International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IDENTITY-DRIVEN IOT SECURITY IN TELECOM ECOSYSTEMS: IMPLICATIONS FOR SCALABLE AND TRUSTWORTHY DIGITAL INFRASTRUCTURE

Shiva Kumara[1*]

[1*]Independent Researcher, reachkumaras@gmail.com

Abstract
The rapid expansion of Internet of Things (IoT) deployments over telecommunications networks is reshaping digital infrastructure across smart cities, industrial automation, healthcare, and intelligent transportation. While 4G/5G evolution and the transition toward 6G enable massive machine-type communications, ultra-reliable low-latency services, and distributed cloud–edge integration, they also intensify security and trust risks. Conventional perimeter-based and network-centric security approaches are increasingly ineffective in telecom IoT ecosystems due to extreme scale, device heterogeneity, mobility, virtualization, multi-tenancy, and cross-domain service composition. This paper advances an identity-driven security perspective that anchors trust in explicit, verifiable identities for devices, services, and network functions rather than network location or implicit boundaries. Using a conceptual and analytical approach without reliance on empirical datasets, the study synthesizes prior work on IoT security, Zero Trust principles, cloud identity management, and telecom identity protections, and then develops an identity-centric security architecture for telecom IoT. The paper formalizes key threat assumptions emphasizing impersonation, unauthorized access, and cross-domain trust exploitation, and derives security and privacy requirements including mutual authentication, least-privilege authorization, continuous verification, accountability, and regulatory alignment. It further compares centralized and decentralized identity models, outlines trust establishment and federation workflows across operators and cloud/edge providers, and analyzes scalability constraints such as automated onboarding, credential lifecycle management, and the effects of network slicing and virtualization. Application-driven discussion across smart cities, Industry 4.0, healthcare, and transportation demonstrates the practical implications of identity-centric security for trustworthy operations. Finally, the paper identifies unresolved challenges—including interoperability, legacy device inclusion, constrained-device overhead, and governance—and highlights future research directions for 6G-era autonomous networks and standardized identity frameworks.

Keywords: - Identity-driven security, Telecom IoT ecosystems, Zero Trust architecture, Identity federation, Scalable trust management

1. Introduction

The Internet of Things (IoT) has become a core element of today's digital environments and telecommunications networks are a key part of the ability to connect on a large scale. The evolution of mobile communication technologies from 4G to 5G, and the research for 6G, have greatly increased the ability of telecom infrastructures to embrace massive machine-type communications, ultra-reliable low-latency services and data-intensive applications [1]. As a result, IoT devices continue to be deployed in a wide range of domains including smart cities, industrial automation, healthcare monitoring, and intelligent transportation systems [2]. These deployments depend on telecom networks to not only provide connectivity but also for services orchestration, mobility management and quality of service guarantees [3]. Despite all these

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

developments, the exponential increase in IoT in the telecom ecosystems has brought in significant security and trust challenges. IoT environment is defined by extreme scale, heterogeneity, and dynamism of billions of devices with various capabilities, ownership models, and lifecycles [4]. Many of these devices are unattended, resource-constrained and used in physically exposed environments, which makes these devices attractive targets for adversaries. Moreover, telecom-enabled IoT systems very often span across multiple administrative domains, including network operators, cloud providers, device manufacturers and enterprise services owners, making the establishment of consistent and enforceable security policies across the end-to-end system a challenging task [5]. Traditional security approaches based on telecom and IT infrastructures have largely been based on the perimeter-based and network-centric models.

Table 1. Comparison of Network-Centric and Identity-Driven Security Approaches in Telecom IoT

Security Dimension	**Perimeter / Network-Centric Security**	**Identity-Driven Security**
Trust Assumption	Implicit trust within network boundaries	Explicit trust based on verified identities
Authentication Basis	Network location or static credentials	Cryptographically verifiable identities
Authorization Granularity	Coarse-grained, role or zone based	Fine-grained, policy- and attribute-based
Scalability	Limited scalability at massive IoT scale	Designed for billions of devices
Suitability for IoT Heterogeneity	Poor support for diverse device types	Supports heterogeneous devices and services
Cross-Domain Trust	Difficult to enforce across domains	Supports federation and multi-domain trust
Resilience to Impersonation	Vulnerable once perimeter is breached	Strong resistance through mutual authentication
Cloud and Edge Compatibility	Limited and fragmented	Natively supports cloud–edge integration
Security Enforcement Model	Static and location-based	Dynamic and context-aware

Table 1 summarizes the basic differences between conventional network-centric approaches to security and identity-based models of security in the context of telecom-enabled IoT ecosystems. These models assume we can implicitly trust entities that work within a defined network boundary and untrust entities that work outside the boundary. Although such assumptions were reasonable in relatively static and well-defined enterprise networks, they are not becoming effective in large-scale IoT deployments [6]. The breaking down of well-defined network perimeters with the advent of virtualization, integration of cloud, and edge computing at the periphery breaks the effectiveness of location-based trust. Furthermore, network centric controls are ill-suited to combat threats like device impersonation, identity spoofing and unauthorized service access, which are common in IoT environments.

In response to these limitations, identity-driven security has received attention as a paradigm that is more consistent with the characteristics of telecom IoT ecosystems. Identity-driven

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

security reframes the concept of location of the network and implicit trust to explicit and verifiable identities of devices, services and users. Under this paradigm, all entities get authenticated and authorized according to their identity and contextual attributes before being given access to network resources or services. This way, fine-grained access control, continuous verification and a better accountability are made possible, which are critical to securing large-scale and multi-tenant IoT deployments.

Telecommunications networks have a unique opportunity to support identity-driven security because of its long use of robust identity mechanisms such as Subscriber Identity Modules (SIM) and Authentication, Authorization and Accounting (AAA) frameworks. Emerging technologies, such as embedded SIM (eSIM) and integrated SIM (iSIM), further enhance the device identity network access binding in the next-generation mobile system . However, the growing diversity of IoT devices and IoT deployment models require the combination of SIM-based identities and non-SIM identity mechanisms, cloud-natives security frameworks and cross-domain trust models [7]. Achieving this integration in a scalable and interoperable way is an open problem.

The motivation of this paper is to discuss how identity-driven security architectures can overcome the trust and scalability requirements of telecom-enabled IoT ecosystems. Rather than offering the specific implementation or empirical evaluation, this work takes a conceptual and analytical approach to explore the architectural principles, threat considerations and trust mechanisms. The main goals are to examine the shortcomings of existing security models, to describe the design of identity-centric architectures for telecom IoT and to examine their consequences for scalability, trustworthiness and compliance with regulations for future digital infrastructures.

The most important contributions of this paper are threefold. First, it offers a formal analysis of security challenges and threat models that are specific to telecom IoT environments. Second, it introduces an identity-based security architecture combining telecom identity primitives with new generation trust models like Zero Trust and cross domain federation. Third, it provides a qualitative assessment of the scalability and trustworthiness of the strategies, showing the benefit, as well as the limitation, of identity-centric strategies in the absence of empirical datasets.

