AI-based Quantum-safe Cybersecurity Automation and Orchestration for edge Intelligence in Future Networks

Aarne Hummelholm, Timo Hämäläinen and Reijo Savola
Faculty of Information Technology, University of Jyväskylä, Finland

aarne.hummelholm@elisanet.fi
timo.t.hamalainen@jyu.fi
reijo.m.savola@jyu.fi

Abstract: The AIQUSEC (AI-based quantum secure cyber security automation and orchestration in the edge intelligence of future networks) brings measurable advances to the cyber security of access and edge networks and their services, as well as Operational Service Technologies (OT). The research aims for significant cybersecurity scalability, efficiency, and effectiveness of operations through improved and enhanced device and sensor securities, security assurance, quantum security, and Artificial Intelligence (AI) based automation solutions. The new application scenarios of near future, the multiple stakeholders within each scenario, and the higher data volumes raise the need for novel cybersecurity solutions. Recently, OT cybersecurity threat landscape has become wider, due to the increase digitalization of services, the increase in virtualization and slicing of networks, as well as the increase in advanced cyber-attacks. Because of recent advances in computing power, AI in cybersecurity analyzing and validations is now becoming a reality. A significant part of currently used encryption technologies which secures communications and infrastructures might become instantly penetrable when quantum computing becomes available. Enabling quantum-safety migration development is a clear goal to the project. The research develops a state-of-the-art information security verification and validation environment that supports the integration of cyber security systems as a reference model, focusing on architectural choices and network connection from different vertical use cases. With the help of the platform and the reference model, common cybersecurity capabilities and requirements can be built, tested, and validated, as well as their fulfillment. In addition to the environment mentioned above, the results of the research are demonstrated and utilized in critical communication systems, water utilities, industrial environments, in physical access solutions and remote work. The developed platform can also be used for auditing devices, systems, and software's in the future. The research integrates new quantum-safe artificial intelligence-based, hardware-hardened, and scalable cybersecurity solutions that have been validated in a standardized way. In this research, we also deal with the requirements of the EU sustainable growth program - issues related to the green transition.

Keywords: edge-intelligence systems, cyber threat, cyber-attacks, AI-based analysing, quantum encryption.

1. Introduction

Our AIQUSEC (AI-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks) is research project consortium of Business Finland's Digital Trust program. Cybersecurity is a core part of the program's roadmap. In the research we consider also post-quantum cryptography issues and what challenges quantum computing coming in the use means in our future information's systems and cybersecurity of them (Roger G. Massmann et al., 2023). University of Jyväskylä (JYU) coordinates the project and research. All research partners are from Finland. AI and it use is one part of our research. One of many AI definitions: "The term 'artificial intelligence' means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments (NAII, 2020). The Main Research Question (MRQ) is: Is it possible to build in cybersecurity effectively and efficiently, in a scalable way, for access and edge services in virtualized and sliced integration environment?

1.1 Grouping of paper

Chapter 1 presents the content of the document. Chapter 2 describes future operating environments. Chapter 3 presents our test environment. Chapter 4 describes cyber threats against our information systems. Chapter 5 deals with ethical considerations and chapter 6 international co-operation. Then the conclusions and future work.

