SRI RAMACHANDRA
INSTITUTE OF HIGHER EDUCATION AND RESEARCH
(Category - I Deemed to be University) Porur, Chennai
SRI RAMACHANDRA FACULTY OF ENGINEERING AND TECHNOLOGY

SECURITY AND PRIVACY IN IOT-INTEGRATED WIRELESS NETWORKS: A SYSTEMATIC LITERATURE REVIEW FROM 5G TO 6G

CSE390 – WIRELESS NETWORKS

CA-4 LITERATURE REVIEW PAPER

Submitted by

HEMAA S – E0222038

YUGESH PADMANABAN V – E0222008

In partial fulfilment for the award of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

(Cyber Security & Internet of Things)

Sri Ramachandra Faculty of Engineering and Technology

Sri Ramachandra Institute of Higher Education and Research, Porur, Chennai -600116

APRIL, 2025

ABSTRACT

The advent of sixth-generation (6G) wireless communication technology is poised to revolutionize the Internet of Things (IoT) ecosystem by delivering ultra-fast data speeds, near-zero latency, and unparalleled connectivity among billions of interconnected devices. As 6G becomes deeply embedded within critical infrastructure, industrial systems, and consumer technologies, it brings not only transformative opportunities but also significant challenges in the areas of security and digital forensics.

This review paper presents a comprehensive examination of the emerging threats, vulnerabilities, and forensic complexities associated with 6G-enabled IoT environments. The integration of advanced technologies such as Artificial Intelligence (AI), edge computing, and massive device heterogeneity within 6G networks significantly complicates traditional approaches to securing systems and investigating cyber incidents. These systems continuously generate enormous volumes of real-time data, thereby increasing the difficulty of detecting anomalies, preserving digital evidence, and tracing malicious activity.

The paper explores the foundational technologies underpinning 6G, their anticipated applications within smart environments, and the implications for digital forensics. It critically evaluates the limitations of conventional forensic methods in addressing the distributed, autonomous, and intelligent nature of next-generation IoT infrastructures. Furthermore, the review highlights current trends and gaps in research, emphasizing the urgent need for scalable and proactive forensic frameworks that can operate effectively in large-scale, heterogeneous 6G IoT networks.

To address these challenges, the paper proposes key future directions, including the development of adaptive forensic readiness models, enhanced privacy-preserving mechanisms, and collaborative security architectures involving industry stakeholders, government agencies, and standardization bodies. By advancing forensic capabilities and security strategies aligned with the complexities of 6G-enabled IoT, this review aims to foster a resilient, secure, and trustworthy digital ecosystem.

1. INTRODUCTION

Security and Digital Forensics in 6G-Enabled IoT Networks: Challenges, Risks, and Future Directions

The evolution of wireless communication technologies has been nothing short of revolutionary. From the advent of 1G analog systems to the current deployment of 5G networks, each generation has contributed to redefining how individuals, businesses, and machines connect and interact. As we approach the era of sixth-generation (6G) wireless networks, this trajectory is expected to continue its rapid ascent, delivering transformative advancements in network performance, capability, and ubiquity. Among the most anticipated outcomes of 6G is its profound impact on the Internet of Things (IoT)—a technological paradigm envisioning seamless connectivity among billions of smart devices, sensors, and systems across every facet of life and industry.

6G is expected to introduce unprecedented improvements in data transmission speeds, latency reduction, and network capacity. With theoretical data rates potentially reaching up to 1 Tbps and latency reduced to microseconds, 6G will significantly outperform 5G in terms of raw performance. More importantly, it will bring transformative functionalities such as integrated AI, intelligent surfaces, terahertz (THz) frequency communications, and even quantum communication protocols. These advancements are highly relevant for the IoT domain, which requires robust, reliable, and scalable communication infrastructure to support large-scale smart systems in areas such as healthcare, transportation, manufacturing, agriculture, and urban infrastructure.

The synergy between 6G and IoT holds the potential to revolutionize interconnected ecosystems. Enhanced by ultra-low latency and real-time data processing, IoT applications under 6G will be capable of supporting complex use cases such as fully autonomous vehicles, intelligent transportation networks, advanced industrial automation, telemedicine, and immersive augmented/virtual reality environments. For instance, real-time sensing and cooperative communication in smart factories will enable predictive maintenance, optimized workflows, and energy-efficient operations. Similarly, smart cities will benefit from intelligent infrastructure capable of responding dynamically to changing environmental conditions, traffic patterns, and public safety needs.

While the integration of 6G with IoT paves the way for groundbreaking innovations, it also introduces a myriad of new complexities—particularly in the areas of security, privacy, and digital forensics. Unlike previous generations, 6G-enabled IoT environments are expected to be more heterogeneous and decentralized, involving a diverse array of edge devices, cloud services, AI-driven analytics, and user interfaces. This expanded attack surface increases the

likelihood of vulnerabilities being exploited by malicious actors, especially when security protocols struggle to keep pace with the rapid deployment of new technologies and services.

One of the core challenges in securing 6G IoT networks lies in the very nature of IoT devices, which often lack sufficient computational and energy resources to implement advanced cryptographic algorithms or security features. When such devices are deployed at scale in critical environments—such as healthcare systems, power grids, or transportation infrastructure—the risk posed by vulnerabilities becomes even more alarming. Moreover, the integration of AI and machine learning algorithms for decision-making and automation introduces additional attack vectors, including data poisoning, adversarial attacks, and model theft.

Beyond proactive security measures, the domain of digital forensics is of paramount importance in 6G IoT systems. Digital forensics involves the identification, preservation, analysis, and presentation of digital evidence following a security breach or criminal activity. In 6G networks, this process becomes increasingly complex due to the distributed architecture, real-time communication, and dynamic behaviour of IoT devices. Conventional forensic techniques, which rely on static data collection from centralized servers or storage devices, may prove inadequate in these next-generation environments.

For example, collecting forensic evidence from a decentralized 6G-enabled smart grid—where devices interact autonomously, often across multiple jurisdictions—requires new methodologies for data acquisition and integrity verification. Furthermore, time-sensitive forensics becomes essential in scenarios where immediate response is critical to prevent cascading failures or further attacks. The ability to trace, attribute, and respond to threats in real time will necessitate advancements in forensic readiness—preparing systems and protocols in advance for potential investigations.

This review paper seeks to present a comprehensive analysis of the security and digital forensic challenges associated with the integration of 6G in IoT networks. The objectives are multifaceted and aim to cover technical, procedural, and strategic aspects of securing and investigating 6G IoT systems:

First, the paper outlines the promising smart IoT environments that will be supported by 6G wireless technology, focusing on key sectors and emerging applications.