2. Related Work and Background

Security in Internet of Things (IoT) estates has been widely studied because of the explosion of the number of connected devices and their integration in critical digital infrastructure. Existing literature emphasizes the fact that IoT security challenges are not limited to technical ones but are architectural and governance in nature especially when IoT systems are deployed in large scale within telecom and cloud-based environments. Recent research focuses on the intersection of IoT, telecommunications, cloud, and artificial intelligence, which has caused a significant change in old threat models and requires more adaptive and identity-aware security models. There are a number of works that present an overview of cybersecurity challenges in the evolving IoT ecosystems. Qudus [8] addresses the increase of attack surfaces caused by the spread of interconnected digital systems, especially in device heterogeneity with decentralized control. The study highlights the fact that conventional security mechanisms have a difficult time achieving consistent protection across distributed IoT deployments, especially when devices are taken into the equation and interact autonomous and across multiple platforms. Similarly, Adam et al. [9] provide a detailed survey of the security, privacy, trust, and architectural challenges for IoT systems, where they point out the issues around identity management and trust establishment as weaknesses that persist in the current IoT security frameworks. Edge computing and cloud native architectures make IoT security more difficult.

Received: August 04, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Mrabet and Sliti [10] analyze security and trust challenges in edge-enabled smart city environments, highlighting the fact that processing data closer to the source of the data will have lower latency and higher efficiency, but brings new trust dependencies between edge nodes, devices and centralized services. Their analysis indicates secure identity verification and trust management is the key to ensuring the integrity of distributed edge computing infrastructures. These findings support the idea that identity must include more than devices and include services, platforms and orchestration components. Critical infrastructure protection has also been a focus of much recent IoT security research. Okika et al. [11] study IoT-based cybersecurity risks in public utility and critical infrastructure systems, stating that when device identities are compromised, cascading failure and large service disruption can happen. The authors argue that identity spoofing and unauthorised access are still some of the most damaging vectors of attack in such environments. This view is consistent with the broader concerns about IoT security failures in telecom-supported infrastructures having societal and economic ramifications, especially when critical services are relying on continuous connectivity. The concept of Zero Trust Architecture (ZTA) has come to the fore as a solution to the shortcomings of the perimeter-based security models. Aramide [12] discusses the principles of Zero Trust identity in next-generation networks emphasizing the need for continuous verification, least-privilege access and context-aware decision-making processes. The study highlights that identity becomes the main trust anchor in Zero Trust systems and replaces the assumption based on network location. While the work is focused on next-generation networks in general, it is important to note the relevance of identity-centric approaches to IoT deployments that operate in telecom infrastructures. Cloud identity management has also been studied from technical as well as societal point of view. Dammalapati [13] discusses the effect of effective cloud identity management on security, scalability and user trust in large-scale digital ecosystems. The analysis identifies that cloud-based identity solutions need to facilitate federation, interoperability and policy consistency across organizational boundaries. These requirements are relevant especially for telecom IoTs ecosystem, where devices, applications, and services often are controlled by different stakeholders and deployed in a hybrid cloud and edge environment. Telecommunications specific identity protection mechanisms have been intensively studied in regards to 5G and emerging 6G networks. Scalise et al. [14] offer a survey of user identity protection techniques in 5G core networks, including improvements such as hidden identifiers and better authentication protocols. However, the authors also list some limitations with current approaches, especially when expanding the concept of identity protection beyond just subscribers to massive numbers of IoT devices. Their work implies that future 6G systems will need more flexible and scalable identity systems which can support different types of devices and trust relationships. In addition to technical surveys there are also insights into regional and organizational perspectives regarding IoT security in the form of position papers. Albaqami et al. [15] discuss the future of IoT security from the perspective of emerging startups, focusing on the need for scalable, cost-effective, and identity-aware security solutions. The authors contend that startups and smaller operators may not have the resources in place to adopt complex security infrastructures and so automated identity management and standardized trust frameworks may be particularly important. Across these studies, there are a number of common themes. First, current IoT security methods are often silos, covering only one aspect of IoT security (e.g., device, network or application security) and lacking the provision of an end-to-end trust model. Second of all, identity management is repeatedly listed as a critical and underdeveloped aspect of IoT security, especially in telecom-enabled environments, where there are scale, mobility, and multi-tenancy. Third, while some potential directions such as Zero Trust and cloud-native security are promising for driving security, there

Received: August 04, 2025

is not enough exploration in literature about their combination with telecom identity mechanisms. This paper elaborates on these observations by explicitly examining the topic of identity-driven security in telecom IoT ecosystems. Unlike previous studies that mostly present an overview of threats or suggest an isolated solution, this paper takes a holistic view from an architectural perspective. By combining knowledge from IoT security surveys, Zero Trust approach, cloud identity management, and telecom identity protection mechanisms, the paper intends to fill the existing research gaps and offer a comprehensive conceptual framework for scalable and trustworthy IoT security in the future telecom infrastructure.

3. Threat Model and Security Requirements

Telecom-enabled IoT ecosystems live and operate in highly distributed, heterogeneous and multi-stakeholder environments, which means that the surface area of threats is much larger than for traditional IT systems. A clear and systematic threat model is thus required to comprehend the security risks and to derive the right security and trust requirements. In identity driven IoT security, threats are mostly related to compromise, misuse or impersonation of identities across devices, services and network components.

3.1 Adversary Model for Telecom IoT Systems

Adversaries that attack telecom IoT ecosystems can be broadly categorized on the basis of their abilities and access levels. External adversaries are outside the trusted boundaries of network operators and service providers and use exposed interfaces, poor authentication mechanisms or misconfigurations to gain access into IoT systems. These types of attackers are usually trying to impersonate legitimate devices or services in order to gain unauthorized access to network resources and sensitive data. Internal adversaries are a more complicated threat class. These may include compromised IoT devices, malicious insiders or hijacked edge nodes that already have some degree of trust within the system. Such adversaries are dangerous in particular because they can get past perimeter defenses and take advantage of implicit trust relationships built into legacy architectures. The increasing autonomy of networked systems brings with it further exposing systems to being used for identity misuse. Emerging research suggests that there will also be threats against future IoT ecosystems, from autonomous and AI-enabled entities. The need for trusted identities has not only been associated with physical devices but also AI agents that are operating within telecom-hosted infrastructures, since such identity compromise can result in any large-scale misuse of delegated authority and automated decision-making processes [16].