1.2 Description of the future operating environment

1.2.1 Threat landscape is getting wider.

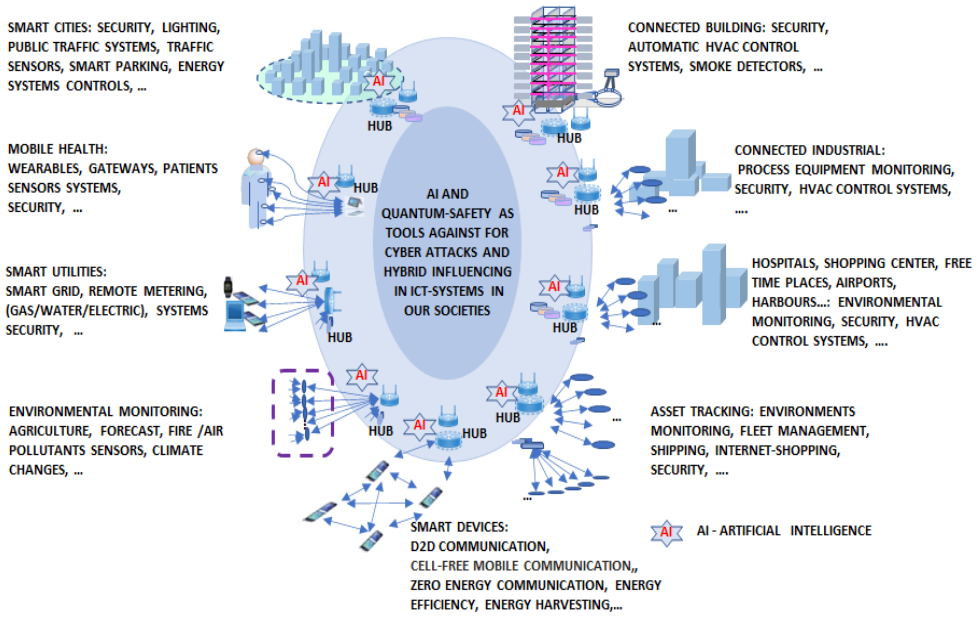

Figure 1. Example of our society's access and edge networks using AI and quantum encryption technologies (Aarne Hummelholm, 2022).

In our society, our devices and services are connected to each other and to other countries. This means a lot of threats and risks, and the situation gives cyber attackers more attack vectors. Threats range from denial-of-service attacks to a variety of new attack methods used everywhere to attack against infrastructures and services across now and in future virtualized and sliced data environments. Figure 1 shows one example of our society's access and edge networks.

1.3 Edge and access services.

Edge computing capabilities and innovations enable value creation and sustainable operations in different vertical use cases, such as smart cities, health, and logistics. Edge computing enhances user data processing in proximity to the point of use the data, introducing data centers functionalities close to the users, for example Multi-Access Edge Computing (MEC) (Hsieh et al., 2020) (ETSI, 2022). Edge access networks are also evolving to include residential and business environments, and mobile networks and virtualization solutions. Rapid development of edge and access technologies calls for more effective cybersecurity solutions than before. The cybersecurity challenges related to rapidly developing future edge and access services are being recognized, and there is a need for novel scalable, effective, and efficient cybersecurity solutions.

1.4 Critical infrastructures and Operational Service Technology (OT).

The services and the critical infrastructures of our digital society should be able to function during and recover from security incidents. Network intrusion by adversaries may lead to a variety of severe consequences from customer information leakage to a cascade of failures, such as massive blackout and destruction of infrastructures. Recent examples of attacks on OT include those suffered by Maersk, Norsk Hydro, SolarWinds, Triton, Stuxnet, as well as power grid attacks in Ukraine. More examples and alarming trends in frequency and sophistication of attacks can be found in the Digital and Cyberspace Policy program's cyber operations tracker – a database of the publicly known state-sponsored incidents that have occurred since 2005 (Cyber Operations Tracker). OT environments are experiencing a major change towards increased cybersecurity awareness (Aziz, A, et al., 2020).

1.5 Quantum safety is a must.

Quantum computing holds great promise for solving some of the most difficult computational problems. But quantum computing also has a dark side. The arrival of quantum computers is imminent and makes arithmetic asymmetric key exchanges unsafe. If data needs to be protected for five to ten years or more, it is necessary to implement quantum secure solutions. It takes up to ten years for countermeasures to be introduced (NICT, 2022). In general, most of the research and development work of the key players is focused on the level of algorithms; while one should think about the whole and that public safety must be considered right from the beginning of the design and development phase, considering the overall architecture and its future use cases. This requires applied research, quantum-safe migration should be possible in different usage scenarios.

1.6 Cybersecurity automation

The application scenarios of edge intelligence will lead to more complexity, with multiple stakeholders, and the growth of collected data, resulting to increased cybersecurity attack surface. Our vision is that especially automation and use of Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL) will bring competitive advantage in answering cybersecurity effectiveness, efficiency, and scalability challenges. Because of recent advances in computing power, AI in cybersecurity is now becoming a reality with comparatively small datasets. AI in cybersecurity no longer requires large structures of high-end servers with expensive processors to function, something that was critical just a few years ago.

2. Test and validation systems for cyber threats to the systems of edge intelligence networks of smart societies in the future.

The research aims for significant cybersecurity scalability, efficiency, and effectiveness of operations through improved and enhanced device and sensor securities, security assurance, quantum security, and artificial intelligence (AI)-based automation solutions, test, and simulation environment, figure 2.