Second, it identifies the core challenges in digital forensics posed by the nature of 6G IoT environments. These include investigation complexities such as device volatility, data sovereignty, evidence correlation across heterogeneous platforms, and chain-of-custody maintenance.

Third, it highlights innovative approaches and methodologies for enhancing forensic readiness in these environments. This includes the development of distributed forensic agents, edge-level forensic data collection, blockchain-based evidence integrity verification, and AI-enhanced threat detection and response systems.

Fourth, the review delves into existing and emerging security vulnerabilities within the evolving 6G protocols. While 6G inherits some risks from 5G—such as supply chain threats, DDoS attacks, and rogue base stations—it also introduces new ones due to its increased reliance on software-defined networking, open-source components, and multi-access edge computing.

Fifth, the paper discusses potential mitigation strategies and the essential roles that industry stakeholders, government regulators, and standardization bodies must play. Effective security policies, robust authentication mechanisms, regulatory compliance frameworks, and collaborative threat intelligence sharing are all vital components of a secure and resilient 6G IoT ecosystem.

In line with these objectives, the review addresses the following central research questions:

I. What are the key security vulnerabilities and threats introduced or amplified by 6G integration in IoT ecosystems?
This includes threats stemming from the increased attack surface, AI integration, and terahertz communication, as well as challenges in securing real-time, mission-critical systems.

II. What specific challenges do 6G IoT networks pose to conventional digital forensic methods?
Traditional forensic practices may falter due to ephemeral data, device mobility, and encryption, necessitating a shift to adaptive, distributed forensic techniques.

III. What are the current trends and innovative approaches aimed at improving forensic readiness for 6G IoT?
Trends include the use of blockchain for immutable evidence storage, AI for pattern recognition, and the development of proactive logging and auditing mechanisms.

IV. Where do current research efforts fall short in terms of security and forensics in the 6G context?
Many current studies focus on theoretical frameworks without practical deployment scenarios. There's a lack of standardized protocols for forensic data sharing and insufficient cross-disciplinary collaboration.

V. What future research directions show the most promise in addressing the unique challenges of 6G-enabled IoT networks?
Promising areas include AI-driven autonomous forensic agents, cross-layer security models, context-aware access control, and privacy-preserving forensics that balance investigative needs with user rights.

To summarize, the integration of 6G with IoT represents a leap forward in wireless communication, with the potential to revolutionize industries and reshape digital experiences. However, the expanded capabilities and complexity also demand a renewed focus on robust security and adaptable forensic methodologies. Addressing these challenges requires coordinated efforts across research, industry, and policy-making communities to ensure that 6G-enabled IoT systems are not only innovative but also secure, trustworthy, and accountable.

2. RESEARCH METHODOLOGY

This review adopts a systematic and structured methodology to analyse and synthesize the existing literature concerning security and privacy in IoT-integrated wireless networks, with a particular focus on the transition from 5G to 6G technologies. Rather than generating or analysing new datasets, this methodology emphasizes the extraction, evaluation, and interpretation of information from selected scholarly publications that examine the intersection of 6G wireless communication, Internet of Things (IoT) infrastructures, and cybersecurity challenges.

The primary sources selected for this review include three key research contributions that collectively provide comprehensive insights into the technological evolution, security concerns, and forensic preparedness relevant to 6G-enabled IoT ecosystems. These sources were chosen due to their direct relevance, depth of analysis, and focus on critical issues such as distributed denial-of-service (DDoS) mitigation, emerging privacy standards, and digital forensic methodologies. The selected studies are:

- A research paper discussing the development of distributed DDoS mitigation techniques in IoT and 5G networks, offering insight into the transition toward more distributed and intelligent network defense mechanisms.
- A survey that maps the progression from 5G to 6G technologies, emphasizing evolving risks, emerging security paradigms, and the role of privacy, policy, and standardization in shaping future communication networks.
- A focused review on the challenges of forensic readiness in 6G-enabled IoT environments, exploring enabling technologies, investigative limitations, and the need for future research in digital forensics.

To ensure a thorough and coherent analysis, the methodology for this review was structured into six distinct phases:

2.1. Careful Reading and Initial Assessment

Each selected publication was meticulously reviewed to grasp its primary objectives, thematic contributions, and relevance to the overall research questions. This phase ensured a comprehensive understanding of each source's scope and helped identify the depth of information provided regarding 6G technologies, IoT integration, security threats, and forensic implications.

2.2. Thematic Identification

Following the initial assessment, key themes were identified across the literature. These included, but were not limited to:

- The evolution of security challenges with the advent of 6G and its convergence with IoT.
- The increasing complexity brought by AI, edge computing, and massive device heterogeneity.
- Digital forensic limitations in large-scale, distributed, and intelligent environments.

- The necessity for standardized forensic processes and proactive evidence collection frameworks.

These themes served as the foundation for organizing the subsequent sections of the paper.

2.3. Information Extraction and Organization

Information relevant to each theme was systematically extracted from the selected literature. Key data points, findings, arguments, and frameworks were recorded and organized in a structured format, ensuring that both general trends and specific case examples were captured. The organization of this data facilitated easier comparison across sources and contributed to a more robust synthesis of insights.

2.4. Cross-Source Synthesis and Comparison

The extracted data was then compared across sources to highlight areas of agreement, divergence, and uniqueness. This cross-source synthesis enabled the identification of dominant viewpoints, emerging perspectives, and research gaps. For example, while all sources acknowledged the complexity introduced by AI and edge computing in 6G networks, they differed in the specific mitigation strategies and forensic solutions proposed. This comparative analysis was critical in forming a well-rounded understanding of the current research landscape.

2.5. Structured Review Development

Based on the themes and synthesized findings, the structure of the review was developed. The paper was organized to provide a logical flow from the background of 6G and IoT integration, through the identification of security and forensic challenges, to the exploration of mitigation strategies and future research directions. Each section of the paper builds upon the previous, creating a cohesive narrative that guides the reader through the complex intersection of 6G technologies and IoT systems.

2.6. Iterative Refinement

The content and structure of the review were refined through multiple iterations to ensure consistency, accuracy, and clarity. Each draft was revisited to enhance coherence, ensure alignment with research objectives, and maintain a professional academic tone. This iterative approach helped eliminate redundancy, sharpen the analytical focus, and strengthen the overall presentation of findings.