3.2 Common Attack Vectors

Identity-related attack vectors are some of the most important threats in large-scale IoT deployments. Identity spoofing and device impersonation this allows for adversaries to pose as a legitimate entity to bypass a network access control and gain unauthorized access to network services and data streams. These attacks are especially damaging in telecom IoT environments, because network access in many cases means trust at many layers of these systems. Weak authentication mechanisms and lack of identity protection are still predominant weaknesses found in 5G-enabled IoT systems. These weaknesses can be exploited to perform denial-of-service attacks, exfiltration of data or lateral movement between interconnected IoT services that can result in the disruption of operations and potential physical harm for industrial or infrastructure deployments. The addition of cloud and edge computing makes it even more extensive. Misuse of service identities and credential leakage, and the exploitation of trust across domains are typical risks in cloud-native environments, particularly when trust relations

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

are static or not properly verified. Such vulnerabilities are compounded in IoT ecosystems in which there is dynamic interaction between devices and multiple services at edge and cloud.

3.3 Security and Privacy Requirements

To counter those threats, telecom systems of the IoT need to meet a set of basic security requirements. Strong and mutual authentication is critical to guarantee that both the devices and services can reliably confirm the identity of each other. Authentication mechanisms must be resistant to impersonation and replay attacks and be lightweight enough to work on the resource-constrained IoT devices. Authorization mechanisms must follow least privilege access, where entities can only get access to those resources they need to perform the role they are designated. Continuous authorization, as opposed to one-time access decisions, is becoming a greater need in dynamic IoT environments when the context of the devices and the trust conditions may rapidly change. Confidentiality and integrity of data as it is in transit and at rest must be ensured through cryptographic mechanisms which are tightly bound to verified identities. Privacy preservation is also very important. IoT devices often process sensitive personal, industrial or operational data. Security architectures must therefore enable controlled identity disclosure, anonymization where suitable, as well as compliance with the relevant regulatory frameworks, without losing too much traceability for accountability [17].

3.4 Trust, Scalability, and Interoperability Requirements

Beyond the conventional security properties, telecom IoT ecosystems must have trust mechanisms that are scalable and can handle massive numbers of devices. Identity management solutions need to provide the ability to automatically provision, rotate and revoke credentials without manual intervention in order to be operationally feasible at scale. Scalable and secure data infrastructures increasingly rely on automated identity and trust orchestration for the support of enterprise-level digital transformation [18]. Interoperability between different heterogeneous platforms and administrative domains is another important requirement. Industrial IoT ecosystems tend to have numerous vendors, operators, and service providers that have different security policies and identity systems. Without interoperable frameworks for identity and federation, trust establishment across such domains remains fragile and error-prone [19]. Resilience and forensic preparedness are also necessary. Trustworthy identity attribution is helpful for digital forensics, incident response and post-incident recovery by enabling accurate accountability and root cause analysis after security breaches [20].

3.5 Summary of Requirements

In summary, it can be said that the threat landscape of telecom-enabled IoT systems is dominated by identity-centric risks, such as impersonation, unauthorized access, and cross-domain trust exploitation. Addressing these threats means that security architectures that focus on robust identity verification, continuous trust assessment, privacy preservation, scalable identity lifecycle management, and trust framework interoperability are needed. These requirements are the basis for the identity driven security architecture proposed in the following sections of this paper.

4. Identity-Driven Security Architecture for Telecom IoT

An identity-driven security architecture prioritizes identity in making every security decision in telecom-enabled IoT ecosystems. Unlike the conventional network-centric approaches that are based on static trust assumptions and perimeter defenses, identity-driven architectures assume

Received: August 04, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

that all devices, services, and interactions are untrusted by default and that they are only explicitly verified.

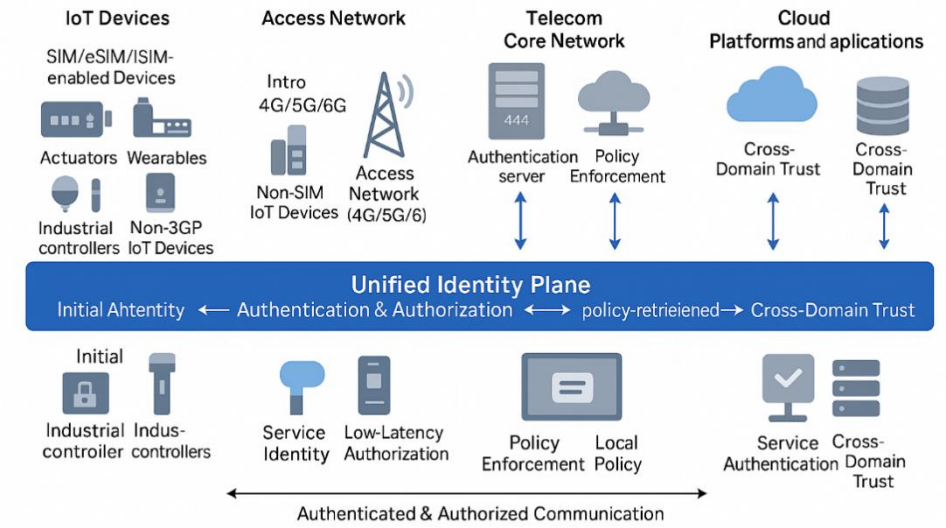

Figure 1. Identity-driven security architecture for telecom-enabled IoT ecosystems.

This paradigm is especially applicable in the realm of telecom IoT environments, where scale, mobility, heterogeneity, and multi-tenancy make implicit trust models useless..

4.1 Design Principles of Identity-Centric Security

The foundational principle of identity driven security is explicit trust establishment. Every entity that is involved in the system, whether it is a device, an application, a network function or a service, must have a verifiable identity that can be authenticated and authorized before accessing resources. Trust is not passed from network location and previous interactions but is constantly being evaluated based on identity attributes and contextual information. Another important principle is separation of identity and connectivity. While telecom networks have traditionally tied identity closely to network access, in modern IoT architectures identities should be able to exist across access technologies, roaming situations and service situations. This separation allows for consistent security enforcement even as devices move between networks, edge platforms and cloud services. Automation and policy driven enforcement is also key to identity driven architectures. Given the scale of telecom IoT deployments, manual identity management cannot be possible. Security policies need to be defined in a declarative way and automatically enforced in all layers of the infrastructure. This helps to ensure consistent application of security controls and helps to reduce the risk of configuration errors.

4.2 Identity Lifecycle Management

Effective identity lifecycle management is required to ensure security is sustained throughout the long operational lifetime of the IoT devices. The lifecycle starts with secure provisioning during which a unique and cryptographically protected identity of a device is assigned. Provisioning can take place at manufacturing time, onboarding or at first network attachment depending on the deployment requirements. Authentication is done whenever a device or service is trying to deal with the network or access resources. In identity-driven architectures, the authentication is usually mutual so that both parties can be sure that each other is who they

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

claim to be. Authorization decisions are then made based on predefined policies which take into account attributes of the identity, the roles and contextual factors such as location or time. Identity revocation and rotation are important and overlooked aspects of the lifecycle. Devices may be decommissioned, compromised or repurposed, which means that their identities and credentials must be revoked in a timely manner. Automated revocation mechanisms ensure that stale, or compromised identities are not allowed to persist within the system. Credential rotation provides an even further reduction of the risk of long-term credential exposure.

