Securing IoT with Resilient Cloud-Edge Continuum

Engin Zeydan*, Awaneesh Kumar Yadav†, Pasika Ranaweera‡, Madhusanka Liyanage§
†§School of Computer Science, University College Dublin, Ireland
*Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Spain
‡School of Electrical and Electronic Engineering, University College Dublin, Ireland
Email: *engin.zeydan@cttc.cat, †awaneesh.yadav@ucd.ie, ‡ pasika.ranaweera@ucd.ie, §madhusanka@ucd.ie,

***Abstract*—In the era of 6G, securing the computing continuum, which includes cloud, edge and IoT infrastructures, is a major challenge. This paper addresses these challenges by presenting a secure framework to develop advanced cybersecurity solutions tailored to this complex environment. The proposed security architecture is designed to comprehensively address issues such as decentralized governance, increasing heterogeneity and an increasingly sophisticated threat landscape. A central focus is on the Zero Trust Architecture (ZTA), which ensures that no internal or external entity is trusted by default, increasing security at every access point. In addition, the integration of AI-powered automated closed-loop security mechanisms is explored, highlighting their role in detecting and responding to threats in real time within the cloud edge continuum. Data security and access management are critical for safeguarding sensitive information in distributed environments. The paper concludes with a discussion of limitations and future research directions, emphasizing the contributions of the proposed framework to improving cybersecurity resilience, preparedness, and awareness in the context of 6G computing environments compared to traditional approaches.**

***Index Terms*—zero-trust architecture, AI-enabled security, threat, detection, response**

I. Introduction

An Internet of Things (IoT) ecosystem is a network of interconnected devices, sensors and software applications that collect, analyze and share data [1]. The emergence of new networks and cloud paradigms with 6G has made it possible to distribute computing resources and processing tasks between centralized cloud servers and edge servers and support many remote devices. This creates a continuum of computing capacity that offers multiple benefits, including lower latency, bandwidth efficiency, data protection and compliance, resilience and reliability [2]. As we move towards an interconnected network of IoT devices and applications, we encounter a variety of entities and devices, each with its own role and potential vulnerabilities. These elements constantly communicate, exchange data and influence each other, creating a complex and extensive ecosystem. Therefore, 6G must employ advanced, intelligent, and flexible security mechanisms to ensure this ecosystem's integrity, interoperability, and functionality, which supports critical infrastructure and applications across multiple industries. These mechanisms must protect the individual components throughout their lifecycle and, therefore, the wider interconnected systems. For this reason, ensuring a secure data processing continuum encompassing both edge and cloud networks is essential to protect the security and privacy of IoT data and its associated systems.

In the future, the 6G network, which includes all components communicating via standard communication paths, will be the biggest attack vector for complex IoT systems [3]. However, determining the appropriate path to security depends on the specific application and service, making it difficult to develop standards and best practices. In addition, large industrial companies often face the challenge of quickly remediating dangerous vulnerabilities in their technical networks and office network perimeters [4]. Cyber attacks can cause data leaks, disrupt internal IT systems and lead to unplanned shutdowns and downtime in production and shipping, sometimes lasting weeks and causing hundreds of millions of euros in losses [5]. According to the EU's Cyber Resilience Act, the annual cost of cybercrime worldwide is estimated at €5.5 trillion by 2021, largely due to successful cyberattacks on hardware and software products [6].

This paper addresses the urgent need for improved cybersecurity in critical infrastructure systems, focusing on developing innovative security solutions for cloud-edge integration. Our contributions in this paper include outlining the proposed framework, describing its architecture, and presenting use cases that demonstrate its effectiveness in improving security, resilience, and efficiency. By introducing advanced security mechanisms such as Zero Trust Architecture (ZTA), Artifical Intelligence (AI)-driven automation and secure data lifecycle management, we aim to mitigate cybersecurity risks and ensure the reliability of critical infrastructure operations in the face of evolving threats. The rest of the paper is organized as follows. Section II details key challenges in securing the compute continuum in 6G. Section III gives the general security architecture. Section IV gives the main bases of architecture, including ZTA aspect, details on AI-powered automatic closed loop security and details on data security and access management. Section V gives the future directions, and finally, Section VI provides the paper's conclusions.

II. Key challenges in securing the computing continuum in 6G

6G is tapping into THz-level communication while catering edge intelligence to reach beyond the constrictions of networking infrastructure put forward by 5G standardization. This enables the envisioned guarantees of $>$ 1 Tbps data rates, $<$ 0.1 ms E2E delay, $<$ 10 ns processing delay, and other amplified aspects [7]. 6G standardization advances current 5G-based solutions through cutting-edge use cases and enabling technologies [8], [9]; that envisages an intelligent IoT or Internet of Everything (IoE) based service infrastructure expanding to the cloud edge continuum [7], [10]. These aspects lead to a more diverse IoT-Edge-Cloud (IEC) continuum infrastructure

979-8-3503-5469-0/24/$31.00 ©2024 IEEE

with 6G that attributes extended heterogeneity, decentralized operation, and highly dynamic ecology. Hence, threat and attack vectors attempt to metamorphose the current threat landscape into one extending to the entire IEC continuum. Key challenges that we have observed in this research are listed below.