The analytical approach employed throughout the review is qualitative in nature. It emphasizes identifying patterns, trends, and knowledge gaps in the existing literature rather than quantitatively assessing empirical data. This method is particularly well-suited to a field like 6G IoT security and forensics, which is still in its early stages and marked by rapid technological evolution and evolving research priorities.

By employing this structured methodology, the review ensures a comprehensive and balanced analysis of the current state of knowledge. It also supports the formulation of well-grounded conclusions and actionable recommendations for future research, policy-making, and technological development in the domain of 6G-enabled IoT networks.

3. LITERATURE REVIEW

3.1. The Convergence of Next-Generation Networks and IoT

The advent of 5G and the ongoing development of 6G technologies mark a significant evolution in wireless communication, promising enhanced data rates, reduced latency, and massive connectivity [1]. These advancements are particularly crucial for the proliferation of IoT devices and applications, which are becoming increasingly integrated into various aspects of our lives, from smart cities and industrial automation to healthcare and autonomous systems [1]. However, this convergence also introduces new and complex security and privacy challenges that require thorough investigation and innovative solutions [8]. Understanding the current state of research in this domain is essential for developing robust and resilient next-generation networks and IoT ecosystems.

3.2. Security Challenges and Solutions in 5G/6G and IoT

Several sources delve into the security challenges and propose various solutions for 5G, 6G, and IoT networks. One article [16] presents an analysis of existing contributions to represent the state-of-the-art in securing IoT networks. It establishes key characteristics and compares different approaches, highlighting its own contribution towards a distributed dual-layer self-protection closed cognitive loop for IoT networks against DDoS attacks [17].

3.3. Frameworks for Attack Detection and Mitigation:

Several works propose frameworks for detecting and mitigating malicious activities in these networks. One study [18] presents a framework for detecting malicious network traffic at the IoT-Edge layer to identify potential threats. Similarly, [19] present related work focusing on attack detection and subsequent analysis for mitigation. Specifically, [19] introduces IoT Botnet Detection and Analysis (IoT-BDA), a framework for detecting, analysing, identifying, and reporting botnets circulating on the Internet. This framework comprises a Botnet Capturing Block (BCB) using honeypots to report suspicious activities and a Botnet Analysis Block (BAB) with tools to analyse the captured traffic and identify botnets [21]. On the other hand, [20] focuses on the firmware of IoT devices, utilizing Deep Learning (DL) techniques with the Long Short-Term Memory (LSTM) algorithm to detect attacks and mitigate them by analysing and disabling infected devices [21]. However, [21] notes that these contributions do not fully address the mitigation of attacks in the overlay networks available in the 5G system.

Another set of works [19, 21–23] focuses on achieving accurate attack detection in simulated 5G environments, allowing for potential deployment on Network Operators' infrastructure [17]. One such framework [22] is capable of detecting Silent Call Attacks and SMS Flooding Attack DDoS attacks in the communications infrastructure for 4G LTE-A architecture. This detection is performed by a DL Convolutional Neural Network analysing

pre-processed traffic in the CORE of the network using the ResNet-50 model [23]. To train this model, an open dataset from Telecom India is used [23]. Another framework, REPEL [10], focuses on detecting signaling DDoS attacks for 5G environments with an emphasis on prevention through scaling virtualized network services. However, it does not detail the architecture of its Intrusion Detection System (IDS), concentrating instead on load balancing and attacker obfuscation [23]. Umbrella [24] presents a defence mechanism against DDoS attacks deployed at the ISP level, claiming to stop various DDoS attacks through multiple layers of work, but it relies on continuous feedback from the victim for a list of trusted Ips [23]. Finally, [11] proposes an IDS based on Machine Learning (ML) techniques in 5G Software Defined Networks (SDN), with a three-layer architecture: forwarding, management and control, and data and intelligence, where ML algorithms analyse anomalous traffic [23]

One study [26] presents a framework for DDoS threat detection in IoT networks by analysing the performance of six different classifiers, concluding that their ADE-based Denial-of-Service (DoS) attack detection scheme shows good performance in simulated experiments [23]. However,[23] points out that this work used simulations rather than a real-world test environment, which is a key difference from the contribution mentioned earlier [23].

3.4. Network Slicing and Mitigation Strategies:

The use of network slicing for security is explored in [27], where a framework for detecting susceptible IoT devices in 4G and 5G networks is presented [25]. The mitigation strategy involves placing the traffic of these devices in quarantine on a dedicated Network Slice (NS) for in-depth analysis to classify malicious attacks [28]. This detection is performed by an application on top of the SDN controller, generating a distrust threshold based on the number of flows in the quarantine NS [28]. However, [28] notes that this approach lacks mitigation capabilities in the DSP, being limited to the ISP level, contrasting with a contribution that aims for collaboration among all stakeholders for infrastructure protection [28]. Palo alto Networks [29] also provides insights into 5G Network Slice Security [23].

3.5. Self-Managed Protection Architecture:

One paper [31] introduces a self-managed protection architecture for IoT networks in the context of 5G multi-tenant networks. This system proposes a self-protection control loop with software components such as Security Monitoring Agent (SMA), Analyser, Decision Maker, Planner, Orchestrator, and Flow Control Agent (FCA) [31].

3.6. Security in 5G and Beyond:

A comprehensive survey [15] on security for 5G and beyond discusses various aspects, including the evolution of mobile network security from 2G to 5G, key security enhancements in 5G, potential threats and vulnerabilities, and security considerations for emerging technologies like IoT, cloud computing, and Software-Defined Networking (SDN) [1]. The survey highlights the importance of addressing security challenges proactively as networks evolve [15]. It references numerous [3] GPP specifications and technical reports related to 5G security architecture [32].

3.7. Security Challenges in Heterogeneous 5G Networks:

The security challenges in 5G Heterogeneous Networks (HetNet) are discussed in [22], highlighting potential vulnerabilities arising from the integration of different network layers and technologies [22].

3.8. Quantum Networking and Security:

The security implications of quantum networking for 5G/6G are explored in [8]. These keywords point towards discussions on Quantum Key Distribution (QKD) and related protocols like BB8 [4] and Cascade, as well as the impact of factors like dephasing on quantum communication security. Quantum-safe communications are also mentioned as a promising mitigation technique for 6G networks in [11].

