The Dependability of 6G Networks

Subjects: Telecommunications

Contributor: Ijaz Ahmad , Felipe Rodriguez , Jyrki Huusko , Kari Seppänen

The sixth-generation (6G) communication networks must be highly dependable due to the foreseen connectivity of critical infrastructures through these networks. Dependability is a compound metric of four well-known concepts—reliability, availability, safety, and security.

6G dependability security reliability availability safety

1. Introduction

The fifth-generation (5G) wireless networks brought innovative technological concepts into the wireless domain that closed the gap between traditional IT domains and communication networks. For example, cloudification and softwarization of networking technologies enabled deploying new use cases and applications in wireless networks. Technologies from the physical layer, such as massive multi-input multi-output (MIMO), to the application layer, such as machine learning (ML) technologies, have increased networks' capacities and capabilities. However, 5G cannot meet the requirements of emerging services such as the Internet of Everything (IoE), due to the inherent limitations of 5G systems [1]. The sixth-generation (6G) communications networks will take a huge leap beyond 5G in order to meet the needs of future services and societies, which will be centered around data centric, intelligent, and automated processes [2]. Novel disruptive technologies in the domains of terahertz and optical communications, cell-less coverage through integrated terrestrial-satellite access technologies [3], distributed end-user terminal-based artificial intelligence (AI) [4][5], and distributed ledger technologies (DLTs) [6], to name a few, will converge to fulfill the needs of emerging applications and use cases [7].

6G is expected to ignite a human transformation, thanks to improved context-aware devices with new human–machine interfaces provided by end-devices that are no longer mere data collectors, but multiple synchronized entities working in unison. This will dramatically improve the way we interact with both the physical and digital worlds. Such services will have have stringent quality of service (QoS) requirements in terms of bandwidth, reliability, and latency that will be challenging for existing 5G networks to provide. For example, ubiquitous and universal computing with resources distributed locally and in the cloud, knowledge systems that store and convert data into actions, and efficient sensing for controlling the physical world cannot be provided in 5G, and thus, focus is put on 6G research. Sixth-generation networks are also envisioned to provide massive-scale connectivity, 3D networking, real-time immersion through extended reality (XR), and haptic applications [8].

To stand on the envisioned promises, 6G must be highly distributed to meet the needs of latency, reliability, and availability of critical services, such as industrial automation systems, UAVs, and autonomous systems. Distributed clouds—edge, fog, and cloudlets [9]—will play a crucial role in providing the necessary computing and storage resources for distributed 6G. Softwarization of network functions and services will enable distributing important services to different network perimeters. Similarly, distributed AI in the distributed network will overcome challenges related to latency, reliability, data criticality, and privacy in 6G [10][11].

Reliability is the probability of a system working correctly for a certain period of time. As 6G networks will be highly distributed, the main concern regarding reliability is effectively coordination of the computing nodes. In order to achieve this, successful communication protocols between those computing nodes are needed, along with a reliable underlying network capable of supporting the amount of traffic generated by storing and retrieving data [12]. Availability refers to the probability of a system working properly at any given time. Distributed AI solutions for 6G networks are an attractive option for improving learning time while reducing resource consumption, and thereby improving the availability of AI-based systems and services. Form factor is an important variable, since it limits the resources, including energy, available for communication with external, distributed solutions. Security refers to capacity of a system for protecting itself by promptly identifying threats, and taking actions that effectively protect the services deployed on the system and data exchanged among the components and users. In the case of 6G network services, distributed AI/ML algorithms are needed to train models locally for threat identification and mitigation, in order to preserve the end user information. Finally, safety refers to the ability of a system to avoid harming human life, the environment, or private property.