A. Decentralized governance

Holistic autonomy in service deployment, operation, maintenance, and termination is a requirement shadowing the 6G use cases, where it is critical with autonomous or connected vehicle-based deployments [11], [12]. Facilitation of autonomy is only possible by distributing the management/orchestration operations to the proximate domains of service delivery points. With these scattered governing domains, maintaining consistency across security policies and specifications is going to be an arduous task, especially considering that decentralization is not only limited to the IoT layer but extends to the edge layer considering the O-RAN integration [13]. The governing/operating policies are changing through the E2E-IEC tunnel of a specific 6G service from local domains to metropolitan, regional, and national levels. From a security perspective, automated security initiatives are limited to access control via authentication and Intrusion Detection and Prevention Systems (IDPS). Decentralization also causes access to digital systems to be domain-specific, where user identity should be verified at each domain crossing through a repeated authentication query since the trust domains are bound to the governing domains. Thus, updating authentication protocol specifications, access control policies, IDPS signature/pattern databases in real-time, and managing user identity trustfully across the continuum is challenging.

B. Extended Heterogeneity and hereditary threat landscape

6G introduces a new perspective to service infrastructures that extends to the IEC continuum. From the IoT device layer end, the expected intelligence within its domain requires more resourceful IoT nodes that feature energy-efficient strategies [14], [15], or a group/array of devices collaborating to achieve complex computations in a secure multi-party manner [16]. The communication in the same domain is exploring less energy-consuming choices to align with Low Rate Wireless Personal Area Networks (LR-WPAN) for intra-IoT sensory/actuator domains and Low Power Wide Area Networking (LPWAN) transceivers for communication of inter-IoT-domains. The heterogeneity observed in this context is obvious and extends beyond devices to the protocol level. This expands the current appraised threat landscape to novel bounds, where low-rate and energy-efficient aspects are most lucrative for attackers since security is expected to be minimal with such deployments. Further, the flexibility offered through O-RAN integration to the immediate edge domains extends the heterogeneity towards the edge domain, which was limited to the device/access or IoT layer in 5G. Interoperability concerns attributed to this extended heterogeneity are perfect hunting grounds for capable cyber intruders, where a successful cyber attack within the edge domain can grant access to IoT and cloud directions in the IEC continuum.

C. Advanced persistent threats (APTs)

As its name implies, APTs are highly sophisticated, long-term cyberattacks often orchestrated by highly skilled hackers aimed at stealing sensitive information, disrupting operations, or causing extensive damage [17]. In the context of 6G, the extended heterogeneity and hereditary interoperability discrepancies facilitate the APTs to be more stealthy within the network. They may use sophisticated techniques to blend in with normal network traffic or evade, making them even harder to detect and allowing them to persist for extended periods [18]. APTs can launch multi-stage operations, but with 6G, they may exploit diverse vectors of autonomous security defences simultaneously [19]. This could involve combining network-based attacks with direct attacks on IoT devices, edge computing infrastructure, and even leveraging quantum computing resources. APT actors can exploit vulnerabilities in 6G technologies, using zero-day exploits and other sophisticated methods to compromise the network.

D. Attacks on automated intelligence in 6G and AI-enabled attack models

AI/Machine Learning (ML) can be beneficial for attackers as well as for defence. Adversarial attacks are the most possible threats that can manipulate AI models to cause incorrect outcomes [20]. Since 6G systems depend more on such intelligence, designing defence for such attacks is paramount. Poisonous attacks hold the same intensity in this threat landscape, while they cause the most impact in distributed/federated learning deployments [17]. Adversaries can leverage AI models to predict the outcomes of typical IDPS entities in traffic analysis and input patterns to the traffic channels that would not be detected by current means through persistent assimilation [21]. Similar approaches can be taken to launch DDoS, bot-based, traffic diverting, and service disruption attempts, where the impact is colossal considering the 6G guarantees.

E. Resource constraints on edge Vs. quantum computing capabilities

It is obvious that edge devices typically have limited computational resources, making it challenging to implement strong encryption and other security measures without impacting performance [22]. This is more critical in the case of O-RAN deployments, where such services are to be operated with a considerable security level [23]. Cloud-based quantum computing services can now be accessed through paid means. Thus, even if traditional means of cryptography are utilized to provide a level of security that compromises edge resources, that possibility dilutes the defence of the IEC tunnel, especially at the edge domain.

Table I tabulates novel solutions that can overcome the above mentioned challenges.

TABLE I: State-of-the-art solutions to overcome the security challenges of 6G IEC continuum

State-of-the-art Solutions	Short Description	Security Challenges				
		Decentralization	Heterogeneity	APTs	AI and ML	Resource Issues
Quantum Resisting Cryptography	Post-quantum methods are designed to withstand the operations of quantum algorithms such as Shor's and Grover's.			[24]	[25]	[26]
Decentralized Identity Management	DIDs are unique identifiers created and managed independently of any centralized registry or authority. They are stored on a decentralized network, such as a blockchain.	[27]	[28], [29]			
Self-sovereign identity	Leverage DID creation, but enhance privacy by minimizing the amount of personal data shared and stored. It employs cryptographic techniques to ensure that identity information is secure and verifiable.	[30]	[31]			
Decentralized Key/Certificate Management	Concepts of blockchain decentralization applied for securing cryptographic keys and certificates.	[32]	[33]			[34], [35]
Security Service Level Agreement Management	Security policies and access levels agreed upon by parties facilitated by a certain service should be traced and monitored for violation, ensuring security.	[36], [37]	[36], [37]	[36], [37]		
Autonomous security orchestration	Integration, as well as coordination of various security tools and processes to streamline and automate security operations to integrate, automate, coordinate, and monitor.	[38]	[38], [39]	[38]		[39]
AI-enabled security defences	Leveraging AI constructs to launch autonomous and active response defence functions.			[40]	[40]	

IoT Device Domain | Edge Domain | IoT+Edge Domains | Edge+Cloud Domains

III. General Security Architecture

We propose a general security architecture in Figure 1 to provide a secure, connected IoT ecosystem across multiple layers of the cloud edge continuum.