3.9. Privacy Concerns in 5G/6G and IoT

Privacy is a significant concern in the interconnected landscape of 5G/6G and IoT. One paper [38] addresses the privacy challenges associated with V2X communication in the cloud by introducing a security evaluation methodology that considers both historical data analysis using AI and real-time vehicle interactions [38]. This Privacy Assessment method with Uncertainty consideration (PAU) aims to enhance the precision of security assessment [38]. The research validates the approach's effectiveness against malicious behaviour and slander-based attacks using historical internet data [38].

3.10. Privacy-Preserving Techniques:

To address privacy limitations in current research, [40] introduces DPSmartCity, an SDN-based technology designed to protect user confidentiality and provide network administrators with more flexibility in smart city IoT deployments [40]. The DPSmartCity framework comprises two main components focused on ensuring the security of individuals' personal information within the IoT infrastructure [40]. Techniques like data fusion and edge computing are also highlighted in [1] as components for real-time data optimization, which can have implications for privacy by processing data closer to the source. Differential privacy is mentioned in [11] as an innovative data protection method for future 6G security enhancements.

3.11. Privacy in Vehicular Networks:

The privacy challenges in 5G-supported vehicular networks are specifically addressed in [41] (cited in [42]), indicating a focus on privacy-preserving techniques and considerations in this domain.

3.12. Spectrum Sharing and Privacy:

One source with the title "A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond)" [12] directly addresses the intersection of spectrum sharing, IoT devices, security, and privacy. While the excerpt itself provides only keywords and publication details, the title suggests a comprehensive exploration of these intertwined issues, likely discussing how spectrum sharing in next-generation networks impacts the privacy and security of IoT devices.

3.13. Forensic Challenges in 6G IoT Networks

The article "Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks" [13] provides a broad overview of the digital forensic challenges related to 6G IoT networks [14]. It discusses the key enabling technologies for 6G and outlines the promising smart IoT network environments that 6G will support, which necessitate a different approach to digital forensic investigations [14].

3.14. Key Forensic Challenges:

The study identifies and presents the digital forensics issues and challenges in key areas of 6G IoT networks, with a detailed discussion on specific investigation challenges [14]. It emphasizes forensic readiness and future research directions aimed at conducting digital forensic investigations in large-scale heterogeneous 6G-enabled IoT networks14 .... The methodology involved a systematic survey of literature related to 6G and IoT from databases like IEEE Explore, Google Scholar, and ScienceDirect, focusing on publications from January 2020 to April 202343 .... The search yielded 157 articles initially, which were filtered based on relevance to 6G, IoT, and digital forensics, resulting in 109 qualified articles [44]. The results indicate that research in this area is growing rapidly, with IEEE Explore being a major source of publications [45]. The themes covered in the selected articles include concepts and opportunities, key enabling technologies, applications of 6G, and associated challenges [45].

3.15. Convergence of Communication, Sensing, and AI in 6G

The integration of communication, sensing, and artificial intelligence is a defining characteristic of 6G networks. One paper46 provides an overview of technologies, opportunities, and challenges related to convergent communication, sensing, and localization in 6G systems, highlighting its potential for enhancing IoT applications1 .... The use of AI and machine learning in 6G is discussed in several sources1 .... AI is envisioned to play a crucial role in various aspects of 6G networks, including security, network management, resource allocation, and the support of advanced applications. For instance,31 proposes a self-protection architecture leveraging AI-driven analysis and decision-making. Machine learning techniques are explored for intrusion detection [11], routing [42], and enhancing ultra-reliable and low-latency services (URLLC) in 6G [40]. The interplay between Generative AI and 5G-Advanced towards 6G is also highlighted [47], suggesting a future where AI and network technologies are deeply intertwined.

3.16. Comparisons with Existing Surveys and Related Work

The research presented in16 includes a table (Table 2) summarizing the contributions that have been analysed to represent the state-of-the-art. Key relevant characteristics are established and compared to give an overview of the main contributions of different works, including the authors' own. Table 1 (mentioned in [16]) provides explanations for the column names in Table 2 to facilitate a better understanding of the carried-out analysis.

The survey on digital forensics in 6G IoT13 also includes a section on related works [43], although the provided excerpts do not detail these comparisons. However, the methodology section43 indicates that the authors placed their work within the context of existing literature to highlight its unique contributions.

Another survey [11] (Table 2) compares itself with existing relevant surveys in the domain of 6G security and privacy, providing insights into how its focus and contributions differ from

those of Nguyen et al.6 and Porambage et al. (both cited in [11]). These existing surveys are described as conducting comprehensive analyses of security and privacy issues in 6G networks, focusing on new threats and promising mitigation techniques like physical layer protection, deep network slicing, quantum-safe communications, and AI-driven security [11]. They also explore the need for dynamic real-time security and innovative data protection methods [11]. The comparison likely highlights the specific niche and advancements offered by [11] in this evolving field.

4. CHALLENGES AND OPEN ISSUES

The evolution from current wireless networks to 6G-enabled IoT systems introduces transformative benefits in terms of connectivity, speed, and real-time responsiveness. However, this shift also brings significant and multi-dimensional challenges, especially in the areas of cybersecurity and digital forensics. These challenges span technical, research-based, and implementation-related domains and must be addressed to ensure the security, integrity, and investigability of future 6G IoT environments. This section categorizes and discusses the key open issues and barriers under three major dimensions: technical challenges, research gaps, and practical implementation barriers.

4.1. Technical Challenges

4.1.1. Increased Complexity and Heterogeneity

6G IoT environments will comprise a massive number of devices with diverse capabilities, communication protocols, and deployment contexts. The heterogeneity spans from low-powered sensor nodes and edge devices to autonomous vehicles and industrial machines. Managing security policies and conducting digital forensic investigations in such a fragmented and dynamically evolving ecosystem presents a significant challenge. Traditional security tools and centralized forensic methods may not scale or adapt efficiently to these highly diverse environments, necessitating the development of new, flexible frameworks capable of addressing device-specific characteristics and contextual nuances.

4.1.2. Real-Time and Low-Latency Requirements

One of the defining features of 6G networks is the support for ultra-low latency and high-speed data transmission. This capability enables time-critical applications such as remote surgery, autonomous navigation, and industrial automation. However, it also limits the applicability of conventional forensic and security approaches that introduce latency or overhead. Real-time monitoring, logging, and evidence collection must be seamlessly integrated into communication flows without degrading system performance. Designing forensic mechanisms that meet these real-time requirements remains a major technical hurdle.