2. Dependability

Dependability is the ability of a system to deliver a service that can justifiably be trusted; in other words, it should avoid frequent and severe service failures [13]. Though crucial in importance, dependability is often overlooked in favor of other research directions. Priority has been given to coordinating computing activities between distributed nodes in order to achieve higher performance, or security mechanisms that help in protecting users and their data. As previously mentioned, dependability is a compound metric and can be discussed through four important indicators: reliability, availability, safety, and security. Although performance and security are important, and as such most of the works focus on them, the other three requirements of dependable systems should not be underestimated [14][15]. Moreover, there are many facets of dependability, for instance, confidentiality and integrity [16]. However, some of the concepts converge into the four aspects discussed throughout this entry.

2.1. Reliability

The complexity of distributed edge networks means that achieving reliability in such an environment is not an easy task. With the increasing number of MCAs solutions on the market, requirements for reliable systems are indispensable, and furthermore, still a challenge to achieve. Rapid changes in computing environments also bring challenges to reliability, for example, asynchronism, heterogeneity of software/hardware, scalability, and fault tolerance, to mention some. In [17], the authors briefly explored reliability issues in edge AI systems and proposed an architecture that meet latency and reliability requirements for many MCAs. It is identified that computation on edge systems occur in three different layers: bottom (end devices), middle (servers), and top (centralized cloud). In order to achieve good communication and a fast response, all three layers must be properly synchronized, like the storing and data access for processing [12].

2.2. Availability

Availability is realized once reliability has been achieved. Reliability is the probability that the system is working, and availability is the probability of it working at a given time. Availability ensures that no denial of authorized access to the system occurs [18]. The advantage of distributed systems is that additional nodes and communication paths help hiding any failure that might exists. Current research trends in edge computing aim at improving system availability by carefully planning task and data offloading from end devices towards edge servers with frameworks that are even capable of performing the offloading based on network statistics and the edge servers' computation capabilities. Another characteristic helping availability is the reassignment of tasks from failing nodes, although common node failures are still a problem, since a task that crashes a node can be moved to another node and causes the same type of crash. Since availability and reliability work together, it is important to notice they can also work at cross purposes; with this in mind, both concepts must be weighted against one another, as different systems might require a different degree of each.

2.3. Safety

Safety is critical for MCAs, especially in use cases where human lives are at danger, such as autonomous driving and telesurgery. The IEC 60601 [18]. which is a technical standard for the safety and performance of the medical electrical equipment, defines safety as the avoidance of any hazards due to the operation of a device under normal or single-fault conditions. However, this definition can be broadened to cover non-medical domains, thereby including faulty conditions such as wrong lane selection in autonomous driving, or task offloading failure affecting the information given to the end user, or creating distractions in an augmented reality application. The current trend in communication networks is to simplify safety through the development of bug-free software or through an AI-based optimization problem. It is necessary to study the interaction between the composing cyberphysical systems (CPS) and the environment of each use case [19]. In [20][21], telesurgery safety considerations from the medical point of view are given. It also mentions their experience with different surgical robots and elaborates on some comparisons.

2.4. Security

Security is one of the main issues in communication networks, as both nodes and the whole network are attacked by malicious users [22][23]. The distributed and data-driven nature of future 6G communication networks and its use cases mean more data, and of course, a wider attack surface. The applications of AI or ML in communications networks are increasing at a higher pace due to apparent reasons [24]; however, AI and ML also bring their own security challenges in communications networks, as elaborated in [25][26]. The most important part is to identify the required level of security for a certain use case and adopt the principles of the security-by-design approach. These concepts are quite important due to the diverse nature of 6G MCAs. Furthermore, the rise in the number of capable attackers targeting communication networks call for stringent security requirements. In [27], the schoolars explore the application of blockchain technology alongside ML in order to protect vehicular networks from cyber attacks.