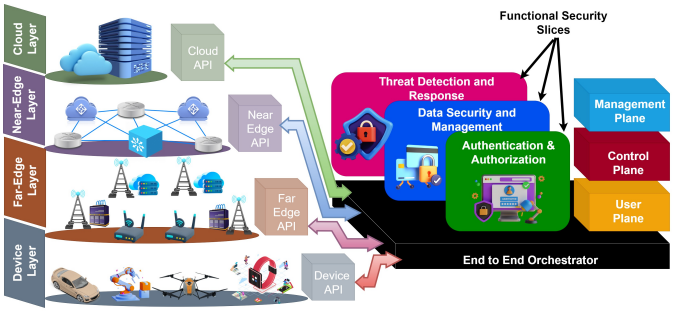

Fig. 1: General Architecture with 6G User, Control, and Management Planes

The proposed architecture provides a comprehensive security framework that safeguards interconnected levels and planes from individual devices to the cloud. It combines security measures with orchestration capabilities to ensure a holistic and adaptable approach to securing the entire ecosystem. The cloud edge continuum network connects sensors, actuators, drives, controllers, robots, machines and other devices that need to communicate in real-time (I/O communication). The architecture is divided into four main blocks comprising the management, control and data planes as follows:

IoT Device Authentication and Authorization: The authentication and authorization of IoT devices at various levels ensures secure access to the network. At the device level, devices are authenticated with specific credentials or digital certificates before gaining access to the network. The far-edge level manages authentication for devices and services with policies and access controls. Similarly, the near-edge level manages authentication to ensure only authorized entities access the network. At the cloud level, authentication extends to cloud services, applications and users.

IoT Data Security and Management: IoT data security and management involves multiple levels of encryption and secure data handling. This includes encryption and secure data management on the devices at the device level. At the far-edge level, data transferred between devices is secured through encryption and access controls. The near-edge level ensures a secure data flow between devices and services. At the cloud level, data security includes encryption at rest and in transit and strict access controls for cloud data.

Threat Detection and Response: Threat detection and response are critical components at all levels of the architecture. At the device level, basic intrusion detection monitors device behaviour for anomalies. Advanced Intrusion Detection and Prevention Systems (IDPS) are used to detect and defend against threats at the far-edge level. The near-edge level analyzes network traffic for potential threats and reacts accordingly. At the cloud level, monitoring includes using Security Information and Event Management (SIEM) systems and AI-based detection to monitor cloud services and infrastructures for security incidents.

End-to-end Orchestrator: The end-to-end orchestrator plays a crucial role in ensuring the security and integrity of the entire architecture. It coordinates authentication, data security and threat detection at all levels and manages policy enforcement, dynamic provisioning and real-time security response. This ensures consistent security measures and automates responses to evolving threats to maintain a robust and resilient IoT ecosystem.

Figure 2 shows the low-level design of the proposed architecture with interacting layers and components. The architecture enables robust protection against lateral movement, granular access control and unified policy enforcement through the Zero-Touch (ZT) Policy Controller, regardless of the underlying infrastructure, allowing it to be deployed flexibly