4.1.3. Integration of Advanced Technologies

6G is expected to integrate advanced technologies such as artificial intelligence (AI), machine learning (ML), and possibly quantum communication. While these innovations offer enhanced functionality and intelligent automation, they also expand the attack surface and introduce novel vulnerabilities. For example, adversarial attacks against AI models can mislead automated security systems. Quantum communication, while secure by design, may require

new cryptographic schemes and corresponding forensic capabilities. Understanding, detecting, and investigating threats emerging from these cutting-edge technologies will require specialized expertise and new toolsets.

4.1.4. Edge Computing Environments

Edge computing plays a central role in 6G architectures by relocating data processing closer to end-user devices. This decentralization improves performance and reduces latency but complicates centralized security management and forensic traceability. In edge environments, data may reside temporarily on devices or edge nodes, creating challenges in evidence acquisition, chain of custody, and data integrity. The absence of a central authority necessitates distributed forensic frameworks that ensure synchronized data logging, anomaly detection, and secure evidence storage across multiple nodes.

4.1.5. Data Overload and Real-Time Analysis

With billions of connected devices operating at high data rates, 6G IoT systems will generate massive volumes of structured and unstructured data. This explosion of data presents significant difficulties for forensic investigators, who must identify relevant information, detect anomalies, and trace attack sources from within this deluge. Traditional forensic tools may struggle with the speed, scale, and diversity of 6G data streams. Future solutions must incorporate real-time filtering, AI-powered analysis, and scalable architectures capable of sifting through large datasets with minimal delay.

4.1.6. Evolving Attack Vectors

As 6G introduces new protocols, frequency bands (such as terahertz), and intelligent networking features, it also opens up avenues for sophisticated cyber threats. New vulnerabilities may emerge at the physical and media access control (MAC) layers, particularly in environments where 5G, 6G, and Wi-Fi coexist. Attackers may exploit protocol mismatches, misconfigured interfaces, or unprotected legacy systems. Forensic systems must be continuously updated to detect and interpret these emerging threats, requiring adaptive and predictive threat intelligence models.

4.2. Gaps in Existing Research

4.2.1. Lack of Specific Forensic Methodologies

Despite growing interest in 6G and IoT integration, there is a notable deficiency in research focused specifically on digital forensics for 6G-enabled environments. Current frameworks are either generic or tailored to older technologies and lack provisions for features unique to 6G, such as distributed AI or massive MIMO systems. There is an urgent need to establish forensic processes that reflect the architectural, temporal, and operational nuances of 6G IoT systems.

4.2.2. Inadequate Forensic Tooling and Techniques

Existing digital forensic tools are ill-equipped to handle the complexity, speed, and distribution of 6G IoT networks. Tools must evolve to support cross-platform compatibility, high-speed data analysis, edge-node integration, and decentralized evidence collection. Additionally, new interfaces are needed to interact with AI models, quantum encryption modules, and other emerging technologies. The development of device-aware and context-sensitive forensic tools remains a largely unexplored area.

4.2.3. Absence of Standardized Forensic Processes

There is currently a lack of standardization in digital forensic procedures for 6G networks, which hinders the reproducibility, interoperability, and legal validity of forensic findings. Without uniform protocols for evidence identification, preservation, and analysis, investigations may vary significantly across regions and sectors. Establishing global standards—similar to those in telecommunications and cryptography—requires collaboration among academia, industry, and regulatory bodies.

4.2.4. Limited Understanding of Technological Impacts

The forensic implications of integrating AI, blockchain, reconfigurable intelligent surfaces, and quantum communication remain largely unexplored. While these technologies offer significant potential, their complexity also introduces unique challenges for forensic tracing and evidence validation. More interdisciplinary research is required to evaluate how such technologies affect the lifecycle of digital evidence and to design methods for effective incident investigation within these new paradigms.

4.3. Practical Implementation Barriers

4.3.1. Cost and Complexity of Deployment

Implementing robust security and forensic mechanisms across a vast and varied 6G IoT infrastructure presents economic and operational challenges. Many IoT devices are resource-constrained, and retrofitting them with advanced security capabilities can be cost-prohibitive. Organizations must balance the trade-offs between performance, security, and financial feasibility, especially in large-scale deployments.

4.3.2. Interoperability and Compatibility Issues

6G IoT environments will encompass devices from multiple vendors, operating on different platforms and network standards. Ensuring compatibility among forensic tools and communication interfaces is a complex task. Without standard APIs, data formats, and

compliance benchmarks, integrating forensic capabilities across heterogeneous systems can become fragmented and ineffective.

4.3.3. Privacy Concerns and Regulatory Constraints

Digital forensics often involves access to sensitive personal and corporate data. With increasing awareness of data privacy and regulatory enforcement (e.g., GDPR, CCPA), forensic activities must be conducted within strict legal and ethical boundaries. This includes ensuring data minimization, user consent, secure storage, and proper authorization for evidence handling.

4.3.4. Skills Gap and Training Requirements

The shift to 6G will demand a new generation of forensic investigators proficient in emerging technologies, AI-driven tools, and real-time threat analysis. However, there is currently a shortage of skilled professionals in this domain. Investment in training programs, certifications, and academic curricula is essential to build the human capacity required to manage security and forensic operations in 6G networks.

5. FUTURE RESEARCH DIRECTIONS

Addressing the challenges and unresolved issues associated with 6G-enabled IoT networks requires a forward-looking and interdisciplinary research approach. The fusion of next-generation wireless networks with a diverse and rapidly expanding IoT ecosystem necessitates innovative security strategies, reimagined digital forensic methodologies, and holistic forensic readiness frameworks. This section outlines key areas for future research to ensure the security, reliability, and investigability of 6G-integrated IoT systems.

5.1 Enhancing Security in 6G IoT

Security in 6G IoT must evolve beyond traditional defense models to meet the dynamic demands of distributed, intelligent, and high-speed environments. Future research should focus on developing multi-layered and proactive security architectures that are scalable, adaptable, and context-aware.

5.1.1. AI and Machine Learning for Proactive Security

Artificial intelligence (AI) and machine learning (ML) will be central to threat detection and response in 6G environments. Research should prioritize the development of models capable of detecting anomalies in real time and automating incident responses with minimal human intervention. Explainable AI (XAI) must also be a key area of focus, ensuring that the rationale behind security decisions is transparent, interpretable, and accountable.

5.1.2. Physical Layer Security Enhancements

The physical layer, particularly with the use of terahertz and millimeter-wave frequencies in 6G, introduces new vulnerabilities. Future studies should investigate advanced physical-layer protection mechanisms such as channel obfuscation, directional signal shielding, and physical-layer authentication schemes to guard against eavesdropping and signal interference.

