Toward Secure Content-Centric Approaches for 5G-Based IoT: Advances and Emerging Trends

Ghada Jaber, Mohamed Ali Zormati, Walid Cavelius, Louka Chapiro, Mohamed El Ahmadi
Université de Technologie de Compiègne, Sorbonne Universités, CNRS,
Heudiasyc UMR 7253, CS 60 319 - 60 203 Compiègne Cedex, France
Email: ghada.jaber@hds.utc.fr, mohamed-ali.zormati@hds.utc.fr,
walid.cavelius@etu.utc.fr, louka.chapiro@etu.utc.fr, mohamed.el-ahmadi@etu.utc.fr

***Abstract*—The convergence of the Internet of Things (IoT) and 5G technologies is transforming modern communication systems by enabling massive connectivity, low latency, and high-speed data transmission. In this evolving landscape, Content-Centric Networking (CCN) is emerging as a promising alternative to traditional Internet Protocol (IP)-based architectures. CCN offers advantages such as in-network caching, scalability, and efficient content dissemination, all of which are particularly well-suited to the constraints of the IoT. However, deploying content-centric approaches in 5G-based IoT environments introduces significant security challenges. Key concerns include content authentication, data integrity, privacy protection, and resilience against attacks such as spoofing and cache poisoning. Such issues are exacerbated by the distributed, mobile, and heterogeneous nature of IoT and 5G systems. In this survey, we review and classify existing security solutions for content-centric architectures in IoT-5G scenarios. We highlight current trends, identify limitations in existing approaches, and outline future research directions with a focus on lightweight and adaptive security mechanisms.**

***Index Terms*—Internet of Things (IoT), 5G networks, Content-Centric Networking (CCN), IoT security.**

I. Introduction

The rapid growth of the Internet of Things (IoT) and the widespread deployment of 5G networks are profoundly transforming communication paradigms. IoT applications, ranging from smart cities and autonomous vehicles to industrial automation and healthcare systems, demand not only ubiquitous connectivity but also efficient, secure, and scalable data management [1]. At the same time, 5G technologies bring new capabilities — such as ultra-reliable low-latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC) — that are essential for meeting the diverse requirements of next-generation IoT systems [2].

Given the evolving demands of IoT applications and the advanced capabilities introduced by 5G networks, Content-Centric Networking (CCN) has emerged as a compelling alternative to the traditional host-centric Internet Protocol (IP) communication model [3]. Rather than focusing on the location of data, CCN centers communication on the content itself. This paradigm shift enables key features such as in-network caching, native multicast, and content-based security, making it particularly well-suited to the dynamic, resource-constrained, and mobility-intensive conditions that characterize IoT-5G environments [4].

However, despite its conceptual advantages, integrating content-centric architectures into 5G-based IoT systems introduces several security challenges [5]. Traditional security models are often location-dependent or centralized, which makes them poorly suited to the decentralized nature of CCN. Furthermore, IoT devices typically have limited processing power, memory, and energy, which complicates the deployment of conventional security mechanisms. Threats such as content poisoning, interest flooding, spoofing, and unauthorized data access are more critical in scenarios with high mobility, heterogeneous devices, and intermittent connections, which are common in 5G-enabled IoT [6].

These challenges raise a critical research question: How can security be effectively and efficiently enforced in content-centric architectures deployed within 5G-enabled IoT, given the constraints and vulnerabilities inherent to both technologies? To address this question, this survey provides an overview of existing approaches and techniques aimed at securing CCN in IoT-5G applications. It categorizes the state-of-the-art solutions, highlights their strengths and limitations, and identifies open issues that remain unresolved. Special attention is given to emerging trends such as lightweight cryptographic mechanisms, trust management models, and the use of machine learning for adaptive threat detection [7].

There has been a significant research effort exploring the individual and combined roles of the IoT, 5G, and CCN, particularly with consideration of their security aspects. However, to the best of our knowledge, no existing work has focused on the security of content-centric 5G-based IoT. Thus, this work aims to address this gap and serve as a starting point for researchers and practitioners designing secure content-centric solutions for next-generation IoT-5G systems.