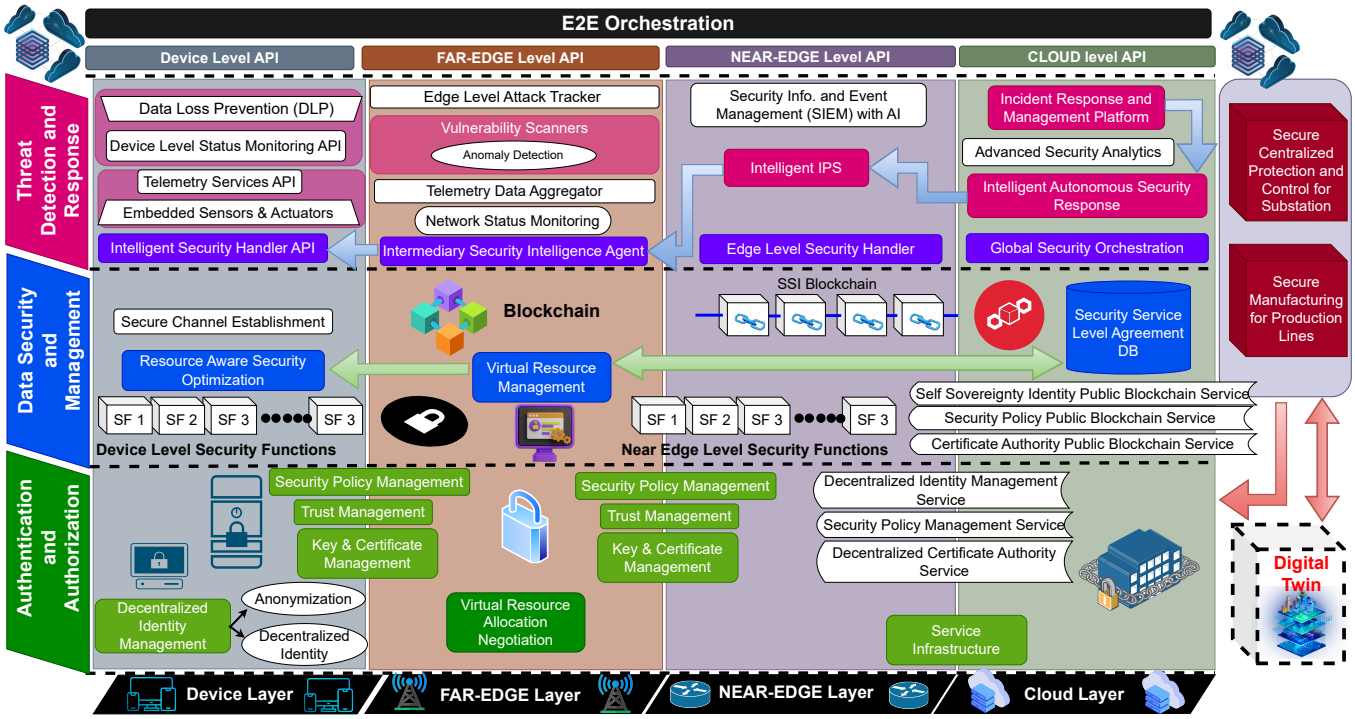

Fig. 2: Low Level Design Architecture of Secure 6G Networks

in the cloud or on-premises. ZT policies are enforced through parallel orchestration across network, cloud/edge and cyber-security domains to ensure end-to-end security. Each domain has custom policy orchestration and automated response via its own controller. The Orchestrator manages network traffic, access, applications, and databases via predefined policies. The orchestrator analyses the collected data, which mitigates threats through automated policy changes. The secure and resilient edge/cloud orchestration layer is critical for efficient service orchestration. It addresses inter-node and intra-node aspects and enables automated closed-loop security in the cloud-edge continuum. Cross-node orchestration treats every interaction and service placement as potentially untrusted to ensure a secure environment across multiple nodes. Continuous auditing and authentication of interactions and resource allocations within a node prevent unauthorized access or compromise. The integrity and authenticity of data are verified at every step to minimize the risks associated with telemetry data and service placement decisions.

IV. Main Pillars of Architecture

In this section, we introduce three main pillars of the proposed architecture, namely ZTA, AI-powered closed-loop security and data security and management and describe how each can help improve the overall security of the IoT networks.

A. Zero Trust Architecture (ZTA)

The proposed architecture's first base is ZTA for the cloud-edge continuum in IoT networks. Fig. 3 shows the logical components of the ZTA that are investigated in this paper. The architecture consists of logical components in management, control and data planes. The policy engine and the policy administrator are in the administration and control levels. At the data plane, the Policy Enforcement Point (PEP) executes the policies with the help of agent interactions. ZTA, as a philosophy implemented through architecture and technology, adopts a "never trust, always verify" approach, enabling micro-segmentation boundaries, continuous authentication, and authorization mechanisms [41]. ZTA verifies IoT devices, assesses risks, enforces policies, and establishes secure connections. It transfers identity, trust, and authority information to the orchestration layer for finer-grained access control. ZTA securely connects IoT devices to resources, reducing the attack surface, preventing lateral propagation and data loss, and minimizing breaches [42]. A secure private cloud acts as a control point to enforce zero-trust policies, ensuring users access only authorized data and resources, enhancing security across risk, cost, and usability dimensions [43].

To ensure security and reduce risks, ZTA performs several actions when IoT devices connect to applications and data. Initially, it checks connection requests, verifies IoT device identity, and assesses the risk level. Technologies like Multi-Factor Authentication (MFA), Blockchain-based Self Sovereign Identity, or Public Key Cryptography (PKI) are crucial to safeguard credentials [44]. ZTA enforces policies, connecting IoT devices only to authorized applications, eliminating the risk of lateral propagation and network segmentation complexities. It establishes secure, outbound-only connections to requested resources, keeping transactions invisible and minimizing attack surfaces. ZTA is expected to perform these actions for every transaction, ensuring scalability and performance [45]. While ZTA is a progressive step towards securing IoT services, it

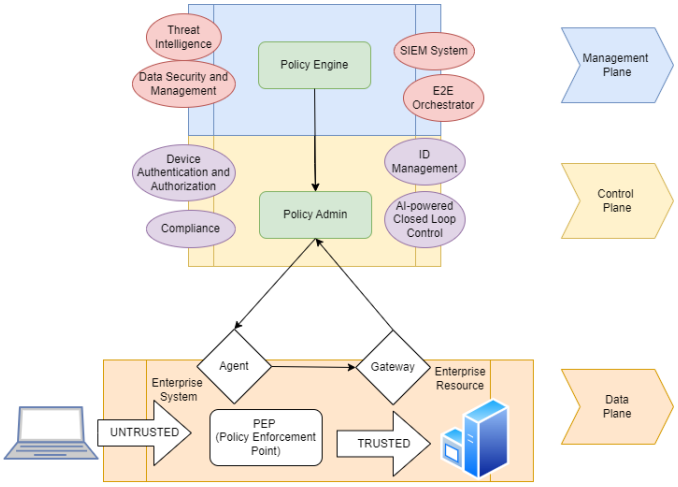

Fig. 3: Zero Trust Architecture Components

requires improvements to address evolving challenges [46].