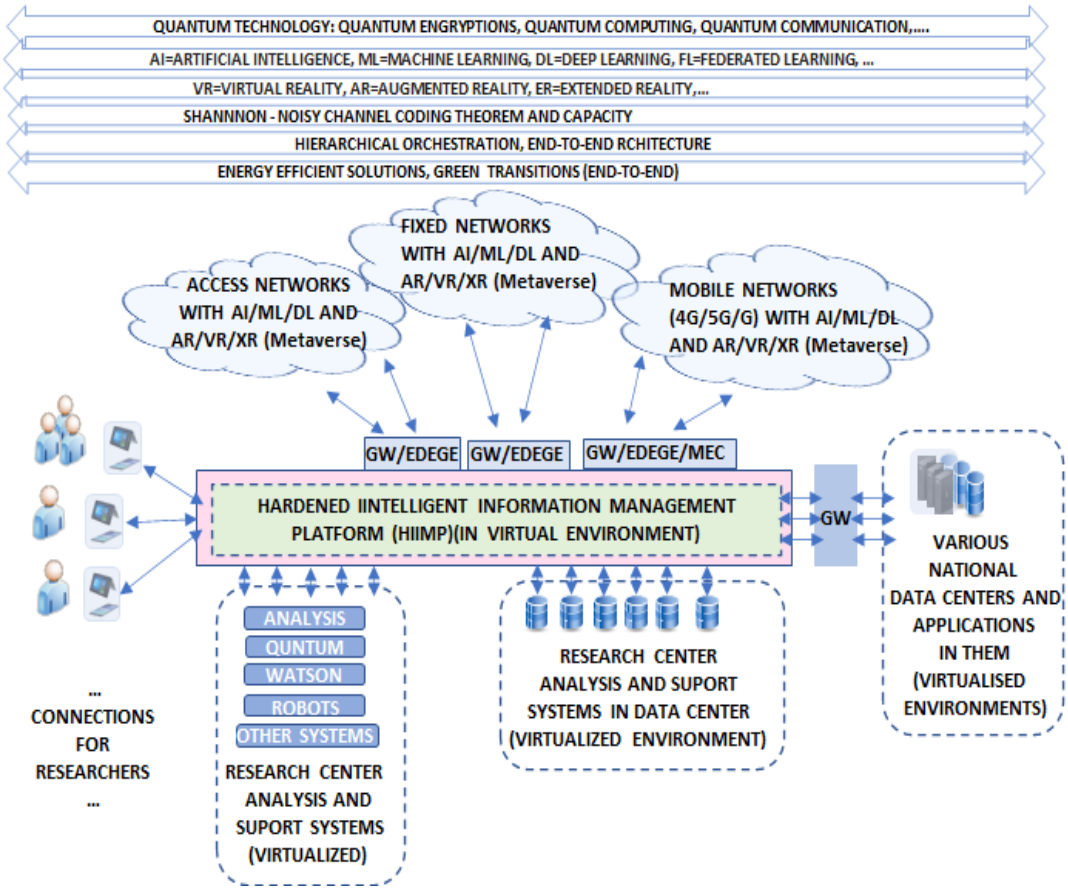

Figure 2. An envisioned security assurance test environment, where cybersecurity system integration reference model is in a core role and together with different simulators (Aarne Hummelholm, 2019).

3. Cyber threats to the systems of edge intelligence networks of smart societies in the future.

AIQUSEC project aims for enhanced device and sensor security, security assurance and artificial intelligence (AI)-based automation solutions, with quantum-safety migration capability. The project will design a leading-edge security assurance and validation environment for edge and access services, with a supporting cybersecurity system integration reference model, with a focus on architectural choices and connection of networks from different vertical use cases. The platform and reference model will enable building, testing, and validating joint cybersecurity capabilities. Attack vectors examples are below.

3.1 Attack vectors in communications networks and devices, figure 3:

- Access networks: Attacks to Mobile End Points, HUB, Smart Devices, IoT devices and sensors (DoS by Flooding, …) (DoS = Denial of Service)
- Attacks on the radio interface (DoS by Jamming) Attack from Physical access to gNodeB (gNodeB = Next Generation Node Base station), …
- Attacks with physical access to the transport Network (Man-in-the-middle attack, Eavesdropping, ...)
- Virtualization: Attacks by Third Party VNF (VNF = Virtual Network function) (Side Channel Attacks)
- Insider Attacks (Data Modification, Data Leakage), API based Attacks (API = Application Programming Interface)
- Attacks from untrusted non-3GPP network (3GPP = The 3rd Generation Partnership Project)
- Attacks from Roaming Network (Theft of Service, Eavesdropping)
- Attacks from Internet and other Networks, (Compromise of Network, DoS, …)