The remainder of the paper is organized as follows. Section II introduces the background of IoT, 5G, and CCN technologies. Section III highlights the key security requirements of CCN for 5G-based IoT. Section IV provides an overview of recent advances in security solutions for content-centric 5G-based IoT. Emerging trends and the most prominent future directions are discussed in Section V. Finally, the review is concluded in Section VI.

II. Background

In this section, we present the main concepts of IoT, 5G networks, and CCN, highlighting their core capabilities and how their integration opens up new opportunities.

A. Internet of Things (IoT)

The Internet of Things (IoT) refers to a distributed network that connects billions of objects (i.e., things) to each other and to the Internet. This connectivity enables a wide range of services across various domains [8]. Notable examples include smart city deployments, connected healthcare systems, and smart agriculture solutions.

The complexity of the IoT primarily stems from the tremendous number of heterogeneous devices connected to the Internet and communicating together. These devices often operate in constrained environments where computational and energy efficiency are critical [9]. Such limitations pose significant security challenges because conventional security mechanisms tend to be resource-intensive. Nevertheless, real-world IoT implementations must ensure essential security properties such as integrity, authentication, and confidentiality [10].

To effectively support its diverse applications, the IoT relies on several networking technologies, most notably the fifth generation of telecommunications networks, known as 5G. 5G is widely recognized as a key enabler of large-scale IoT deployment [2].

B. Fifth-Generation (5G) Networks

The fifth-generation (5G) mobile communication system, defined by the 3rd Generation Partnership Project (3GPP), represents a major advancement in mobile telecommunications. It introduces significant improvements in data rates, latency, reliability, and support for massive device connectivity [11]. The 5G requirements and vision for applications and services are captured in three primary usage scenarios: eMBB, URLLC, and mMTC. The relevance of specific key capabilities depends on the use case, although all key capabilities are significant in most cases. All of these scenarios are relevant to IoT use cases and are defined as follows [12].

- **Enhanced Mobile Broadband (eMBB):** Targets high data throughput and extended coverage for bandwidth-intensive applications. It enables IoT use cases such as augmented and virtual reality, remote diagnostics, etc.
- **Ultra-Reliable Low Latency Communications (URLLC):** Focuses on delivering ultra-low latency (below 1 ms) and extremely high reliability (99.999%) for mission-critical services. This is essential for time-sensitive IoT applications like autonomous driving, industrial automation, and remote surgery.
- **Massive Machine-Type Communications (mMTC):** Supports the simultaneous connection of a vast number of low-power devices (up to one million per square kilometer) making it ideal for large-scale IoT deployments such as smart cities, precision agriculture, and industrial monitoring.

By addressing the diverse communication requirements, 5G serves as a foundational enabler for the large-scale deployment of IoT systems. However, despite its advances in connectivity and performance, 5G has traditionally relied on a host-centric communication model, which limits performance in highly dynamic, data-intensive environments. Recent developments, particularly through the Open Radio Access Network (O-RAN) architecture, introduce disaggregated control via elements such as the RAN Intelligent Controller (RIC), enabling more flexible, intelligent, and service-oriented paradigms that move beyond strict host-centricity. To further address these challenges, content-oriented architectures have emerged as a promising alternative, offering greater efficiency, scalability, and flexibility for next-generation IoT-5G ecosystems [13].

C. Content-Centric Networking (CCN)

Content-Centric Networking (CCN) represents a paradigm shift from the traditional host-based IP model toward a content-oriented communication architecture. In CCN, data is requested and delivered based on content names rather than host addresses, allowing users to retrieve information regardless of its physical location [14]. In CCN, communication occurs through the exchange of two packet types: Interest packets, which request content by name, and Data packets, which carry the requested content and its signature [15].