4.3 Device, Network, and Service Identity Relationships

Telecom IoT ecosystems involve multiple layers of identity that must be securely linked.

Table 2. Identity Types and Trust Relationships in Telecom-Enabled IoT Systems

Identity Type	Entity Examples	Primary Trust Anchor	Security Function	Deployment Layer
Device Identity	Sensors, actuators, IoT endpoints	Hardware root of trust / certificates	Device authentication and attribution	Device / Access Layer
SIM / eSIM / iSIM Identity	Cellular IoT modules	Telecom operator credentials	Network access and mobility authentication	Access / Core Network
Network Function Identity	Core and virtual network functions	Operator-managed PKI	Secure inter-function communication	Core Network
Service Identity	Applications, microservices	Cloud or platform identity provider	Service authentication and authorization	Edge / Cloud
Platform Identity	Edge nodes, cloud platforms	Federated trust frameworks	Policy enforcement and orchestration	Edge / Cloud
User / Operator Identity	Administrators, operators	Enterprise identity systems	Management and control access	All Layers

Table 2 describes the main types of identities that can be found in the telecom-enabled IoT systems and their corresponding trust anchors, security roles and deployment layers: Device identities are physical or virtual IoT endpoints. Network identities are access rights and connectivity scenarios in the telecom infrastructure. Service identities are applications, platforms, and microservices that are running in edge and cloud environments. An identity-driven architecture creates secure bindings between these layers to create end-to-end trust. For instance, a device identity can be linked to a certain network slice and be permitted to access a determined number of services. These relationships are enforced using policy-based controls as opposed to static configurations, which makes it possible to dynamically adapt these relationships as devices and services change. This multi-layer identity model also offers some accountability and traceability. By ensuring that the relationship between device action with regards to network context and interactions within the services remains clear, the architecture allows for an effective auditing and incident response process and does not take the implicit trust assumptions.

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4.4 Role of SIM-Based and Non-SIM Identities

SIM-based identities such as those offered by SIM, eSIM and iSIM technologies have strong cryptographic roots of trust and are closely embedded in telecom authentication frameworks. These identities are especially useful in providing network access security and mobility management. However, not all IoT devices have SIM technology and many interactions take place outside of the network access layer. Non-SIM identities (e.g. certificate-based or token-based identities) are therefore key ingredients of a full-fledged identity-driven architecture. These identities are allowing for secure interactions at the application and service layers, especially when it comes to cloud native and edge computing environments. Some of the requirements on a unified architecture are: a unified architecture needs to support coexistence and interoperability between SIM-based and non-SIM identity mechanisms. Mapping and federating identities between these mechanisms enables devices to have a consistent security posture across network, edge and cloud domains. This integration helps prevent trust fragmentation and facilitates hormones communications of the security policies at the entire IoT ecosystem.

4.5 Integration with Core, Edge, and Cloud Environments

Telecom IoT architectures are expanding to cover the core network, distributed edge platforms, and centralized cloud infrastructures. Identity-driven security therefore needs to be uniformly enforced across all these environments. In the core network there are identity mechanisms for access control, mobility, and network slicing. At the edge, the identities provide for the processing of data for security, low-latency decision-making, and local enforcement of policies. In the cloud, there are identity controls to protect application logic, data storage and service orchestration. A single common point of identity spanning core, edge and cloud environments allowing for cohesive policy enforcement and trust management. Such an approach helps in reducing security holes due to architectural fragmentation and also simplifies security decision based on consistent identity information irrespective of where processing takes place, which is especially important when dealing with user-centric and safety-sensitive IoT environments such as smart homes and consumer IoT systems [21].

4.6 Architectural Benefits and Limitations

Identity-driven security architectures have a number of benefits such as mitigating against impersonation attacks, fine-grained access control, and scalability through automation. By separating trust from network boundaries, these architectures can also work very well with the modern telecom and IoT deployment models. However they also introduce challenges, such as added architectural-complexity, necessary identity-gov, and overhead for constrained devices. These limitations highlight the need for cautious architectural design and provide impetus for further study of lightweight as well as interoperable identity mechanisms.

5. Identity Models and Trust Mechanisms

Identity-driven security architectures are based on well-defined identity models and powerful trust mechanisms that can be used to facilitate secure interaction between devices, services and network components within telecom IoT ecosystems. Given the scale, heterogeneity and multi-domain nature of such environments, no unique identity model is sufficient by any stretch of the imagination. Instead, different identity paradigms have different tradeoffs in terms of scalability, resilience, governance and operational complexity. Understanding these trade-offs is critical to design trustworthy and adaptable frameworks for IoT security that can work across telecom, edge and cloud domains.

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.1 Centralized Identity Models

Centralized models of identity are premised on the existence of one authoritative provider of identities responsible for identity provision, authentication, and policy enforcement. In telecom worlds, centralized models are a natural fit to existing operational models, in which network operators already have centralized repositories of subscriber and device identities and services. This alignment allows standard security policy enforcement and simplified identity governance and enforcement across a large population of devices [14]. Centralized identity systems have benefits in terms of administrative control, auditability and integration with legacy telecom infrastructures. They support fast revocation of credentials, ability to coordinate policy changes, and central monitoring that is important for operational stability for regulated telecom environments. These models also bring in structural limitations. Centralized identity providers are potential single points of failure and tempting targets for an attacker. Moreover, as IoT ecosystems increasingly transcend multiple operators, cloud providers and enterprise domains, centralized models have a hard time offering a means to support cross-domain trust without complicated and tightly coupled federation mechanisms [7].

5.2 Decentralized and Distributed Identity Models

Decentralized identity models try to mitigate the need for centralized authorities by sharing the control of the identity with a number of entities. In such models, identities are often self-managed or those identities are anchored in distributed trust infrastructures allowing self-proving or the devices and services in the system are independent from one central provider. This improves resilience and systems risk from centralized compromise [7]. In telecom IoT ecosystems, decentralized models are especially appealing for use in case of cross-operator collaboration, roaming and multi-cloud deployments. They allow dynamic establishment of trust between devices and services that are operated by different administrative domains. However, decentralized identity models raise challenges with regards to governance, standardization and consistency of policy. Without clear and well-defined trust anchors, lifecycle management processes and governance frameworks, decentralized systems might have difficulty enforcing uniform security requirements at scale [16].

5.3 Public Key Infrastructure and Certificate-Based Authentication

Public Key Infrastructure (PKI) remains one of the foundational trust mechanisms that is used in both centralized and decentralized identity models. Certificate based authentication provides the ability to strongly authenticate the identity of the devices and allows mutual authentication among devices and services. In telecom applications for IoT, PKI is a scalable way of establishing trust among heterogeneous platforms, access networks and service layers [19]. Despite all the strengths, PKI has added a lot of operational complexity especially when it comes to handling certificate lifecycles for billions of IoT devices. Certificate issuance, renewal, revocation and validation should be highly automated so as not to cause administrative bottlenecks. Furthermore, the lightweight certificate profiles and optimization of validation mechanisms are often needed to cover the resource constrained devices without compromising security guarantees [19].