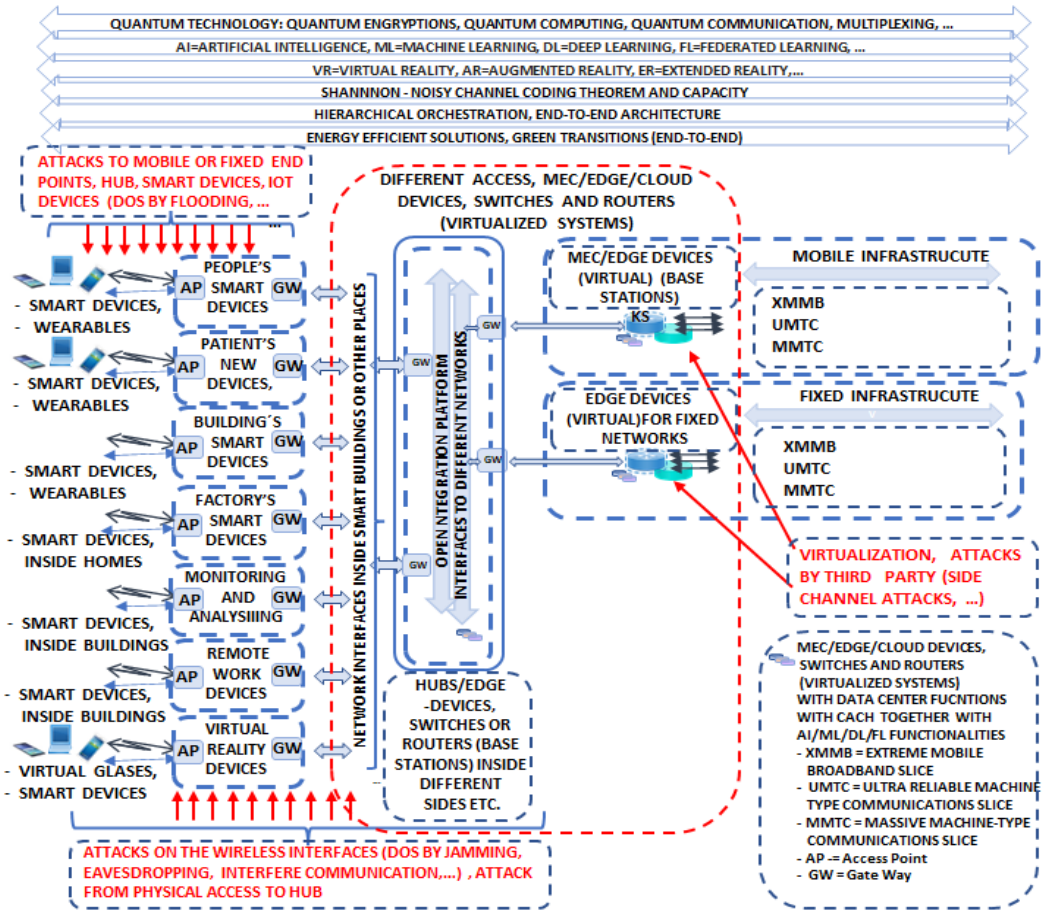

Figure 3. Example of communication systems of future access networks, using artificial intelligence methods and virtual reality interfaces including examples of attack vectors in different use cases (Aarne Hummelholm, 2021), (Ashutosh Dutta, 2021) (Chafika Benza, Tarik Taleb, 2020).

AI/ML/DL-specific threats, figure 3: (Andrew Marshall et al., 2022) (Amit Khullar, Anjani Kumar, 2020) SeukGue Hong et al.,2023)**.** Cyber attackers also use nowadays artificial intelligence methods. Taking advantage of sophisticated and intelligent technology solutions, they can attack everywhere and every system in both the software and physical domains etc.:

- Adversarial Perturbation
    - Targeted misclassification
    - Source/Target misclassification
    - Random misclassification
    - Confidence Reduction
    - Targeted Data Poisoning
    - Indiscriminate Data Poisoning
- Model Inversion Attacks
- Membership Inference Attack
- Model Stealing
- Neural Net Reprogramming
- Adversarial Example in the Physical domain (bits->atoms)
- Malicious ML providers who can recover training data
- Attacking the ML Supply Chain
- Backdoor Machine Learning
- Exploit software dependencies of the ML system
- …

The biggest security threats in using machine learning methods today are data poisoning due to a lack of methods and standards for treats detection and mitigation in this space, combined with reliance on untrusted/unvalidated used public datasets as data sources. Digital Twin and AI/ML/DL are used together to research, developing and optimization of different systems, processes, and services (Cem Dilmegani, 2023). These use cases must be considered also in our work.