B. AI-powered automatic closed loop security in cloud-edge continuum

The second base of the proposed architecture focuses on AI-powered data security in the cloud edge continuum. Usability testing ensures that these AI-powered security measures maintain data processing efficiency. Continuous updates to AI models and security measures are prioritized to meet evolving data security requirements. ML techniques, including federated learning, preserve privacy during data communication and ensure a comprehensive approach to AI-powered data processing. ML-based anomaly detection algorithms identify suspicious data access patterns, increasing overall security [47]. The cloud edge continuum seamlessly integrates edge and cloud computing and optimizes data processing by combining local processing at the edge with the advanced capabilities of cloud computing. AI, automation and cloud-native technologies enhance security measures and complement traditional methods, especially in automated closed-loop security control [48]. AI is used to analyze the behavior of IoT devices and units, detect anomalies and threat hunting. This includes analyzing trends over time, correlating data from different sources and developing comprehensive threat eradication plans. Post-incident activities, including lessons learned and continuous improvement of protection, detection and response to new types of attacks, are essential.

C. Data security and access management

The third base of the proposed architecture is authentication mechanisms for the IoT combined with continuous monitoring and strict access control, whereby the proposed architecture assumes that there is no trust within the IoT-enabled cloud-edge continuum networks [49]. The proposed architecture's identity infrastructure will be critical to building ZTA's identity-based capabilities. The proposed architecture continuously monitors security. Each user, device, and application will be independently verified, and the automated security of each user, device, and application will ensure that access authorization is dynamically and automatically adjusted in real-time based on trust level (based on attributes, behaviours, and access context). Some zero trust authentication mechanisms such as MFA, continuous authentication, IoT device health assessment, user and entity behaviour analysis (using AI algorithms), micro-segmentation, application-level security (beyond the network level), software-defined perimeter, Identity and Access Management (IAM), digital certificates, and passwordless authentication are also critical aspects to be embedded into the design.

V. Limitations and Future Directions

The deployment of the proposed architecture is challenging, and the following limitations of the main pillars should be considered in order to fully take advantage of it.

A. AI-powered closed-loop security

Although AI-powered security has made significant progress in the cloud edge continuum, it faces limitations, including:

- **Ensuring data confidentiality and integrity between edge devices and cloud servers**, for instance, poses significant privacy and security risks during AI model learning. The proposed architecture uses Federated Learning (FL) techniques to train models for security functions across multiple decentralized devices and servers to keep data localized. With secure model aggregation techniques, FL prevents sensitive data from being transmitted and reduces their exposure.
- **Evolving cyber threats:** The latest threat patterns require continuous learning and adaptation, which can be resource-intensive and challenging to manage in a distributed cloud-edge environment. For this reason, AI models may not perform equally well across different environments or against novel attack vectors. Ensuring that these robust models can generalize well across diverse scenarios is a significant challenge. In addition, training and maintaining AI models, especially in a distributed environment like the cloud-edge continuum, can be resource-intensive regarding data, computing power, and expert personnel. The proposed architecture adopts Machine Learning Operations (MLOps) to maintain up-to-date, security-efficient AI models and facilitate rapid adaptation to new data by automating key aspects of the model lifecycle to provide actionable intelligence and automated responses. Connecting AI systems to various Cyber Threat Intelligence (CTI) sources is also vital. These sources provide up-to-date information about the latest cyber threats, vulnerabilities, and attack strategies. The proposed architecture integrates this intelligence, AI models can be trained with the most current data (not only log data but also network traffic, endpoint activities, edge/cloud events, threat intelligence and IoT or device behaviour in both real and digital twin environments), helping them recognize and respond to new and emerging threats more effectively. In addition, the proposed architecture integrates with up-to-date security tools, executing remediation actions and improving threat detection capabilities.

TABLE II: Comparisons of Proposed ZTA-enabled and Traditional Security Management Approaches

Characteristic	Proposed ZTA-based Approach	Traditional Approach
Authentication	— Blockchain-based authentication mechanisms.	— Traditional username and password authentication. — MFA methods. — PKI based authentication.
Security	— High level of security due to ZTA framework — AI-driven models for threat detection and anomaly detection. — AI-based intrusion detection systems (IDS). — Federated learning for collaborative threat intelligence.	— Relies on perimeter-based security measures — Traditional firewall and intrusion detection/ prevention systems.
Flexibility	— Provides flexibility in system architecture and device integration with advanced security orchestration and automation platforms for automated security deployments.	— Limited flexibility due to rigid security perimeters — Traditional security management platforms
Scalability	— Scalable architecture suitable for large-scale deployments	— Limited scalability, especially in dynamic environments
Resilience	— Offers resilience against cyber threats through real-time monitoring and adaptive security measures — AI-based vulnerability assessment tools. — Automated incident response using SOAR (Security Orchestration, Automation, and Response) tools.	— Traditional vulnerability scanning and patch management. — Vulnerable to cyber-attacks and may require manual intervention and incident response for mitigation
Efficiency	— Optimized resource utilization and efficient data processing with cloud-native security solutions	— May suffer from resource bottlenecks and performance issues
Cost	— Initial setup costs may be higher but offers long-term cost savings through improved security	— Lower initial costs but may incur higher expenses for security breaches and maintenance

- **Adhering to evolving regulatory requirements and ethical standards**, especially in different jurisdictions, is a complex and ongoing challenge. The proposed architecture aims to explore and understand regulatory boundaries for compliance with key EU directives like the NIS (2016), NIS 2 (2022), EU Cybersecurity ACT (2019), and Cyber Resilient ACT (2022), ensuring seamless integration of technologies within these frameworks and addressing potential barriers proactively.
- **Automating closed-loop security with policy enforcement and orchestrating security responses** are critical for managing Zero Trust networks' complexity and dynamic nature. The use of AI firstly enhances the predictive capabilities of ZTA systems to anticipate threats before they occur, such as the prevention of APTs or analyzing CTI from various sources to understand the threat landscape, followed by a real-time response to detected threats and anomalous behavior. The proposed architecture aims to interact with a CTI source by receiving and analyzing threat data, including indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs) of adversaries. This intelligence is integrated into the proposed architecture's monitoring and detection systems, enhancing their ability to identify and respond to potential threats. The proposed architecture uses this information for proactive threat hunting to refine its incident response strategies and update defense mechanisms based on insights gained from the intelligence.