5.4 Zero Trust Access Control for IoT Devices

Zero Trust principles dramatically change the way in which trust is applied as they eliminate the use of implicit trust and require constant verification. Zero Trust models do not have their identity verification in a one-time basis but rather as a process that evaluates identity, context and risk throughout the interaction lifecycle. Access decisions are also dynamically adjusted

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

depending on real time conditions instead of static credentials [12]. Applying Zero Trust to IoT Ecosystems Imposing access control mechanisms on devices and capabilities and operational constraints. Many IoT devices are constrained in terms of processing power and contextual awareness, requiring devices to be enforced in a hybrid model that includes device identity, network context and controls at the service level. If put into practice, Zero Trust mechanisms greatly limit the effect of compromised devices by limiting lateral movement and unauthorized access throughout telecom IoT environments [12].

5.5 Cross-Domain Trust and Federation

Telecom IoT ecosystems often feature interactions between organizations and administrative boundaries. Devices can connect to another device, process data at edge platform run by another provider, and interact with cloud services run by a third party. Cross domain trust is therefore an essential requirement. Federated identity mechanisms can be used by multiple identity providers to form trust relationships without having to share sensitive credentials. Through federation, identities issued in one domain are able to be recognized and authorized in another domain based on predetermined trust agreements and policies. Effective federation needs common or standard representations of identities, interoperable authentication protocols, and common or consistent governance frameworks to provide security enforcement throughout the domains [7].

5.6 Trust Establishment and Verification Workflows

The process of trust establishment in case of identity driven architectures is based on a structured workflow. An entity first states its identity credentials and an entity has them validated against trusted authorities or distributed trust anchors. Authorization policies are then evaluated to determine what is allowed to be done based on the identity attributes and the contextual factors. Continuous monitoring and verification is taken to ensure trust is upheld over a period of time and is adapted as operational conditions and threat levels change [16].

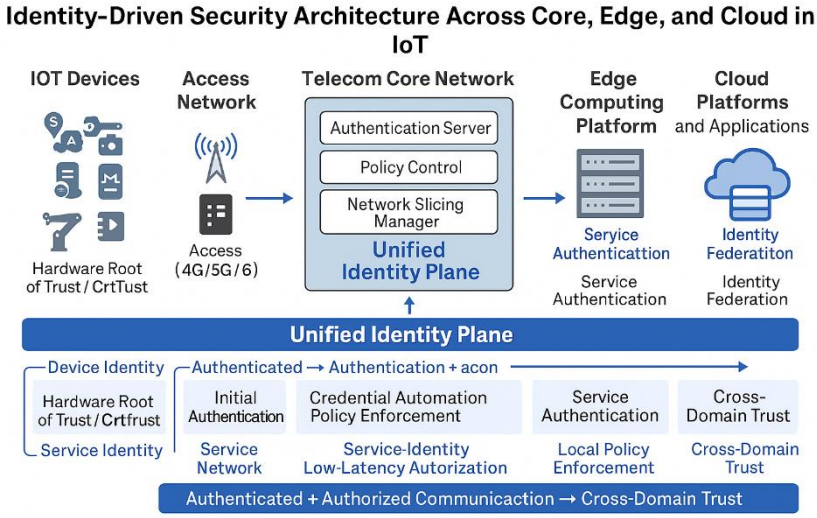

Figure 2. Identity lifecycle and continuous trust verification workflow in telecom IoT systems.

Such workflows make it possible to trust dynamically, so that telecom IoT systems react proactively to changing threats and operational situations. By installing trust check mechanisms

Received: August 04, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

into every interaction guarantees the resilience of systems and lowers the depreciation of static security assumptions that are no longer viable at IoT scale.

6. Scalability Analysis

Scalability is one of the defining requirements of telecom-enabled IoT ecosystems where the number of connected devices is expected to reach billions in fighting. Identity-based security architectures need to be able to scale to huge numbers of devices, multiple administrative domains, and highly dynamic network environments, therefore. Unlike classic security approaches based on static configurations or static processes, scalable identity-centered approaches need to scale out a lot of automation, federation, and enforcement driven by policies to be operational in order to be operationally viable in next-generation telecom networks [5].

6.1 Challenges of Scaling Identity Management

The key scalability challenge in telecom IoT systems is to manage the complete lifecycle of identity of an enormous number of devices. Every device must be securely provisioned, credentials stored, authenticated, authorized and revoked. When such processes are done manually or semi-manually, operational overhead increases exponentially with the scale, which increases the risk of configuration mistakes and systemic security gaps [18]. Authentication Latency also is a critical concern at scale. Telecom IoT deployments frequently require an element of real-time or near-real-time interaction, for which added delays introduced by identity verification may degrade service quality and hurt application performance. Identity-driven architectures must therefore operate with strong security guarantees, and at the same time, stringent latency and throughput requirements especially, for latency-sensitive services such as Industrial Automation and smart infrastructure [10]. Another major challenge is the range of capabilities of different devices. IoT ecosystems consist of a least constrained devices and more capable endpoints with different processing, storage and energy constraints. Designing identity mechanisms that scale across this heterogeneous landscape with an acceptable level of overhead for constrained devices is a very difficult design problem for large-scale telecom deployments [18].

6.2 Automated Onboarding and Credential Management

Automation is necessary to implementing scalability in identity-driven IoT security. Automated onboarding mechanisms allow devices to safely acquire identities and credentials with very little human involvement, which can decrease the time required to deploy the device and the complexity of the operation. Such mechanisms make it possible to apply security policies consistently from the time a device is brought into the network and is especially important in large-scale and rapidly evolving IoT environments. [18] Automated credential management also furthers the cause of scalability when it comes to regularly rotating, renewing and revoking credentials without manual oversight. This provides for longer lived credentials risks, and continuous security posture improvement. Policy-driven automation enables the identity lifecycle processes to dynamically adapt to changes in operation, such as a change in device role, mobility, or network reconfiguration [5].

6.3 Identity Federation Across Operators and Tenants

Telecom IoT ecosystems are often across different network operators, service providers and enterprise tenant. Identity federation is, therefore, an important scalability enabler which enables identities issued in one administrative domain to be recognized and trusted in another. Without federation, every domain would have to deal with having different identities for the

Received: August 04, 2025

same device, creating duplication, inconsistency and additional administrative load [18]. Federated identity models are a way of supporting scalability by allowing trust relationships to be built at the domain level, as opposed to the individual device level. This greatly simplifies the problem of cross-domain identity management and can be used to achieve seamless operation of devices across different heterogeneous networks and service environments. However, federation brings with it governance, policy consistency and trust assurance challenges which must be carefully managed to maintain security and operational consistency [5].