This design enables several key features that are particularly relevant for dynamic, distributed, and resource-constrained IoT-5G systems [13]:

- **In-network caching:** Intermediate nodes can temporarily cache content, enabling future requests to be served locally. This reduces latency, minimizes bandwidth usage, and improves data availability. This is valuable for IoT devices that typically have limited connectivity.
- **Native multicast support:** Any node that holds the matching data can satisfy a single interest (i.e., request) packet, enabling efficient one-to-many data distribution without redundant transmissions. This is particularly beneficial for IoT deployments (e.g., firmware updates).
- **Decoupling of content from location:** Data retrieval is based on content names rather than network addresses. This approach supports mobility and dynamic topologies. This flexibility is essential for IoT-5G systems, as devices often change locations or network conditions.

CCN provides valuable security features, one of which is content-based security [16]. In this design, security is embedded directly into the data, typically via cryptographic signatures. This ensures the integrity and authenticity of the data, regardless of the source or delivery path.

Despite its advantages, integrating CCN into IoT-5G environments presents security challenges [5]. CCN lacks native mechanisms for confidentiality, access control, and privacy. Cached data in the network is difficult to restrict to authorized users, and the open, distributed nature of in-network caching exposes the system to threats such as unauthorized access, interest flooding, and content poisoning.

These issues are amplified by the limited resources of IoT devices and the high degree of mobility and heterogeneity of 5G networks. Therefore, designing a secure content-centric 5G-based IoT requires addressing a set of security requirements with novel, lightweight, context-aware mechanisms that go beyond conventional approaches.

III. Security Requirements in Content-Centric 5G-Based IoT

The combination of CCN, 5G networks, and the IoT creates a powerful yet challenging environment. Each paradigm offers its own advantages and presents different challenges. Ensuring security in this multifaceted environment requires addressing the vulnerabilities inherent to each technology. In the following, we introduce the key security requirements for content-centric 5G-based IoT.

- **Resource constraints of IoT devices:** IoT devices typically have severe limitations in terms of processing power, energy, and memory. Traditional cryptographic solutions, such as Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA), are too computationally expensive [17]. Therefore, lightweight cryptographic schemes are necessary.
- **Confidentiality and integrity in 5G:** 5G networks introduce security enhancements, such as the use of temporary identifiers and robust key distribution schemes, to preserve user confidentiality. However, vulnerabilities can still arise from unreliable hardware or misconfigured network slicing policies [18]. The large-scale wireless nature of 5G increases exposure to risks such as eavesdropping and signal jamming, and rogue base stations [19], all of which must be considered when designing secure IoT systems.
- **Content integrity and authenticity in CCN:** In CCN, data is cached and retrieved based on content names. This model requires mechanisms that ensure content has not been altered during caching or transmission. Solutions include digital signatures, Hash-Based Message Authentication Codes (HMACs), and secure hash-based naming [20]. However, due to limitations of IoT devices, these verification methods must be efficient.
- **Access control and trust management:** Since CCN decouples content from its source, access control must be enforced at the content level rather than through traditional, host-based mechanisms. This requires dynamic, context-aware access control schemes to manage permissions across distributed caches. Various trust management strategies have been proposed, including centralized trusted authorities, blockchain-based frameworks, zero-trust architectures, and named tokens [21].
- **Attack detection and resilience:** The convergence of the IoT, 5G, and CCN technologies has created a complex threat landscape that is vulnerable to Distributed Denial-of-Service (DDoS) attacks, content poisoning, spoofing, and unauthorized data access, to name a few. Edge-based anomaly detection mechanisms that leverage machine learning (ML) models have proven effective in combating these threats [22]. Multi-access edge computing (MEC) further enhances security by enabling localized threat detection and mitigation, improving real-time responsiveness, and reducing centralized bottlenecks [23].

Securing content-centric, 5G-based IoT systems demands a cross-layered approach. Resource-constrained IoT devices require lightweight cryptography, while 5G capabilities can be used to isolate and delegate security tasks. CCN needs embedded, data-centric protections such as content-naming-based signatures and decentralized trust. Effective defense combines secure transmission, adaptive access control, distributed trust management, and edge-level threat detection to build scalable, resilient, and trustworthy systems at the intersection of IoT, 5G, and CCN.