AR/VR/XR environments threats, figure 3: (Jassim Happa et al., 2019) (Ben Dickson, 2018). AR (Augmented reality), VR (Virtual Reality) and XR (Extended Reality) devices and systems are used even more in different segments and functionalities of our smart societies. That means that cyber attackers will find ways to exploit vulnerabilities in virtual and augmented reality technology and will use them to infect devices and steal personal data and other types of sensitive data stored in the users' devices. It important to understand these vulnerabilities and find solutions for them. These are the most sensitive aspects which are identified so far:

- Ransomware Risks
- Fast Releases - Security Checks are maybe late
- Gaining Control of Devices
- Interference with AR Medical Devices
- Sabotaging VR/AR Shopping Apps…
- Social Engineering Attacks and must
- …

Metaverse is new working environment, which uses AR/VR/XR devices and systems, and it must consider also in our research and test environments (Metaverse, 2018).

4. Ethical considerations

- When AI is used in decision support automation, it needs to be interpretable, in order the general legitimacy and lack of public trust not to become the showstoppers of advanced automation. That would be unfortunate, as on the other hand AI automation could improve safety and security, by its accelerating effects to rapid response (to, e.g., detection of hazards to human lives in an ongoing mission). The project work studies AI capabilities that can be made transparent to the public safety agencies.

- Research integrity: The European Code of Conduct for Research Integrity (European Code of Conduct for Research Integrity of ALLEA) (All European Academies) and ESF (European Science Foundation) of March 2011 are followed.
- Experimentation subjects: N/A, no persons/animals involved.
- EU directives (EU GDPR, EU MDR, ...) must be considered and fulfilled.

5. International co-operation

International co-operation will be carried out daily throughout the project, in research publications and technical issues in co-operative networks. Specific planned co-operation includes also:

- Research exchanges (1) from JYU - University of Jyväskylä to NR – Norwegian Computing Centre (Oslo), concentrating on the cybersecurity system integration techniques and security metrics and measurements. (2) from JYU to Swiss company ID Quantique SA (Geneva), focusing on quantum-safety.
- Standardization of relevant parts of the reference model is planned to be opened as a standardization proposal. Direct collaboration with ISO/IEC JTC 1/SC 27 is planned. Moreover, the project activities link to IoT and digital twin standardization. Direct collaboration with ISO/IEC JTC 1/SSC 24 is planned. Arto Toppinen of Savonia is SESKO member and a project editor in several ISO/IEC SC41 groups related to IoT.
- Connect research cooperation between Savonia and JYU to iTrust – Centre for Research in Cyber Security (Singapore University of Technology and Design) in the critical infrastructure sector.

6. Conclusions

Answer to the main research question (MRQ): The requirements and fulfillment of a cyber-secure and hardened test and validation environment suitable for testing and analyzing various smart devices, sensors and systems are currently very challenging because information and communication infrastructures are changing rapidly.

In virtualized and sliced information and communication infrastructures services will be orchestrated end-to-end, which means that the same infrastructure's resources will be used and shared by different telecom operators, service providers, private operators, application providers, data center resource providers, service providers including many very critical areas service. These areas will be challenging for this project.

Many different smart devices, sensors, actuators, IoT devices, etc. are connected to our different information environments (pictures 1 - 3), and the devices' hardware and software are in different stages of their life cycle. This is a demanding and big challenge area in the whole project.

The big question is whether these companies participating in the research project have time to get sufficiently extensive information about future operating environments, their development, and challenges in this project time.

Enabling quantum-safe migration development is a clear goal of the research. This area of quantum technology is also one big challenge, because our project is quite short and is there enough time to develop devices and applications, considering the future cyber security challenges caused by quantum computing and AI?

This situation is a big new challenge for research partners, what to include now and what to leave for the next research phase.

7. Future work

One of the project's important future works is international cooperation, which is carried out daily throughout the project in research publications and technical issues in cooperation networks. The specially planned cooperation also includes research exchange, peer countries are selected for active research and business cooperation in the form of joint workshops and visits. The partners also conduct research in many highly critical areas in the field of telecommunications, cyber security, industrial automation, Smart City environments, the water sector and physical access solutions. In standardization issues, the standardization of the relevant parts of the reference model will be opened as a standardization proposal.