B. Data security and access management

- **Securing access management:** In IoT-enabled cloud edge networks is a significant challenge, particularly as the IoT evolves alongside computer networks and the Internet. The complexity of the digital landscape, especially with the advent of 6G, underscores the necessity for robust, scalable, and automated authentication methods [50]. Securing IoT data, particularly for low-cost devices with limited storage space that store all information on cloud servers, is a pressing issue. With the introduction of 6G authentication, where cloud servers utilize AI to process data, securing cloud data becomes even more intricate. Key considerations for protecting IoT data in the edge-cloud continuum include device authentication and authorization, secure communications, end-to-end encryption, device lifecycle management, secure boot, firmware updates, access control, and security audits.
- **PKI or Digital signature:** These technologies have become integral for secure web communication, enabling servers to verify their identity through digital certificates [51]. In the context of IoT, PKI and digital signatures are not only relevant but also complementary. They are crucial in establishing secure, trusted, and verifiable communication channels between IoT devices and the edged/Cloud servers. These channels are foundational for the reliable functioning of advanced technologies in these domains, especially when AI is utilized in the cloud server. The traditional method of obtaining certificates can be costly, but with AI and blockchain, certificate issuing and revocation can be faster, more efficient, and cost-effective for users.
- **Quantum-safe authentication:** It is being used due to the development of quantum computers. Mostly used ECC and RSA are prone to quantum attacks, and the quantum algorithms are very costly [52]. So, we may use the hybrid approach to secure communication from quantum attacks and be cost-effective for the user. Also, we can use the conventional approach to secure communication during authentication. Advanced Encryption Standard (AES), 256 bits, can resist quantum attacks.

C. Zero Trust Architecture

- **Internal Threat Handling:** As cyber threats evolve, continuous adaptive risk and trust assessment capabilities are needed to adjust to new threats dynamically. For example, while the ZTA effectively verifies trust before access, it may still be vulnerable to threats from insiders to whom access has already been granted. For this reason, techniques for continuous behavioural analysis and anomaly detection systems must be enhanced to quickly and accurately identify anomalous behaviour that may pose a risk of insider threats, orchestrate appropriate security responses and enforce security policies. In this paper, we propose to build an incident handling plan in line with the NIST4 Incident Response framework, which includes cyclical activities of continuous learning and progress to discover how best to protect a system such as an IoT network with an autonomous threat detection and mitigation framework.
- **Performance Degradation:** The use of cloud services for security offers scalability and flexibility, allowing organisations to deploy zero-trust controls in a variety of environments seamlessly. However, additional security controls and continuous monitoring can lead to performance degradation, so optimisation is necessary to ensure that security measures do not degrade system or service performance. This paper aims to propose a sophisticated security orchestrator capable of instructing container orchestrators to implement updates in network services. The primary objective of these updates will be to effectively contain or eradicate any security incidents and guarantee the uninterrupted and correct operation of all network services during and after the implementation of security measures.
- **Resource Constrained Devices:** The ZTA focuses primarily on IT devices, and there is a gap regarding other connected devices, such as IoT devices, which can be large in number to control and may not support advanced security features. Additional mechanisms are therefore needed to manage security and trust on a large scale and across the diversity of IoT ecosystems. This paper proposes a strategy for segmenting connected devices to prevent lateral movement attacks. Additionally, it aims to implement extra control functions within the network to enhance the protection of devices with limited security features.
- **Usability:** Strict authentication processes can sometimes lead to a tedious user experience, with repeated login prompts and delays. This calls for innovative solutions that reconcile security and ease of use, such as more adaptive authentication methods that exploit user behaviour and context to reduce unnecessary frustration. This paper aims to introduce an advanced continuous verification mechanism for ZTAs. At its core, this mechanism leverages an innovative and unobtrusive Multi-Factor Authentication (MFA) approach. The key feature of this MFA method is its transparency, which eliminates user interaction, thereby streamlining the authentication process. Additionally, This paper aims to design this approach for easy integration with existing platforms, enhancing security and user experience without compromising operational efficiency.

Finally, Table II compares the proposed ZTA-enabled and traditional security management approaches.

VI. Conclusion

In this paper, we have shown that it is possible to improve security, resilience and efficiency in areas such as smart grids and manufacturing by developing and implementing innovative security solutions, including zero-trust architecture, AI-driven automation and secure data lifecycle management. This is an important step in addressing cybersecurity challenges for critical infrastructure systems. Our findings underscore the importance of proactive measures to protect critical infrastructure from cyber threats and highlight the effectiveness of a comprehensive approach that combines advanced technologies with security best practices. Further research and collaboration are essential to advance the state of the art in cybersecurity and ensure the long-term security and reliability of critical infrastructure systems.