5.1.3. Quantum-Safe Cryptography and Communication

As quantum computing threatens conventional cryptographic standards, it is imperative to design and deploy post-quantum cryptographic algorithms. These should be lightweight enough for IoT devices and adaptable to hybrid networks where classical and quantum systems may coexist. Research is also needed to explore the application of quantum key distribution (QKD) in large-scale 6G IoT environments.

5.1.4. Blockchain and Distributed Ledger Technologies

Blockchain and distributed ledger technologies (DLTs) offer a decentralized and tamper-resistant means of ensuring data integrity and access control. Future research should explore their application in identity management, secure communications, and trust management in IoT ecosystems. Challenges such as scalability, energy efficiency, and consensus algorithm optimization must be addressed for practical deployment.

5.1.5. Zero-Trust Security Architectures

The zero-trust model—"never trust, always verify"—is particularly suitable for the distributed and heterogeneous nature of 6G IoT. Research should focus on developing adaptive zero-trust frameworks that support continuous authentication, dynamic authorization, and policy enforcement at every network layer and device interaction point.

5.1.6. Lightweight and Efficient Security Mechanisms

Many IoT devices operate under resource constraints, making conventional security mechanisms unsuitable. Future security solutions must be designed to be lightweight yet robust, capable of protecting constrained devices without degrading their performance or draining power sources. This may involve cryptographic optimization, hardware-accelerated encryption, and intelligent resource allocation models.

5.2 Advancing Digital Forensics for 6G IoT

Digital forensics in 6G IoT environments will require a paradigm shift. Traditional forensic approaches are inadequate for the speed, scale, and distribution of data in 6G networks. Research must focus on rethinking forensic tools, techniques, and methodologies.

5.2.1. 6G-Specific Forensic Methodologies

There is a critical need to develop forensic models tailored to 6G IoT's architectural and operational characteristics. These methodologies should define standardized procedures for evidence collection, preservation, and analysis in distributed, dynamic, and AI-driven environments. Frameworks must also ensure legal admissibility and chain-of-custody compliance.

5.2.2. Scalable Forensic Analysis Frameworks

6G IoT will generate massive volumes of data across multiple sources. To handle this, research should develop scalable and modular forensic analysis frameworks capable of parallel processing, distributed analytics, and dynamic data filtering. These systems should also support forensic triage to prioritize high-risk events.

5.2.3. AI and ML for Automated Investigations

AI and ML can significantly streamline the forensic process by automating tasks such as log analysis, anomaly detection, malware classification, and behavior prediction. Future research should focus on developing intelligent forensic assistants capable of correlating events, identifying causality, and providing real-time forensic feedback to security systems.

5.2.4. Forensics in Edge Computing Environments

In 6G, a significant portion of computation and data processing will occur at the network edge. Forensic investigations must adapt by developing edge-specific techniques for evidence acquisition and analysis. Research should focus on secure logging, tamper-proof local storage, and federated forensic models that preserve privacy while enabling distributed investigations.

5.2.5. Cross-Layer Forensic Techniques

Investigating complex cyber incidents in 6G requires visibility across all network layers—from physical and link layers to the application and user interface. Future forensic tools must support multi-layered event correlation, integrating signals such as protocol behavior, system logs, and user activity for holistic incident reconstruction.

5.2.6. Investigation of Attacks on Emerging Technologies

As 6G incorporates advanced technologies like massive MIMO, reconfigurable intelligent surfaces (RIS), and terahertz communication, forensic research must also focus on understanding their vulnerabilities. Specialized techniques are needed to detect and investigate attacks that exploit these innovations, such as signal jamming, beam spoofing, or RIS manipulation.

5.3 Enhancing Forensic Readiness in 6G IoT

Forensic readiness ensures that digital investigations can be conducted efficiently and effectively, even in complex, large-scale, and fast-moving environments. Achieving readiness in 6G networks requires proactive planning, architecture-level integration, and regulatory compliance.

5.3.1. Proactive Evidence Preservation

Mechanisms should be embedded within network and device architectures to automatically capture and preserve critical forensic data during incidents. This includes tamper-proof logs, traffic snapshots, and system states, all maintained in compliance with privacy and legal standards.

5.3.2. Standardized Logging and Auditing

Consistency in audit trails is crucial for forensic reliability. Research should focus on defining standardized, tamper-evident logging frameworks that can operate across various devices and platforms. Timestamp accuracy, log integrity verification, and automated summarization are key areas of enhancement.

5.3.3. Integrated Security and Forensics Architectures

Security and forensic functions must not operate in isolation. Research should explore designs where forensic capabilities are embedded directly into security mechanisms, such as intrusion detection systems, access control modules, and threat response systems. This integration enables real-time incident detection, investigation, and response.

5.3.4. Guidelines and Best Practices for Readiness

The development of forensic readiness guidelines, checklists, and reference architectures can assist organizations in preparing their 6G infrastructure for investigations. These resources should address operational, technical, legal, and organizational aspects of readiness, providing actionable recommendations tailored to different deployment contexts.

5.3.5. Training and Education

With the rapid advancement of 6G and its associated technologies, a well-prepared forensic workforce is essential. Research institutions and industry leaders must collaborate to develop specialized training programs, certifications, and academic curricula that cover forensic readiness, AI and quantum forensics, and ethical hacking in 6G environments.

By focusing research efforts in these strategic directions, stakeholders across academia, industry, and government can build resilient and secure 6G-enabled IoT ecosystems. Future advancements in security, forensics, and readiness will be vital to maintaining trust and accountability in a world increasingly dependent on hyperconnected, intelligent infrastructure.

6. CONCLUSION

This review has comprehensively examined the emerging landscape of security and digital forensics within the context of 6G-enabled Internet of Things (IoT) networks. As the technological paradigm shifts toward 6G, the convergence of ultra-fast wireless communication with vast, heterogeneous IoT ecosystems introduces a wide array of transformative capabilities. However, these advancements are accompanied by significant challenges, particularly in the domains of security assurance and digital forensic readiness.

The findings of this review reveal that the increasing complexity and diversity of 6G IoT environments—driven by the integration of advanced technologies such as artificial intelligence (AI), edge computing, and quantum communication—amplify both the attack surface and the complexity of incident investigations. These developments undermine the effectiveness of traditional security models and forensic methodologies, which were largely designed for more centralized and less dynamic environments.