IV. Review of Existing Security Solutions

This section provides an overview of existing security solutions in the context of the integration of IoT, 5G, and CCN, and evaluates how these solutions address the key challenges outlined beforehand. The solutions are categorized into three main areas: cryptographic mechanisms, trust management models, and access control with privacy preservation. This structure reflects the multifaceted nature of securing content-centric 5G-based IoT systems.

A. Cryptographic Mechanisms

Cryptographic mechanisms form the foundation of all subsequent security services. These mechanisms enable data confidentiality through encryption, data authenticity and integrity through digital signatures, and secure key exchanges, which are essential for secure communication.

Asymmetric cryptography allows content producers to sign data for widespread verification of its authenticity and integrity. Examples of these algorithms include RSA and Elliptic Curve Cryptography (ECC), which are often used in identity-based schemes [30]. However, public key operations can be computationally intensive for resource-constrained IoT devices, as well as for network-wide verification. The use of Public Key Infrastructure (PKI) also introduces additional computational overhead.

Symmetric key cryptography is generally faster for encrypting data once a shared key is established, making it suitable for constrained devices if key distribution is managed efficiently. Schemes based on symmetric principles, such as those using hash functions and *XOR* operations for token generation, are designed to be lightweight and efficient. Although robust algorithms like AES exist, their suitability for the most constrained devices is still a concern. Consequently, a hybrid approach using asymmetric methods for key establishment and symmetric methods for data protection is often practical. For example, the Elliptic Curve based Multicasting Handshake Protocol (ECMHP) [29] proposes an ECC-based secure handshake mechanism for multicasting in CCN-IoT environments to efficiently secure group communications.

TABLE I
OVERVIEW OF RECENT SECURITY SOLUTIONS FOR CONTENT-CENTRIC 5G-BASED IOT SYSTEMS

Reference	Year	IoT	5G	CCN	Lightweight	Security Requirements				
						Integrity	Confidentiality	Authentification	Control	Trust
[20]	2020	✓	✗	✓	✓	✓	✗	✓	✗	✗
[24]	2021	✓	✗	✓	✓	✓	✗	✓	✗	✗
[25]	2021	✗	✗	✓	✓	✓	✗	✗	✗	✓
[5]	2022	✗	✓	✓	✗	✗	✗	✓	✗	✗
[26]	2023	✓	✗	✓	✓	✗	✓	✗	✓	✗
[27]	2024	✓	✗	✓	✓	✗	✓	✓	✓	✗
[28]	2024	✓	✗	✓	✓	✓	✗	✓	✗	✓
[29]	2024	✓	✗	✓	✓	✓	✓	✗	✗	✗

A (✓) denotes that the corresponding aspect is addressed in the work; a (✗) indicates it is not.

In CCN systems, security is bound to the data itself. Content-based signatures attach digital signatures to data packets to verify their authenticity and integrity network-wide. This is key to preventing attacks like content poisoning, in which malicious content is injected into the network. Producers sign the content, and these signatures travel with the data, enabling any node to verify them. The lightweight identity-based signature (IBS) scheme using HECC, as proposed in [20], is an example of a solution tailored for IoT-based CCN. It aims to reduce PKI overhead while ensuring content integrity and authenticity.

Additionally, the limited resources of IoT devices make lightweight cryptography essential. Traditional algorithms are often too demanding. There is a strong focus on developing cryptographic mechanisms, including ciphers, hash functions, and signature schemes, that provide adequate security while minimizing computational and communication costs.

B. Trust Management Models

Using cryptographic mechanisms naturally presents the challenge of managing trust within the network. Various approaches have been proposed, which we categorize into two main groups: those that rely on a centralized trust entity and those that implement decentralized trust architectures.