3. 6G and Dependability

3.1. Brief Introduction to 6G Networks

The rapid development of multimedia applications for use cases such as high-fidelity holograms, tactile Internet, and the support of MCAs require a higher bandwidth, lower latency, and higher reliability than that offered by the current 5G communication networks [28][29]. Therefore, 6G aims to fulfill these requirements through base-station densification (mmWave and terahertz tiny cells, temporary hotspots) with other means for distribution of network functions, such as extended edge computing, and exploration of higher frequencies above 300 GHz, as discussed in [1]. The resulting 6G networks, thus, will be expected to provide more than just communications, i.e., to interconnect communication, computing, and sensing technologies with the physical, biological, and cyber worlds, thereby acting as distributed neural networks that will enable intelligence of everything. Sixth-generation networks will transform the way we communicate, from connected people and devices to connected intelligence. This means bringing intelligence closer to every person, home, or business, for example, in the form of edge intelligence. Therefore, 6G networks are bound to be large-scale, use heterogeneous access with cell-free or cell-less coverage, and dynamic with heavily-distributed storage and computation capabilities [30].

The transition from 5G to 6G requires changes not only in bandwidth, but from the physical to the application layer in order to meet the new requirements of emerging services, such as the Internet of Everything (IoE) [31]. Furthermore, 6G networks are expected to achieve data rates in the range of terabits per second, thanks to the developments in terahertz communications; and improvements in massive MIMO, beamforming, and novel coding schemes. A successful combination of these next-generation wireless networks with cloud, edge, and fog platforms is vital in order to realize increased network intelligence. To meet the requirements of latency and privacy, bringing cloud platforms closer to the sources of data, for instance, in the far edge, will be inevitable. Edge intelligence [17][32] thus opens up new horizons for achieving and exploiting the full potential of 6G networks.

Since the first generation (1G), the complexity of communication networks have increased while expanding both horizontally and vertically, thereby rendering them difficult to manage. Furthermore, along with complexity, the security threat landscape has also increased constantly [22]. Edge computing can play an important role in addressing both of these challenges, i.e., complexity and security. By devolving control into multiple control units, compared to centralized ones, security through redundancy can be increased as a general phenomenon. For instance, the chances of single points of failure, and of a single target for denial of service (DoS) and resource exhaustion attacks, are highly complicated in such distributed environments. Furthermore, edge computing plays a vital role in 6G communication networks, as it provides the computing the resources necessary for carrying out management and analysis close to end-users' devices [33].

Fast and focused data processing through edge computing is the cornerstone of applications in 6G, for example, in vehicle-to-everything communications [34]. In-depth data analysis could be carried out by the centralized cloud at the expense of delays [35]. **Figure 1** shows a simplified architecture of an AI-based 6G network, which is divided into three parts: user environment, networks, and management and control. In the management and control, functions such as parameter optimization, resource management, and task scheduling are carried out. In the network part, some of the tasks performed are data filtering, knowledge discovery, and feature extraction for data analytics, besides the usual network layers' work. Finally, in the user's environment, all the sensing, monitoring, and data collection occurs. The increase in data volumes being processed at the edge of the network represents a difficulty in properly identifying useful data for a primary analysis, prior to passing them to the centralized cloud. These requirements have paved the way to the intelligentization of the edge computing, referred to now as edge intelligence or EdgeAI [36], transforming it into a AI-based platform capable of offering intelligent services [37]. In order to achieve this, research hs departed from the centralized cloud-based approach, sparkling an interest in distributed, low-latency, and reliable AI at the edge [38][39].

