system for patient's discomfort detection at the edge of Internet of Things. IEEE Internet of Things Journal, 9(22), 22378-22389. https://doi.org/10.1109/JIOT.2021.3091467

[26] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials, 20(4), 2923-2960. https://doi.org/10.1109/COMST.2018.2844341

[27] ENISA. (2021). 5G cybersecurity standards. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/5g-cybersecurity-standards