Cryptography, especially digital signatures, effectively guarantees content integrity and authenticity, thus protecting against attacks such as content poisoning. Centralized solutions, as in [20] and [24], use trusted entities, such as a network manager or private key generator (PKG), to generate and distribute cryptographic keys. These approaches offer lightweight, identity-based signature schemes that minimize the computational burden of signature verification, providing a practical alternative to traditional PKI models.

An alternative strategy is to eliminate the need for a trusted authority by implementing a decentralized architecture. This can be achieved by setting up a reputation-based trust system. In a CCN network, any node can cache data and respond to an interest. Assigning a reputation level to nodes indicates the reliability of the content they relay.

Decentralized trust models aim to eliminate reliance on a central authority by leveraging reputation-based systems. In CCN environments, where any node may cache and serve data, assigning reputation levels to nodes reflects their reliability in content delivery. For example, the fuzzy reputation trust model proposed in [25] offloads signature verification to clients, which reduces the computational demands on intermediate nodes. This approach is well-suited for resource-constrained IoT devices. Additionally, blockchain technology has been explored to establish decentralized, certificateless trust frameworks that ensure content integrity and authenticity without the probabilistic uncertainties inherent in reputation systems, as demonstrated in [28].

C. Access Control and Privacy

Access control and privacy preservation are among the most critical concerns when deploying CCN for 5G-based IoT systems. The inherent CCN characteristics of in-network caching and content name visibility exacerbate privacy risks and complicate traditional access control mechanisms.

Several lightweight access control mechanisms have been proposed to address these challenges. One example is Attribute-Based Encryption (ABE), which allows content producers to encrypt data based on an access policy defined by user attributes. Only consumers whose attributes satisfy the policy can decrypt the content. The work presented in [27] introduces a lightweight variant of ABE tailored for CCN-based IoT systems. This variant features a hierarchical structure composed of multiple attribute authorities, each responsible for managing a subset of attributes and distributing the corresponding encryption keys. This decentralized design enhances scalability, allows for efficient attribute revocation, and enables the implementation of symmetric key exchange mechanisms, reducing computational overhead.

An alternative to traditional access control mechanisms is the use of decentralized approaches based on blockchain technology. In [5], the authors introduce a decentralized authentication protocol for ICN-based 5G networks known as Blockchain-Based Decentralized Authentication Protocol (BDAP). It uses a distributed, immutable ledger to record

authentication events, ensuring that only legitimate users can access protected content and network resources. Notably, the system is designed to operate without significant modifications to existing ICN-5G network infrastructure, thus promoting deployment and scalability in real-world environments.

Blockchain can be combined with Proxy-Based Re-Encryption (PBE) to enable fine-grained access control, as demonstrated in [26]. PBE enables a semi-trusted proxy to transform ciphertexts from one user to another without accessing the underlying plaintext. Delegating computationally intensive cryptographic operations to a proxy is particularly advantageous in resource-constrained IoT environments, where end devices often lack the capability to perform complex encryption tasks. Furthermore, since the proxy does not need to be fully trusted, this approach simplifies trust management, enhances system scalability, and maintains data confidentiality.

In summary, securing CCN-based 5G IoT systems requires a multidimensional approach that is tailored to this architecture's unique characteristics. Cryptographic mechanisms must be lightweight yet effective, balancing performance with protection in environments with limited resources. Trust management enables secure, decentralized decision-making, allowing content and identities to be evaluated without relying on central authorities. Access control strategies, whether via attribute-based encryption or blockchain-enhanced delegation, must be scalable, granular, and privacy-preserving to match the dynamic, distributed nature of these systems. Table I provides an overview of recent solutions that address these challenges.

Together, these security components form a cohesive framework that meets the evolving demands of the IoT, 5G, and CCN. This framework paves the way for secure and resilient next-generation communication systems.