Security challenges in 6G IoT are particularly pronounced due to the real-time requirements of critical applications, the proliferation of resource-constrained devices, and the use of intelligent, autonomous systems. Many current surveys and studies emphasize the urgent need for innovative security frameworks that can offer dynamic, adaptive, and scalable protection mechanisms. Proposed solutions include AI-driven anomaly detection, quantum-safe cryptography, and blockchain-based identity and access control systems. The overarching goal is to develop security infrastructures that can evolve in tandem with the rapidly changing technological landscape of 6G.

From a digital forensics' perspective, the situation is equally pressing. The review identifies a clear gap in the availability of forensics methodologies and tools specifically designed for 6G IoT. The decentralized and data-intensive nature of 6G environments renders traditional forensic approaches inadequate. Effective investigation in such systems demands the development of scalable, multi-layered forensic frameworks that can operate across various architectural layers, from edge to core. AI-based tools for automated evidence collection and analysis, along with new techniques for conducting investigations in edge computing and AI-integrated environments, will be essential.

Moreover, this review underscores the critical importance of forensic readiness-defined as the proactive preparation for conducting digital investigations in complex technological environments. Forensic readiness in 6G IoT will require the integration of logging and auditing mechanisms into network infrastructure, the development of standardized procedures for evidence handling, and the establishment of legal and ethical frameworks for cross-platform investigations. Without such measures, it will be difficult to ensure accountability, legal compliance, and effective incident response in the face of advanced and distributed cyber threats.

The implications of these findings are far-reaching. For researchers, the gaps identified in the literature highlight numerous opportunities for innovation in both security and forensics. There is a strong need for interdisciplinary collaboration between experts in wireless communication, cybersecurity, AI, and digital forensics to create holistic solutions tailored to the unique

characteristics of 6G IoT systems. Research efforts must not only propose novel architectures and algorithms but also evaluate their feasibility, scalability, and compliance with real-world regulatory standards.

For practitioners-security engineers, forensic investigators, and system architects—the findings serve as a call to action. It is imperative to start adopting a proactive stance by integrating forensic readiness into system design, investing in new tools and technologies, and staying informed of evolving threats. Organizations must also prioritize workforce development, ensuring that professionals are equipped with the knowledge and skills to manage the challenges introduced by 6G IoT.

One notable limitation of this review is its reliance on a limited number of sources provided for analysis. While these sources were relevant and insightful, a more exhaustive literature review covering a wider array of academic publications, technical whitepapers, and industry reports would likely offer a broader and deeper understanding of the topic. Nevertheless, this review serves as a foundational contribution, outlining the core issues and charting a path for future inquiry and technological development.

In conclusion, securing the future of 6G-enabled IoT requires a multifaceted approach. This includes advancing the state of security technologies, developing specialized digital forensic capabilities, and embedding forensic readiness into system and network design. By addressing these critical areas, stakeholders can ensure that the benefits of 6G connectivity are realized in a secure, resilient, and trustworthy manner-paving the way for a future where smart devices and systems can operate with confidence and integrity.

7. REFERENCES

Peer-Reviewed Journal Articles (2020–2025):

1. D. P. Moya Osorio et al., "Towards 6G-Enabled Internet of Vehicles: Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 3, pp. 82-105, 2022, doi: 10.1109/OJCOMS.2022.3143098. https://ieeexplore.ieee.org/abstract/document/9681822
2. S. Son, D. Kwon, S. Lee, H. Kwon and Y. Park, "A Zero-Trust Authentication Scheme With Access Control for 6G-Enabled IoT Environments," in IEEE Access, vol. 12, pp. 154066-154079, 2024, doi: 10.1109/ACCESS.2024.3484522. https://ieeexplore.ieee.org/abstract/document/10729236
3. D. Yu, J. Ren, Q. Yang, S. Tarkoma, M. Siddula and F. Dressler, "Guest Editorial Special Issue on When Blockchain Meets 5G/6G—Enabling Endogenously Secure IoT," in *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 11946-11948, 15 July15, 2023, doi: 10.1109/JIOT.2023.3275289. https://ieeexplore.ieee.org/abstract/document/10174842
4. M. Wazid, A. K. Das, S. Shetty, P. Gope and J. J. P. C. Rodrigues, "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap," in *IEEE Access*, vol. 9, pp. 4466-4489, 2021, doi: 10.1109/ACCESS.2020.3047895. https://ieeexplore.ieee.org/abstract/document/9309301
5. R. Meng *et al.*, "Efficient Gaussian Process Classification-Based Physical-Layer Authentication With Configurable Fingerprints for 6G-Enabled IoT," in *IEEE Transactions on Consumer Electronics*, doi: 10.1109/TCE.2025.3557239. https://ieeexplore.ieee.org/abstract/document/10947359
6. P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081. https://ieeexplore.ieee.org/abstract/document/9426946
7. M. Noor-A-Rahim *et al.*, "6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities," in *Proceedings of the IEEE*, vol. 110, no. 6, pp. 712-734, June 2022, doi: 10.1109/JPROC.2022.3173031. https://ieeexplore.ieee.org/abstract/document/9779322
8. A. Koren and R. Prasad, "IoT Health Data in Electronic Health Records (EHR): Security and Privacy Issues in Era of 6G," in *Journal of ICT Standardization*, vol. 10, no. 1, pp. 63-84, 2022, doi: 10.13052/jicts2245-800X.1014. https://ieeexplore.ieee.org/abstract/document/10255403
9. Y. Luo *et al.*, "Securing 5G/6G IoT Using Transformer and Personalized Federated Learning: An Access-Side Distributed Malicious Traffic Detection Framework," in *IEEE Open Journal of the Communications Society*, vol. 5, pp. 1325-1339, 2024, doi: 10.1109/OJCOMS.2024.3365976. https://ieeexplore.ieee.org/abstract/document/10436365