6.4 Impact of Network Slicing and Virtualization

Network slicing and virtualization are fundamental characteristics of telecom networks of the future and of telecom networks today, allowing several logical networks to run on common physical networking infrastructure. While these technologies enhance flexibility and resource utilization, they add more scalability aspects to identity-based security architectures [5]. In sliced networks environments, damages could "dynamically move or change their devices from one slice to another slice based on the service requirements or based on the operational conditions." Identity driven security mechanisms must then facilitate the ability to quickly reassign access rights and policies without affecting trust and security. Virtualized network functions and cloud-native service architectures become even more dynamic in terms of environment and consequently demand identity systems that can adapt in real time to changing network and service environments [10].

6.5 Scalability Without Empirical Datasets

Whilst this paper does not provide empirical measurements of scalability, through a process of analytical reasoning it could be reasoned that identity-driven architectures provide superior scalability to static network-centric security models. By automating identity lifecycle management processes, making better use of federation, and separating trust from network boundaries, identity-centric approaches can reduce the complexity of operations, and operational complexity, and can provide for consistent security enforcement at scale [18]. However, scalability is not entirely a technical challenge. Organizational processes, governance structures and standardization efforts have a decisive role to play in deciding whether or not identity-driven security can be effectively scaled across global telecom IoT ecosystems. These considerations point to the need for ongoing research, cooperation with the industry and compatibility with emerging telecom standards [5].

7. Trustworthiness and Security Implications

Trustworthiness is an important characteristic of telecom-enabled IoT ecosystems in general, especially as such systems are used for safety-critical, mission-critical and socially sensitive applications. Failures in trust can lead not only to breaches of data but also cause physical harm, interruptions of service and societal outcomes. Identity-driven architectures for security have noteworthy implications in the way trust is built, sustained and validated between devices, networks and services. By making security decisions based on verifiable identities, as opposed to otherwise unchecked assumptions, such architectures help deliver stronger, auditable, and more transparent trust models from complex IoT deployments [9].

7.1 Data Integrity and Authenticity

One of the most immediate benefits of identity driven security is data integrity and authenticity. When data exchanges are cryptographically bound to authenticated identities, it will be possible to verify the source of data as well as integrity during transmission and processing. This

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

capability is particularly important in telecom IoT environments where the data may pass through a number of network segments, edge platforms and cloud services before it is consumed by applications [17]. Identity-based authentication ensures that data is coming from any legitimate device and service to minimize the possibility of data injection, manipulation or replay by unauthorized entities. Integrity mechanisms that are linked to identity credentials offer high assurance of ensuring that data has not been changed en route, making it possible to make trustworthy and accurate decisions in downstream applications. This is of utmost importance in industrial automation, healthcare monitoring, and in intelligent transportation systems, where the wrong or tampered data may have serious ramifications in terms of operation and safety [11].

7.2 Secure Device-to-Device and Device-to-Cloud Communication

Identity-driven security provides communication security in variation of interactions throughout IoT ecosystem. Device-to-device communication has mutual authentication, which means that the involved entities can authenticate each other's identity before exchanging data. This greatly helps in reducing the chances for man-in-the-middle attacks, unauthorized message injection and spoofed command execution in peer to peer IoT interactions [9]. Similarly, device to cloud communication is improved with the help of identity aware access control and encryption mechanisms. By enforcing security policies based on the device and service identities that can guarantee that only permitted entities are able to access sensitive data or call critical services on a cloud platform. This approach alleviates the need for network-level protections and provides for secure communication even in highly dynamic, distributed and multi-tenant telecom IoT environments [17].

7.3 Resilience Against Identity-Based Attacks

Identity-based attacks - such as impersonation, credential theft and unauthorised access - are some of the worst threats to large-scale IoT systems. Identity-based security architectures provide mitigation over these risks by demanding strong authentication, least-privilege authorisation and constant verification. Even if a device or a credential is compromised, it is limited in the extent of damage as granular access controls and real-time trust assessment mechanisms [20]. In addition, the capacity for detection and response is improved by identity-centric monitoring. Through correlating actions with certain identities, security systems can better recognize abnormal behavior and track attack routes and trigger immediate mitigation actions. This capability contributes to the overall system resilience and aids quicker recovery from external attack as well as internal threats, which is of particular importance in industrial and critical infrastructure IoT deployments [11].

7.4 Privacy Preservation and Regulatory Compliance

Privacy preservation is a basic need in many IoT applications especially those that involve personal, medical or sensitive operational data. Identity-driven security architectures support the privacy concept by allowing controlled identity disclosure and exposure of identifying information. Techniques such as pseudonymous identities, attribute-based access control and role separation allow systems to balance accountability and privacy protection [9]. From a regulatory standpoint identity-centric approaches make it easier to comply with data protection and cybersecurity regulations. Clear identity attribution helps in the areas of auditability support, incident reporting, and accountability, which are usually required by regulatory frameworks relevant to the critical infrastructure, healthcare, and public services. At the same

Received: August 04, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

time, flexible identity models enable organizations to adjust security controls to changing legal, ethical and policy requirements without necessarily redesigning system architectures [17].

7.5 Trust Assurance Across the IoT Value Chain

Telecom IoT ecosystems have a complex value chain with device manufacturers, network operators, platform providers, application developers and the end user. This value chain requires trust between each component to ensure sustainable growth of the ecosystem and mass adoption. Identity-driven security lays a common ground of trust by allowing all stakeholders to authenticate identities, enforce consistent security policies, and set up clear accountability relationships [20]. By standardizing on identity and trust mechanisms, telecom IoT ecosystems can help to reduce fragmentation, improve interoperability and enhance confidence between participants. This in turn helps in more widespread adoption of IoT technologies in safety-critical and regulated fields. However, end-to-end trust needs not only strong technical solutions, but also consistent governance models and cooperation between ecosystem participants across organizational and jurisdictional boundaries [11].

8. Application Scenarios and Use Cases

Identity-driven security architectures are relevant in many domains of telecom-enabled IoT, especially those that are characterised by large-scale deployment, multi-stakeholder participation and high security and trust requirements. As IoT applications continue to intersect with critical services and the public infrastructure, identity-centric approaches have the potential to offer a unifying framework for enforcement of security policies, accountability and enable trustworthy cross-domain interactions [1]. This section addresses some representative application scenarios to demonstrate the use of identity-driven security to improve operational resilience, trust and efficiency in different IoT application scenarios.

8.1 Smart Cities and Critical Infrastructure

Smart city deployments are using IoT devices in the transportation system, energy grid, water management, public safety and environmental monitoring systems. These environments have various public and private stakeholders, each of which have different systems that have to interoperate securely at scale. Identity-driven security allows for clear attribution of the actions of devices, and it can ensure that data streams and control commands come from authenticated and authorized objects [10]. By adding verifiable identities to sensors, actuators, and digital services, the smart city platforms can ensure fine-grained access control and prevent unauthorized access to and manipulation of the critical infrastructure. Identity-centric architectures also enable secure sharing of data between departments in a municipality as well as external service providers with accountability and auditability. This kind of capability is especially relevant for incident response and forensic investigation after security events, for which reliable attribution of the identity is crucial for root cause analysis and recovery [1].