V. Emerging Trends and Future Research Directions

As IoT, CCN, and 5G technologies converge, they are redefining the landscape of modern communication systems. New trends and research directions are emerging to address the growing need for security, scalability, and adaptability. Key emerging trends include:

- **ML-driven security and network management:** 5G capabilities support ML-based security integration. As shown in [31], ML enables functionalities like threat detection and automated remediation. In [32], a DoS detection system using ML is proposed for IoT in CCN. ML facilitates rapid detection and response. Federated Learning (FL), in particular, is being explored to detect malware in IoT without centralizing data. The combination of FL with CCN-enabled IoT-5G supports decentralized intelligence while preserving privacy, aligning with CCN's data-centric model [33].
- **Zero Trust Architectures (ZTA) in distributed environments:** Traditional perimeter-based security is inadequate for dynamic, distributed systems. ZTA enforces "never trust, always verify" by embedding security into content rather than endpoints [34]. In CCN-5G settings, ZTA fits naturally. The model proposed in [35] combines ZTA with Artificial (AI) for policy-based, context-aware access in 5G slices using Open RAN.
- **Blockchain and Distributed Ledger Technologies (DLTs) for trust management:** DLTs provide immutable, decentralized trust and complement CCN by securing content provenance, key management, and reputation systems without central authorities. Recent works integrate blockchain with IoT and edge computing for tamper-proof data sharing, smart contract-based access control, and trustless consensus [36].
- **Post-Quantum Cryptography (PQC) for constrained devices:** As quantum computing advances, traditional cryptography (e.g., RSA, ECC) becomes vulnerable [37]. PQC provides quantum-resistant alternatives critical for CCN and IoT. In CCN, PQC is explored for content signing, secure naming, and key distribution [38].
- **Emerging technologies for 6G-IoT security and context awareness:** As research moves beyond 5G, 6G is expected to natively support intelligence, sensing, and global coverage, extending the capabilities of today's IoT-5G systems. Several disruptive technologies will shape secure, intelligent 6G-IoT architectures. Non-Terrestrial Networks (NTNs) enhance coverage and resilience, especially in remote or infrastructure-less areas [39]. Virtual MIMO (V-MIMO) enables energy-efficient, high-capacity communications for large-scale IoT. THz sensing offers unprecedented resolution and bandwidth for context-aware applications, supporting adaptive security. Generative AI is emerging for proactive threat hunting, creating synthetic attack scenarios and improving predictive defense. Finally, explainable AI (XAI) [40] enhances transparency and trust in ML-based security decisions, crucial for sensitive domains such as healthcare and autonomous systems.

The integration of AI/ML, Zero Trust Architectures, Blockchain/DLTs, and Post-Quantum Cryptography into the IoT-CCN-5G ecosystem marks a pivotal shift toward building resilient, intelligent, and secure communication infrastructures. These emerging trends tackle pressing issues such as distributed trust, data privacy, and post-quantum threats, while also enabling scalable, autonomous, and future-ready network architectures.

VI. Conclusion

While the integration of the IoT, 5G, and CCN unlocks innovative applications, it also brings complex security challenges. In this paper, we examined the key security requirements for content-centric, 5G-based IoT systems and analyzed existing solutions. We conclude that more research efforts should be made toward comprehensive solutions. Future work will focus on developing intelligent, context-aware security mechanisms for 5G-based, content-centric IoT systems.

References

[1] A. M. Rahmani, S. Bayramov, and B. Kiani Kalejahi, "Internet of Things Applications: Opportunities and Threats," *Wireless Personal Communications*, vol. 122, no. 1, pp. 451–476, Jan. 2022.

[2] S. Wijethilaka and M. Liyanage, "Survey on Network Slicing for Internet of Things Realization in 5G Networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 957–994, 2021.

[3] P. C.N., H. Vimala, and S. J., "A systematic survey on content caching in ICN and ICN-IoT: Challenges, approaches and strategies," *Computer Networks*, vol. 233, p. 109896, Sep. 2023.

[4] X. Chen and X. Wang, "Content-centric framework for Internet of Things," *Multimedia Tools and Applications*, vol. 81, no. 9, pp. 12 371–12 385, Apr. 2022.