10. S. F. Ahmed *et al*., "Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities," in *IEEE Access*, vol. 12, pp. 13125-13145, 2024, doi: 10.1109/ACCESS.2024.3352508. https://ieeexplore.ieee.org/abstract/document/10387440
11. A. Dogra, R. K. Jha and S. Jain, "A Survey on Beyond 5G Network With the Advent of 6G: Architecture and Emerging Technologies," in *IEEE Access*, vol. 9, pp. 67512-67547, 2021, doi: 10.1109/ACCESS.2020.3031234. https://ieeexplore.ieee.org/abstract/document/9224777
12. R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran and L. Mostarda, "Survival Study on Blockchain Based 6G-Enabled Mobile Edge Computation for IoT Automation," in *IEEE Access*, vol. 8, pp. 143453-143463, 2020, doi: 10.1109/ACCESS.2020.3013946. https://ieeexplore.ieee.org/abstract/document/9159552
13. I. Cetintav and M. Tahir Sandikkaya, "A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs," in *IEEE Access*, vol. 13, pp. 37703-37723, 2025, doi: 10.1109/ACCESS.2025.3546147. https://ieeexplore.ieee.org/abstract/document/10904450
14. V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi and A. Rezaki, "Security and Trust in the 6G Era," in *IEEE Access*, vol. 9, pp. 142314-142327, 2021, doi: 10.1109/ACCESS.2021.3120143. https://ieeexplore.ieee.org/abstract/document/9570274
15. A. S. Khan *et al*., "Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network," in *IEEE Access*, vol. 11, pp. 20524-20541, 2023, doi: 10.1109/ACCESS.2023.3249969. https://ieeexplore.ieee.org/abstract/document/10054371
16. X. Chen, W. Feng, N. Ge and Y. Zhang, "Zero Trust Architecture for 6G Security," in *IEEE Network*, vol. 38, no. 4, pp. 224-232, July 2024, doi: 10.1109/MNET.2023.3326356. https://ieeexplore.ieee.org/abstract/document/10288499
17. S. Prasad Tera, R. Chinthaginjala, G. Pau and T. Hoon Kim, "Toward 6G: An Overview of the Next Generation of Intelligent Network Connectivity," in *IEEE Access*, vol. 13, pp. 925-961, 2025, doi: 10.1109/ACCESS.2024.3523327. https://ieeexplore.ieee.org/abstract/document/10816608
18. J. Cook, S. U. Rehman and M. A. Khan, "Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions," in *IEEE Access*, vol. 11, pp. 39295-39317, 2023, doi: 10.1109/ACCESS.2023.3268064. https://ieeexplore.ieee.org/abstract/document/10103890
19. M. Hojjati, A. Shafieinejad and H. Yanikomeroglu, "A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks," in *IEEE Access*, vol. 8, pp. 216461-216476, 2020, doi: 10.1109/ACCESS.2020.3041710. https://ieeexplore.ieee.org/abstract/document/9276451
20. W. Yi, Y. Fu, J. Cao, Y. Zhang, B. Niu and H. Li, "AotmAuth: Atomic Function Module-Based 6 G Authentication Protocol Combination Framework," in *IEEE Transactions on Dependable and Secure Computing*, doi: 10.1109/TDSC.2025.3553474. https://ieeexplore.ieee.org/abstract/document/10937231

21. T. -V. Le, C. -F. Lu, C. -L. Hsu, T. K. Do, Y. -F. Chou and W. -C. Wei, "A Novel Three-Factor Authentication Protocol for Multiple Service Providers in 6G-Aided Intelligent Healthcare Systems," in *IEEE Access*, vol. 10, pp. 28975-28990, 2022, doi: 10.1109/ACCESS.2022.3158756. https://ieeexplore.ieee.org/abstract/document/9732957
22. Benlloch-Caballero, P., Wang, Q., & Calero, J. M. A. (2023). Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. *Computer Networks*, *222*, 109526. https://www.sciencedirect.com/science/article/pii/S1389128622005606
23. Muheidat, F., Dajani, K., & Lo'ai, A. T. (2022). Security concerns for 5G/6G mobile network technology and quantum communication. *Procedia Computer Science*, *203*, 32-40. https://www.sciencedirect.com/science/article/pii/S1877050922006123
24. Yang, M., Qu, Y., Ranbaduge, T., Thapa, C., Sultan, N., Ding, M., ... & M'rabet, S. (2024). From 5g to 6g: A survey on security, privacy, and standardization pathways. *arXiv preprint arXiv:2410.21986*. https://arxiv.org/abs/2410.21986

Top-Tier Conference Papers:

25. Xu, T., Wang, N., Pang, Q., & Zhao, X. (2024). Security and privacy of 6G wireless communication using fog computing and multi-access edge computing. *Scalable Computing: Practice and Experience*, *25*(2), 770-781. https://scpe.org/index.php/scpe/article/view/2629
26. Rachakonda, L. P., Siddula, M., & Sathya, V. (2024). A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). *High-Confidence Computing*, 100220. https://www.sciencedirect.com/science/article/pii/S2667295224000230
27. Akinbi, A. O. (2023). Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks. *Wiley Interdisciplinary Reviews: Forensic Science*, *5*(6), e1496. https://wires.onlinelibrary.wiley.com/doi/full/10.1002/wfs2.1496
28. Bhide, P., Shetty, D., & Mikkili, S. (2024). Review on 6G communication and its architecture, technologies included, challenges, security challenges and requirements, applications, with respect to AI domain. *IET Quantum Communication*. https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/qtc2.12114
29. Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and beyond. *IEEE Communications Surveys & Tutorials*, *21*(4), 3682-3722. https://ieeexplore.ieee.org/abstract/document/8712553

White Papers and Industry Standards:

30. Ericsson, *5G Spectrum for Local Industrial Networks*, White Paper, Feb. 2020. [Online].

https://www.ericsson.com/en/reports-and-papers/white-papers/5g-spectrum-for-local-industrial-networks

31. Ericsson, *Energy Performance of 6G RAN*, White Paper, Feb. 2023. [Online]. https://www.ericsson.com/en/reports-and-papers/white-papers/energy-performance-of-6g-ran
32. Ericsson, *Network Resilience Through Zero Trust Architecture*, White Paper, Jan. 2024. [Online]. https://www.ericsson.com/en/reports-and-papers/white-papers/network-resilience-through-zero-trust-architecture
33. Ericsson, *5G Advanced – Evolution Towards 6G*, White Paper, Sep. 2023. [Online]. https://www.ericsson.com/en/reports-and-papers/white-papers/5g-advanced-evolution-towards-6g
34. CWNP, *Wireless Network Security: Designing and Maintaining Secure Wireless for Enterprise*, White Paper, 2022. [Online]. https://www.cwnp.com/uploads/1658_cwnp-cwnp-whitepaper_final.pdf

Technical Report:

35. Bharat 6G Alliance, *Working Group Report*, 2023. [Online]. https://bharat6galliance.com/bharat6G/Home/content/Working-Group-Report/Working-Group-Report
36. Bharat 6G Alliance, *Bharat 6G Vision and Mission Report*, 2023. [Online]. https://bharat6galliance.com/bharat6G/public/assets/report/document_14876603.pdf