8.2 Industrial IoT and Industry 4.0

Industrial IoT implementations are the basis for automation, predictive maintenance, and real-time monitoring for manufacturing and production environments. These systems are frequently closely linked with physical processes, i.e., the failure of cybersecurity can directly convert to the physical damage, safety hazards, or severe economic loss. Identity driven security ensures that only authenticated and authorized devices and services can interact with industrial control systems (reducing the attack surface of cyber-physical operations) [15]. And, by tying device identities to specific roles, functions and operational situations, industrial IoT platforms are able

Received: August 04, 2025

to enforce least privilege access and limit the impact of compromised components. Identity-based trust mechanisms also provide for secure integration of third-party vendors, maintenance providers and supply chain partners supporting collaboration without having to expose sensitive operational assets. This is becoming increasingly important in Industry 4.0 environments, where production systems are of deep interconnectedness across organizational boundaries [10].

8.3 Healthcare and Remote Monitoring

Some of the healthcare IoT applications are remote monitoring of patients, wearable health devices, and connected medical equipment. These systems deal with highly sensitive personal and medical information and are subjected to strict controls in terms of regulatory and ethical guidelines. Identity-driven security architectures are a core part of ensuring patient data confidentiality, integrity, and availability and supporting reliable clinical workflows [21]. By attaching strong and verifiable identities to medical devices and systems, medical service providers can authenticate data sources and avoid tampering or unauthorised access. Identity-based access control to ensure that only authorized clinicians, applications, and backend systems have access to patient information. In addition, identity-centric logging and auditing capabilities help with regulatory compliance and traceability in case of data breaches, system failures or adverse clinical events [21].

8.4 Transportation and Connected Vehicles

Transportation systems are now increasingly dependent on connected vehicles, intelligent traffic management and vehicle to everything (V2X) communication. These applications require ultra low latency, high reliability and strong security guarantees, as failures can have a direct impact on the safety of the public. Identity-driven security offers a basis for trust-worthy communication between vehicles, roadside infrastructure and backend services [1]. By authenticating the identity of vehicles and infrastructure, transportation systems can prevent spoofing, unauthorised message injection and malicious control commands. Identity-centric trust models further allow the dynamic authorization from contextual parameters such as the role of the vehicle, location or operational state. This is for adaptive traffic management, collision avoidance and safety-critical services. Identity-based accountability is also helpful in regulating oversight and liability after traffic accidents or system failures [15].

8.5 Comparative Security Implications Across Domains

While the specific operational requirements of each application domain are different, common security problems arise across scenarios, such as identity spoofing, unauthorized access and cross-domain trust management. Identity-driven security architectures aim at solving these issues by offering a consistent way to build trust, enforce policies and ensure accountability in heterogeneous IoT environments [10]. The flexibility of the identity-centric approaches enables them to be adapted to domain-specific constraints (e.g. latency sensitivity in transportation / privacy requirements in healthcare) while preserving the same security principles. These application scenarios prove that identity-driven security is not just limited to a single vertical but is a basic enabler for secure, scalable and trustworthy telecom IoT ecosystems across a wide range of domains [21].

9. Challenges, Limitations, and Open Research Issues

Despite the benefits that identity-driven security architectures offer in telecom-enabled IoT ecosystems, there are still a number of challenges and limitations that prevent large-scale

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

adoption and successful deployment. Dealing with those issues is critical in achieving executions of scalable trustworthy and interoperable IoT infrastructures.

9.1 Deployment Complexity and Interoperability Challenges

One of the main challenges related to identity-driven security is complexity at the time of deployment. Implementing identity-centric architectures requires an integration of the identity management systems across network, edge and cloud environments, all of which may use different technologies and operational models. This is not a simple task if consistent policy enforcement is to occur at all these layers, especially in heterogeneous telecom ecosystems that address multiple vendors and service providers. The issue of interoperability makes deployment more difficult. IoT ecosystems are typically comprised of a variety of devices and platforms that can support a variety of identity standards and protocols. Without common frameworks and interfaces, it is still not easy to have seamless identity federation and trust establishment across domains. This fragmentation can mean that the security posture is not consistent and the benefits of identity-driven approaches can be lost.

9.2 Legacy Device Integration

Many current IoT deployments have legacy devices in them that do not support modern identity and security mechanisms. These types of devices can be devices that have limited processing power, have outdated firmware, or have hard-coded credentials, which makes them hard to integrate into identity-centric architectures. Replacing or upgrading such devices may not be economically or operationally possible, especially in a large-scale industrial deployment or for infrastructure application. Bridging the gap between legacy and modern systems in many cases will require compensations in the form of controls, such as gateway-based identity enforcement or network-level isolation. While these measures can help reduce some of the risks, they can also add a certain level of complexity and reduce the granularity of security controls that can be applied to the identity.

9.3 Identity Management Overhead in Constrained Devices

Resource-constrained IoT devices come with inherent limitations when it comes to security (identity-based, to be precise). Cryptographic operations, storage of credentials and continuous authentication impose a considerable computational and energy cost. Balancing good security guarantees and device limitations is an open challenge. Lightweight identity mechanisms and cryptographic protocols are needed to optimize the implementation of identity-driven security in constrained devices at all. However, designing such a mechanism without weakening security properties has to be carefully analyzed and requires further research.

9.4 Standardization and Governance Issues

The lack of common standards around identity management in telecom IoT ecosystems is an important hurdle in the adoption. While different identity frameworks and protocols exist, their applicability and interoperability in the large IoT domain is not always well defined. Inconsistent standards make it hard to have cross-domain trust and make it hard to be compliant with regulation. Governance is also of paramount importance. Identity driven security requires clear policies on identity ownership, trust delegation and accountability. In multi-stakeholder ecosystems, it is actually complex to align governance models across organizations and jurisdictions and this often includes issues around legal and regulatory considerations beyond technical design.

Received: August 04, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

9.5 Open Research Directions for 6G and Beyond

Looking to the future, new 6G architectures present new research challenges from the point of view of identity-driven security. Ultra-dense networks, network management powered by AI, and digital twins will make the system even more complex and dynamic. Research is needed to focus on establishment of how identity models can cope in environments with high levels of autonomy, where devices and services may dynamically build and dissolve trust relationships. Formal security model sortains, trust verification mechanisms and standardised identity frameworks are promising paths to research. Addressing these open issues will be important to ensuring that identity-based security is able to support future telecom IoT ecosystems effectively and sustainably.