[5] B. Nour, S. Mastorakis, R. Ullah, and N. Stergiou, "Information-Centric Networking in Wireless Environments: Security Risks and Challenges," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 121–127, Apr. 2021.

[6] D. Shur, G. Di Crescenzo, Q. Zhang, T. Chen, R. Krishnan, Y.-J. Lin, Z. Patni, S. Alexander, and G. Tsudik, "SEDIMENT: An IoT-device-centric Methodology for Scalable 5G Network Security," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2022, pp. 49–54.

[7] A. Anjum, P. Agbaje, A. Mitra, E. Oseghale, E. Nwafor, and H. Olufowobi, "Towards named data networking technology: Emerging applications, use cases, and challenges for secure data communication," *Future Generation Computer Systems*, vol. 151, pp. 12–31, Feb. 2024.

[8] M. A. Zormati and H. Lakhlef, "An Overview of Machine Learning-Enabled Network Softwarization for the Internet of Things," in *2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Sep. 2023, pp. 1–6.

[9] W. Mao, Z. Zhao, Z. Chang, G. Min, and W. Gao, "Energy-Efficient Industrial Internet of Things: Overview and Open Issues," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7225–7237, Nov. 2021.

[10] Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in Internet of Things: A survey," *SN Applied Sciences*, vol. 3, no. 1, p. 121, Jan. 2021.

[11] Q. V. Khanh, N. V. Hoai, L. D. Manh, A. N. Le, and G. Jeon, "Wireless Communication Technologies for IoT in 5G: Vision, Applications, and Challenges," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 3229294, 2022.

[12] O. O. Erunkulu, A. M. Zungeru, C. K. Lebekwe, M. Mosalaosi, and J. M. Chuma, "5G Mobile Communication Applications: A Survey and Comparison of Use Cases," *IEEE Access*, vol. 9, pp. 97 251–97 295, 2021.

[13] Z. Zhang, C.-H. Lung, X. Wei, M. Chen, S. Chatterjee, and Z. Zhang, "In-Network Caching for ICN-Based IoT (ICN-IoT): A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14 595–14 620, Aug. 2023.

[14] G. Jaber and R. Kacimi, "A collaborative caching strategy for content-centric enabled wireless sensor networks," *Computer Communications*, vol. 159, pp. 60–70, Jun. 2020.

[15] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. Briggs, and R. L. Braynard, "Networking Named Content," in *Proceedings of the 5th international conference on Emerging networking experiments and technologies (CoNEXT '09)*. ACM, 2009, pp. 1–12.

[16] G. Jaber, R. Kacimi, L. Alfredo Grieco, and T. Gayraud, "An adaptive duty-cycle mechanism for energy efficient wireless sensor networks, based on information centric networking design," *Wireless Networks*, vol. 26, no. 2, pp. 791–805, Feb. 2020.

[17] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77–89, Apr. 2022.

[18] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, S. B. Taher, M. Kabir, S. M. Muyeen, and A. H. Gandomi, "Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities," *IEEE Access*, vol. 12, pp. 13 125–13 145, 2024.

[19] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G Security Challenges and Solutions: A Review by OSI Layers," *IEEE Access*, vol. 9, pp. 116 294–116 314, 2021.

[20] S. S. Ullah, I. Ullah, H. Khattak, M. A. Khan, M. Adnan, S. Hussain, N. U. Amin, and M. A. K. Khattak, "A Lightweight Identity-Based Signature Scheme for Mitigation of Content Poisoning Attack in Named Data Networking With Internet of Things," *IEEE Access*, vol. 8, pp. 98 910–98 928, 2020.

[21] S. Li, M. Iqbal, and N. Saxena, "Future Industry Internet of Things with Zero-trust Security," *Information Systems Frontiers*, vol. 26, no. 5, pp. 1653–1666, Oct. 2024.

[22] A. Afaq, N. Haider, M. Z. Baig, K. S. Khan, M. Imran, and I. Razzak, "Machine learning for 5G security: Architecture, recent advances, and challenges," *Ad Hoc Networks*, vol. 123, p. 102667, Dec. 2021.