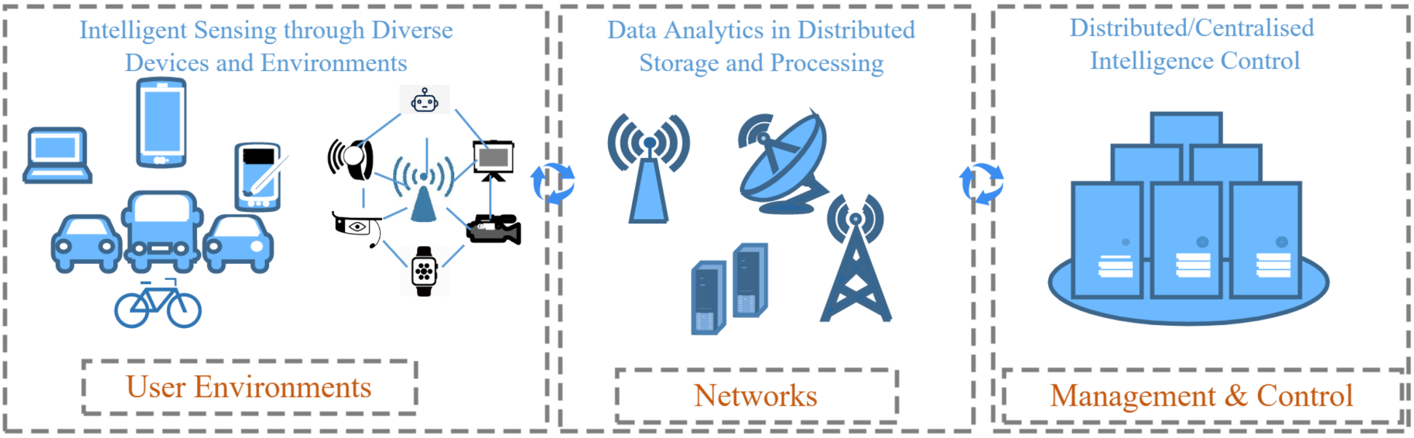
Intelligent Sensing through Diverse Devices and Environments
User Environments
Data Analytics in Distributed Storage and Processing
Networks
Distributed/Centralised Intelligence Control
Management & Control

Figure 1. An abstract representation of enabling intelligence in 6G networks.

3.2. Dependability in 6G Networks

3.2.1. Reliability

Sixth-generation networks are expected to offer extremely high reliability. EdgeAI supports the vision of 6G through offering more computational power near users or services while reducing overall latency. Reliability requires checking the necessary requirements instead of assuming that these are fulfilled and constantly monitoring the network [40]. Although in terms of performance, EdgeAI supposes a step forward, its distributed nature, combined with the high number of servers required, might well introduce other issues. First, there has asynchronism. As the number of edge servers rises, they are also expected to be capable of working in unison; this means being synchronized. Synchronization is improved when servers are aware of the status of neighboring servers; in other words, the exchange of information, such as available memory or processing power, is shared in a timely manner.

Another issue is the heterogeneity of software and hardware at the nodes. Although it brings benefits in the long run, the adoption of heterogeneous solutions might also pose challenges. As an example, heterogeneous EdgeAI servers might have different power consumption and performance levels due to non-identical CPU architectures. In the same manner, distinct feature support could hinder synchronism. Scalability could also be a problem for networks, as it increases the complexity of management, and it might also create issues with synchronism. As 6G networks will be highly scalable, fault tolerance is also important in order to ensure reliability. As a system scales to be hundreds of nodes in size, a fault tolerant system will enable the operations or services to continue at a reduced level, though not stopping completely.

3.2.2. Availability

Availability is the assurance of access to services and resources by legitimate users, or the quality of being ready or present for immediate use [41]. As mentioned in Section 2, reliability and availability are both intertwined. As a combination of highly distributed systems, 6G networks will be capable of dissimulating failures at the edge servers by rapidly offloading the assigned processes towards a nearby server that possesses the required resources. In the context of EdgeAI, if an edge server fails, then its tasks are offloaded towards a neighboring edge. This is where synchronism plays a major role, and in order to achieve this, servers must be aware of the status of each other.

3.2.3. Safety

Safety and security, looking intertwined, are highly complicated in terms of defining their roles in communications networks. Safety, also defined similarly in [42], is a system's characteristic of preventing losses due to unintentional actions by normal, non-harmful actors. Security, on the other hand, relates to deliberate actions (mostly harmful) by deliberate actors. Safety in 6G communications networks can be achieved by taking several measures that are also related to security, which are discussed in the following security part. Aside from foolproof security, safety can be achieved by improving monitoring and response systems, increasing multiplicity or redundancy, and distributing important control functions throughout the network. EdgeAI thus plays a very important role in providing opportunity for redundant resources and distributing important network control functions. The concept of devolving control functions, with the help of miniaturizing edge to the extreme, as discussed in [43], can improve safety in terms of minimizing the impact of failures and delimiting the consequences.