10. Conclusion and Future Work

The explosive growth in the number of IoT deployments to telecom ecosystems has fundamentally changed the requirements for security, trust, and scalability of the digital infrastructure. Traditional models of perimeter-based and network-centric security are no longer sufficient in environments where massive device populations, dynamic connectivity and interactions between multiple stakeholders are prevalent. This paper has argued that identity-driven security is a paradigm shift at its core that can address these challenges in a systematic and scalable way. Through a conceptual and architectural analysis, the paper analyzed how identity-centric approaches make it possible to establish trust explicitly, control access fine-grained and continuously verify across devices, networks, and services. And by putting identity at the heart of security decision making, telecom IoT ecosystems can enable telecom companies to lessen dependence on implicit trust assumptions and increase resilience to impersonation, unauthorized access and cross-domain attacks. The analysis included realizing the importance of identity lifecycle management, the integration of SIM-based and non-SIM identities, and the same security enforcement of security policies across a core, edge and cloud environment. The discussion of identity models and mechanisms for trust showed that there are great capabilities for both centralized and decentralized approaches based on deployment context and governance requirements. Scalability analysis further proved that automation, federation and policy-driven enforcement are necessary for telecom IoT scale management of identities. Application scenarios in the areas of smart cities, industrial IoT, healthcare and transport demonstrated the actual relevance of identity-based security in various security-sensitive areas. Despite its benefits, there are some limitations to using identity-driven security. Deployment complexity, interoperability issues, integration with legacy devices, and constraints of resources on IoT devices continue to be major barriers. Further, there are still no unified standards and governance frameworks to enable seamless cross-domain trust. These challenges highlight the importance of ongoing research and collaboration between telecom operators, technology providers, standards bodies and policymakers, to ensure the successful adoption of 5G. Future work should be aimed at creating formal security models to represent identity-centric trust in highly dynamic telecom environments. Simulation-based assessment and strategic implementations of prototypes may help gain more insight into the performance and scalability trade-offs. In addition, there will be further alignment to emerging 6G architectures such as AI-enabled network management and autonomous service orchestration. Research in lightweight identity mechanisms, interoperable federation frameworks and globally consistent governance models will have a major role to play in achieving trustworthy and sustainable telecom IoT ecosystems. In conclusion, identity-based security presents an interesting and compelling foundation for the development of scalable and trustworthy digital infrastructure in the digital age of pervasive IoT and next-generation telecommunications. Its successful adoption will be

Received: August 04, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

instrumental in achieving secure innovation and long term confidence in future connected systems.

REFERENCES

[1] A. Banerjee, "Securing the future: AI-driven data transmission in IoT-powered smart cities," Soft Computing Fusion with Applications, vol. 2, no. 1, pp. 33–53, 2025.

[2] A. Hassan, N. Nizam-Uddin, A. Quddus, S. R. Hassan, A. U. Rehman, and S. Bharany, "Navigating IoT security: Insights into architecture, key security features, attacks, current challenges and AI-driven solutions shaping the future of connectivity," Computers, Materials & Continua, vol. 81, no. 3, 2024.

[3] A. Uzoka, E. Cadet, and P. U. Ojukwu, "The role of telecommunications in enabling Internet of Things (IoT) connectivity and applications," Comprehensive Research and Reviews in Science and Technology, vol. 2, no. 2, pp. 55–73, 2024.

[4] C. C. Nwoye, "Next-generation protection protocols and procedures for securing critical infrastructure," International Journal of Research Publication and Reviews, vol. 5, no. 11, pp. 4830–4845, 2024.

[5] E. Rodriguez et al., "A Security Services Management Architecture Toward Resilient 6G Wireless and Computing Ecosystems," IEEE Access, vol. 12, pp. 98046–98058, 2024.

[6] H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, "A literature review on security in the Internet of Things: Identifying and analysing critical categories," Computers, vol. 14, no. 2, p. 61, 2025.

[7] J. K. Manda, "Blockchain-based identity management in telecom: Implementing blockchain for secure and decentralized identity management solutions," SSRN, Paper ID 5136783, 2024.

[8] L. Qudus, "Advancing cybersecurity: Strategies for mitigating threats in evolving digital and IoT ecosystems," International Research Journal of Modern Engineering, Technology and Science, vol. 7, no. 1, p. 3185, 2025.

[9] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, "A survey on security, privacy, trust, and architectural challenges in IoT systems," IEEE Access, vol. 12, pp. 57128–57149, 2024.

[10] M. Mrabet and M. Sliti, "Towards secure, trustworthy and sustainable edge computing for smart cities: Innovative strategies and future prospects," IEEE Access, 2025.

[11] N. Okika, G. A. Nwatuzie, L. Odozor, O. Oni, and I. P. Idoko, "Addressing IoT-driven cybersecurity risks in critical infrastructure to safeguard public utilities and prevent large-scale service disruptions," International Journal of Innovative Science and Research Technology, vol. 10, no. 2, 2025.

[12] O. Aramide, "Zero-trust identity principles in next-gen networks: AI-driven continuous verification for secure digital ecosystems," World Journal of Advanced Research and Reviews, vol. 23, no. 3, pp. 3304–3316, 2024.

[13] P. K. Dammalapati, "Societal impacts of effective cloud identity management: A technical perspective," Journal of Computer Science and Technology Studies, vol. 7, no. 5, pp. 408–416, 2025.

[14] P. Scalise, M. Hempel, and H. Sharif, "A survey of 5G core network user identity protections, concerns, and proposed enhancements for future 6G technologies," Future Internet, vol. 17, no. 4, p. 142, 2025.

[15] S. Albaqami, M. Nekovee, and I. Khan, "The future of IoT security in Saudi Arabian startups: A position paper," International Journal of Advanced Computer Science and Applications, vol. 15, no. 11, 2024.

Received: August 04, 2025

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[16] S. Barros, "Trusted identities for AI agents: Leveraging telco-hosted eSIM infrastructure," arXiv preprint, arXiv:2504.16108, 2025.

[17] S. F. Ahmed et al., "Toward a secure 5G-enabled Internet of Things: A survey on requirements, privacy, security, challenges, and opportunities," IEEE Access, vol. 12, pp. 13125–13145, 2024.

[18] T. Adenuga, A. T. Ayobami, U. Mike-Olisa, and F. C. Okolo, "Enabling AI-driven decision-making through scalable and secure data infrastructure for enterprise transformation," International Journal of Scientific Research in Science, Engineering and Technology, vol. 11, no. 3, pp. 482–510, 2024.

[19] T. Arif, B. Jo, and J. H. Park, "A comprehensive survey of privacy-enhancing and trust-centric cloud-native security techniques against cyber threats," Sensors, vol. 25, no. 8, p. 2350, 2025.

[20] V. R. Kebande and A. I. Awad, "Industrial Internet of Things ecosystems security and digital forensics: Achievements, open challenges, and future directions," ACM Computing Surveys, vol. 56, no. 5, pp. 1–37, 2024.

[21] Y. G. Hassan, A. Collins, G. O. Babatunde, A. A. Alabi, and S. D. Mustapha, "Secure smart home IoT ecosystem for public safety and privacy protection," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 5, no. 1, pp. 1151–1157, 2024.

Received: August 04, 2025