[23] P. Ranaweera, A. Jurcut, and M. Liyanage, "MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures," *ACM Computing Surveys*, vol. 54, no. 9, pp. 1–37, Dec. 2022.

[24] S. Hussain, S. S. Ullah, A. Gumaei, M. Al-Rakhami, I. Ahmad, and S. M. Arif, "A Novel Efficient Certificateless Signature Scheme for the Prevention of Content Poisoning Attack in Named Data Networking-Based Internet of Things," *IEEE Access*, vol. 9, pp. 40 198–40 215, 2021.

[25] V. P. Singh and R. L. Ujjwal, "NDN Content Poisoning Attack Mitigation Using Fuzzy-Reputation Based Trust," in *Innovations in Cyber Physical Systems*, J. Singh, S. Kumar, and U. Choudhury, Eds. Singapore: Springer, 2021, pp. 325–336.

[26] K. Srikanth, P. G. Rajesh, N. D. Prasad, M. Asmathulla, and T. P. K. Reddy, "Proxy-Based Re-Encryption Design for the IoT Ecosystem," in *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, May 2023, pp. 1–6.

[27] F. Mecerhed, Y. Imine, A. Gallais, S. Fischer, and M. A. Hail, "An Efficient Decentralized Fine-grained Access Control for IoT Ecosystems over NDN," in *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Sep. 2024, pp. 1–6.

[28] C. Wang, X. Deng, M. Ma, Q. Li, H. Bai, and Y. Zhang, "An anonymous and efficient certificateless signature scheme based on blockchain in NDN-IoT environments," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, p. e4979, 2024.

[29] K. K. Saha, S. Ray, and M. Dasgupta, "ECMHP: ECC-Based Secure Handshake Protocol for Multicasting in CCN-IoT Environment," *IEEE Transactions on Network and Service Management*, vol. 21, no. 5, pp. 5826–5842, Oct. 2024.

[30] M. A. Shaaban, A. S. Alsharkawy, M. T. AbouKreisha, and M. A. Razek, "Efficient ECC-based authentication scheme for fog-based IoT environment," *International journal of Computer Networks & Communications*, vol. 15, no. 04, pp. 55–71, Jul. 2023.

[31] K. Patel, A. Vadher, M. Patel, J. Thaker, and A. Bhise, "AI-Based Security System for 5G Enabled IoT," in *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, Feb. 2024, pp. 1–7.

[32] R. Bukhowah, A. Aljughaiman, and M. M. H. Rahman, "Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions," *Electronics*, vol. 13, no. 6, p. 1031, Jan. 2024.

[33] V. Rey, P. M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet, "Federated learning for malware detection in IoT devices," *Computer Networks*, vol. 204, p. 108693, Feb. 2022.

[34] M. A. Aleisa, "Blockchain-enabled zero trust architecture for privacy-preserving cybersecurity in iot environments," *IEEE Access*, 2025.

[35] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Computer Networks*, vol. 217, p. 109358, Nov. 2022.

[36] M. Usman, M. S. Sarfraz, M. U. Aftab, U. Habib, and S. Javed, "A Blockchain Based Scalable Domain Access Control Framework for Industrial Internet of Things," *IEEE Access*, vol. 12, pp. 56 554–56 570, 2024.

[37] A. K. Sharma, M. S. Peelam, B. K. Chauasia, and V. Chamola, "Qiotchain: quantum iot-blockchain fusion for advanced data protection in industry 4.0," *IET Blockchain*, vol. 4, no. 3, pp. 252–262, 2024.

[38] A. Sharma and S. Rani, "Post-Quantum Cryptography (PQC) for IoT-Consumer Electronics Devices integrated With Deep Learning," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2025.

[39] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6g era: Challenges and opportunities," *IEEE network*, vol. 35, no. 2, pp. 244–251, 2020.

[40] A. B. Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins *et al.*, "Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai," *Information fusion*, vol. 58, pp. 82–115, 2020.