One of the project’s future works will be integrating new quantum-secure AI-based, hardware-based, and scalable cybersecurity solutions validated in a standardized way.

One of the project's future research works will be Metaverse and Mixed reality (MX) research.

In this research, we also must consider the coming EU directives that deal with artificial intelligence and its use in our operating environments (EU, Brussels, 21.4.2021).

Reference

Aarne Hummelholm, "Future Smart Societies' Infrastructures and services in the Cyber Environments", Springer, 2022, p. 151. – 182.

Aarne Hummelholm, modified from: "E-health systems in digital environments", ECCWS 2019.

Aarne Hummelholm, modified from "Cyber Security Analysis for Ships in Remote Pilotage Environment", ECCWS 2021.

Amit Khullar, Anjani Kumar, INFOSYS, Knowledge Institute," AI and ML in Cybersecurity Risk Management", Whitepaper, 2020, Available from: https://www.infosys.com/iki/perspectives/cybersecurity-risk-management.html

Andrew Marshall et al., Jugal Parikh, Emre Kiciman and Ram Shankar Siva Kumar," Threat Modelling AI/ML Systems and Dependencies", 11/02/2022, Available from: https://learn.microsoft.com/en-us/security/engineering/threat-modeling-aiml

Ashutosh Dutta, "5G Threat Vectors", IEEE, Future Network, Artificial Intelligence, and Machine Learning, 27-29.9.2021

Aziz, A.; Schelén, O.; Bodin, U., "A Study on Industrial IoT for the Mining Industry: Synthesized Architecture and Open Research Directions". IoT 2020, 1, 529-550, Available from: https://doi.org/10.3390/iot1020029

Ben Dickson, "Will AR and VR create new cybersecurity threats", February 6, 2018, Available from: https://bdtechtalks.com//2018/02/06/ar-vr-security-privacy-concerns/

Chafika Benza, Tarik Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler", 2020, Aalto University, University of Oulu, Finland

Cem Dilmegani, "Digital twins in 2023: What it is, Why it matters & Top Use Cases", AI-Multiple, January 2, 2023, Available from: https://research.aimultiple.com/digital-twins/

Cyber Operations Tracker is provided by Council on Foreign Relations, Available from: https://www.cfr.org/cyber-operations/#Glossary

ETSI, MEC security; Status of standards support and future evolutions, 2022, Available from: https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-46-2nd-Ed-MEC-security.pdf

EU, "LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS", Brussels, 21.4.2021, COM (2021) 206 final

EU-GDPR, The General Data Protection Regulation, 2016/679.

EU- MDR, The Medical Devices Regulation, 5/2017.

Hsieh et al., Liu, Guo, Gazda, Task Management for Cooperative Mobile Edge Computing, 2020 IEEE/ACM Symposium on edge computing (SEC), Available from: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=928585

Jassim Happa et al., Mashhuda Clencross, Anthohy Steed, "Cyber Security Threats and Challenges in Collaborative Mixed-Reality", 09 April 2019,University of Oxford and London, Available from: https://www.frontiersin.org/articles/10.3389/fict.2019.00005/full

Metaverse v.3.0, 2018, Available from: https://mvs.org/learn/.

NAII, About Artificial Intelligence, 2020, DIVISION E, SEC. 5001, Available from: https://www.ai.gov/about/#NAIAC_-_National_AI_Advisory_Committee

New Technologies– "Tempting Target for Cyber Criminals", Available from: https://arpost.co/category/technology/virtual-reality/

NICT (National Institute of Information and Communications Technology), "Overview of the functional structure of Beyond 5G/6G to achieve the SDGs and realize Society", 5.0, 18.02.2022,

Parachute Technology: "2022 Cyber-attack statistics, data and trends", Available from: https://parachutetechs.com/2022-cyber-attack-statistics-data-and-trends/

Roger G. Massmann et al., Nick M. Grantham, Akalanka B. Mailewa," Quantum Computing: An Assessment into the Impacts of Post-Quantum Cryptography", Saint Cloud State University, St. Cloud, Minnesota, 2023, Available from: https://www.researchgate.net/publication/369776982

SeukGue Hong et al., HyungBin Seo, MyungKeun Yoon, "Data Auditing for Intelligent Network Security Monitoring", IEEE Communications Magazine, March 2023

Water/wastewater utilities leveraging IIoT, Available from: https://iiot-world.com/connected-industry/water-wastewater-utilities-leveraging-iiot/