Acknoledgements

This work is partly supported by the Science Foundation Ireland under the CONNECT phase 2 (Grant no. 13/RC/2077_P2).

References

[1] S. Bansal and D. Kumar, "Iot ecosystem: A survey on devices, gateways, operating systems, middleware and communication," International Journal of Wireless Information Networks, vol. 27, no. 3, pp. 340–364, 2020.

[2] J. Santos, T. Wauters, B. Volckaert, and F. De Turck, "Towards low-latency service delivery in a continuum of virtual resources: State-of-the-art and research directions," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2557–2589, 2021.

[3] B. D. Son, N. T. Hoa, T. Van Chien, W. Khalid, M. A. Ferrag, W. Choi, and M. Debbah, "Adversarial attacks and defenses in 6g network-assisted iot systems," IEEE Internet of Things Journal, 2024.

[4] E. D. Knapp, Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Elsevier, 2024.

[5] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, "Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems," International Journal of Critical Infrastructure Protection, vol. 35, p. 100464, 2021.

[6] EC, "Cyber Resilience Act ," https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act/, 2022, [Online; accessed June-2024].

[7] C. De Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, and M. Liyanage, "Survey on 6g frontiers: Trends, applications, requirements, technologies and future research," IEEE Open Journal of the Communications Society, vol. 2, pp. 836–886, 2021.

[8] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6g networks: Use cases and technologies," IEEE Communications Magazine, vol. 58, no. 3, pp. 55–61, 2020.

[9] M. A. Uusitalo, P. Rugeland, M. R. Boldi, E. C. Strinati, P. Demestichas, M. Ericson, G. P. Fettweis, M. C. Filippou, A. Gati, M.-H. Hamon et al., "6g vision, value, use cases and technologies from european 6g flagship project hexa-x," IEEE access, vol. 9, pp. 160 004–160 020, 2021.

[10] J. Kumar, J. K. Samriya, M. Bolanowski, A. Paszkiewicz, W. Pawłowski, M. Ganzha, K. Wasielewska-Michniewska, B. Solarz-Niesłuchowski, M. Paprzycki, I. L. Úbeda et al., "Towards 6g-enabled edge-cloud continuum computing–initial assessment," in International Conference on Advanced Communication and Intelligent Systems. Springer, 2022, pp. 1–15.

[11] B. Yang, X. Cao, K. Xiong, C. Yuen, Y. L. Guan, S. Leng, L. Qian, and Z. Han, "Edge intelligence for autonomous driving in 6g wireless system: Design challenges and solutions," IEEE Wireless Communications, vol. 28, no. 2, pp. 40–47, 2021.

[12] A. M. Algarni and V. Thayananthan, "Autonomous vehicles with a 6g-based intelligent cybersecurity model," Ieee Access, vol. 11, pp. 15 284–15 296, 2023.

[13] R. Firouzi and R. Rahmani, "5g-enabled distributed intelligence based on o-ran for distributed iot systems," Sensors, vol. 23, no. 1, p. 133, 2022.

[14] A. Mukherjee, P. Goswami, M. A. Khan, L. Manman, L. Yang, and P. Pillai, "Energy-efficient resource allocation strategy in massive iot for industrial 6g applications," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5194–5201, 2020.

[15] H. Babbar, S. Rani, O. Bouachir, and M. Aloqaily, "From massive iot toward ioe: Evolution of energy efficient autonomous wireless networks," IEEE Communications Standards Magazine, vol. 7, no. 2, pp. 32–39, 2023.

[16] A. P. Kalapaaking, V. Stephanie, I. Khalil, M. Atiquzzaman, X. Yi, and M. Almashor, "Smpc-based federated learning for 6g-enabled internet of medical things," IEEE Network, vol. 36, no. 4, pp. 182–189, 2022.

[17] M. A. Ferrag, O. Friha, B. Kantarci, N. Tihanyi, L. Cordeiro, M. Debbah, D. Hamouda, M. Al-Hawawreh, and K.-K. R. Choo, "Edge learning for 6g-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses," IEEE Communications Surveys & Tutorials, 2023.

[18] A. Sharma, B. B. Gupta, A. K. Singh, and V. Saraswat, "Advanced persistent threats (apt): evolution, anatomy, attribution and countermeasures," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 7, pp. 9355–9381, 2023.

[19] N. I. Che Mat, N. Jamil, Y. Yusoff, and M. L. Mat Kiah, "A systematic literature review on advanced persistent threat behaviors and its detection strategy," Journal of Cybersecurity, vol. 10, no. 1, p. tyad023, 2024.

[20] Y. Wang, T. Sun, S. Li, X. Yuan, W. Ni, E. Hossain, and H. V. Poor, "Adversarial attacks and defenses in machine learning-empowered communication systems and networks: A contemporary survey," IEEE Communications Surveys & Tutorials, 2023.

[21] İ. Z. Altun and A. E. Özkök, "Securing artificial intelligence: Exploring attack scenarios and defense strategies," in 2024 12th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2024, pp. 1–6.

[22] S. U. Jamil, M. A. Khan, and S. U. Rehman, "Resource allocation and task off-loading for 6g enabled smart edge environments," IEEE Access, vol. 10, pp. 93 542–93 563, 2022.

[23] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open ran security: Challenges and opportunities," Journal of Network and Computer Applications, vol. 214, p. 103621, 2023.

[24] Z. Liu, K.-K. R. Choo, and J. Grossschadl, "Securing edge devices in the post-quantum internet of things using lattice-based cryptography," IEEE Communications Magazine, vol. 56, no. 2, pp. 158–162, 2018.

[25] D. Dharminder, A. K. Das, S. Saha, B. Bera, and A. V. Vasilakos, "Post-quantum secure identity-based encryption scheme using random integer lattices for iot-enabled ai applications," Security and Communication Networks, vol. 2022, no. 1, p. 5498058, 2022.

[26] S. Ebrahimi, S. Bayat-Sarmadi, and H. Mosanaei-Boorani, "Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in iot," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5500–5507, 2019.

[27] M. Luecking, C. Fries, R. Lamberti, and W. Stork, "Decentralized identity and trust management framework for internet of things," in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020, pp. 1–9.

[28] O. A. Khashan and N. M. Khafajah, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous iot systems," Journal of King Saud University-Computer and Information Sciences, vol. 35, no. 2, pp. 726–739, 2023.

[29] Z. Wu, Y. Xiao, E. Zhou, Q. Pei, and Q. Wang, "A solution to data accessibility across heterogeneous blockchains," in 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2020, pp. 414–421.

[30] M. Shuaib, S. Alam, M. S. Alam, and M. S. Nasir, "Self-sovereign identity for healthcare using blockchain," Materials Today: Proceedings, vol. 81, pp. 203–207, 2023.

[31] E. Samir, H. Wu, M. Azab, C. Xin, and Q. Zhang, "Dt-ssim: A decentralized trustworthy self-sovereign identity management framework," IEEE Internet of Things Journal, vol. 9, no. 11, pp. 7972–7988, 2021.

[32] S. Wijethilaka, A. K. Yadav, A. Braeken, and M. Liyanage, "A novel blockchain-based decentralized multi-party certificate management framework," in 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2023, pp. 1361–1368.

[33] M. A. Kandi, D. E. Kouicem, M. Doudou, H. Lakhlef, A. Bouabdallah, and Y. Challal, "A decentralized blockchain-based key management protocol for heterogeneous and dynamic iot devices," Computer Communications, vol. 191, pp. 11–25, 2022.

[34] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based decentralized authentication modeling scheme in edge and iot environment," IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2116–2123, 2020.

[35] M. S. Haghighi, M. Ebrahimi, S. Garg, and A. Jolfaei, "Intelligent trust-based public-key management for iot by linking edge devices in a fog architecture," IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12 716–12 723, 2020.

[36] N. Weerasinghe, R. Mishra, P. Porambage, M. Liyanage, and M. Yliantila, "Novel consensus mechanism for blockchain-based service level agreement management systems," Network, vol. 1, p. S3.

[37] ——, "Proof-of-monitoring (pom): A novel consensus mechanism for blockchain-based secure service level agreement management," IEEE Transactions on Network and Service Management, 2023.

[38] S. Wijethilaka and M. Liyanage, "The role of security orchestrator in network slicing for future networks," Journal of Communications and Networks, vol. 25, no. 3, pp. 355–369, 2023.

[39] N. Moradi, A. Shameli-Sendi, and A. Khajouei, "A scalable stateful approach for virtual security functions orchestration," IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 6, pp. 1383–1394, 2021.

[40] H. Li, J. Wu, H. Xu, G. Li, and M. Guizani, "Explainable intelligence-driven defense mechanism against advanced persistent threats: A joint edge game and ai approach," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 757–775, 2021.

[41] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero trust architecture for 6g security," IEEE Network, 2023.

[42] V. Stafford, "Zero trust architecture," NIST special publication, vol. 800, p. 207, 2020.

[43] M. Tsai, S. Lee, and S. W. Shieh, "Strategy for implementing of zero trust architecture," IEEE Transactions on Reliability, 2024.

[44] H. Sedjelmaci and N. Ansari, "Zero trust architecture empowered attack detection framework to secure 6g edge computing," IEEE Network, 2023.

[45] K. Gai, Y. She, L. Zhu, K.-K. R. Choo, and Z. Wan, "A blockchain-based access control scheme for zero trust cross-organizational data sharing," ACM Transactions on Internet Technology, vol. 23, no. 3, pp. 1–25, 2023.

[46] Y. He, D. Huang, L. Chen, Y. Ni, X. Ma et al., "A survey on zero trust architecture: Challenges and future trends," Wireless Communications and Mobile Computing, vol. 2022, 2022.

[47] S. Zehra, U. Faseeha, H. J. Syed, F. Samad, A. O. Ibrahim, A. W. Abulfaraj, and W. Nagmeldin, "Machine learning-based anomaly detection in nfv: A comprehensive survey," Sensors, vol. 23, no. 11, p. 5340, 2023.

[48] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and trust in the 6g era," Ieee Access, vol. 9, pp. 142 314–142 327, 2021.

[49] S. W. Shah, N. F. Syed, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Lcda: Lightweight continuous device-to-device authentication for a zero trust architecture (zta)," Computers & Security, vol. 108, p. 102351, 2021.

[50] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, K.-K. R. Choo, and G. Min, "A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things," IEEE Transactions on Computers, vol. 72, no. 2, pp. 501–512, 2022.

[51] J. J. D. Rivera, A. Muhammad, and W.-C. Song, "Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication," IEEE Open Journal of the Communications Society, 2024.

[52] D. Mishra, M. Singh, P. Reval, K. Pursharthi, N. Kumar, A. Barnawi, and R. Rathore, "Quantum-safe secure and authorized communication protocol for internet of drones," IEEE Transactions on Vehicular Technology, 2023.