3.2.4. Security

As one of the main concerns regarding modern networks, security in 6G is of paramount importance. Novel technologies in 6G networks will also introduce new security concerns. TeraHertz (THz) technology, which is believed to hinder the ability of malicious users to perform eavesdropping; however, recent research has shown it is still possible, although difficult, to intercept the signals, even when transmitted with narrow beams [44]. Quantum communications are also expected to make a significant contribution in 6G networks, mainly from the perspectives of communications security, such as quantum and post quantum cryptography [45]. Nevertheless, the technology is still at its infancy, and although many advances have been made in the quantum cryptography field, there are still issues regarding operation errors in long distance communications. Furthermore, quantum computing can raise significant challenges to existing cryptographic security protocols [46].

4. Machine Learning, Dependability, and 6G

AI and its major branch, ML, will shape 6G networks [24][30]. Due to its tight QoS requirements, future 6G networks will posses such a complex architecture that performing legacy network operations will be deemed unsound. For this, ML techniques are emerging as a response to achieve truly intelligent orchestration and network management [47]. The dynamic nature of communication networks provides data for ML-enabled spectrum management and channel estimation, which are the basis of ultra-broadband techniques. Additionally, ML is being used to improve security, resource allocation, mobility management, and low-latency services in MCAs [24]. In particular, ML techniques such as deep learning have proved to be extremely efficient in preventing serious security attacks, such as distributed DoS attacks [48]. Distributed ML will be highly important in 6G due to the emerging needs of distributed processing at the edges of the network [49]. FL is currently among the most used distributed ML techniques in communication networks [32][50] and is highly important for 6G due to its ability to be used in a distributed manner, much like the foreseen distributed control nature of 6G networks.

Reliability

ML techniques rely heavily on data. Data quality is fundamental for achieving high accuracy during the learning task. Client selection is a critical issue in FL, as clients are the ones updating the local models previous to the global aggregation, it is fundamental to properly select the clients that train the models using the highest quality of data. Most of the FL systems select their clients in a random manner, or based on resource conditions. Such selection of course might affect the global performance, as non-trustable nodes can also be selected. Moreover, the complexity of conceiving client selection in a communications network due to its dynamic nature also hinders their reliability. Even further, as it is difficult for the centralized entity that performs the selection to actually monitor a large-scale behavior, the selected untrustable clients are unlikely to be removed.

Availability

A lack of, or improper, criteria when selecting the clients for local training does not only affect reliability, but availability also. Untrusted clients using low quality data for training hinders the whole learning process and may severely affect predictions. In this manner, a FL framework whose accuracy is not as desired cannot be deployed, nor can services trust it, thereby rendering it unavailable. Availability in FL systems is complex to achieve due to the distributed nature of the model training, and the centralization of global model aggregation; in other words, it is not possible to hide a “faulty” or badly trained model when several untrusted clients have performed training with corrupted data.

Safety

Damage done by the selection of untrusted clients goes further than that of a faulty or badly trained model. Since learning is crucial for many use cases, untrusted clients might hinder the prediction capacity of a system. This can cause safety-related issues for users. It can consider an autonomous vehicle with an positioning model based on FL, which is trained collectively with other autonomous vehicles. If a malicious vehicle is allowed to send its trained model for aggregation, this could affect the driving decisions of other vehicles, putting the passengers' lives at risk. The problem is only exacerbated by the centralization issue raised in the previous subsection, where weak aggregation algorithms do not help discriminating good from bad trained models.

Security

Security is an important challenge in ML [25]. Even when FL improves user data privacy, security is still a main concern. An untrusted client that is selected to participate in a FL round could perform attacks, such as maliciously using unreliable data or injecting false data. Additionally, a malicious client could also launch attacks alongside other malicious users aimed at increasing misclassification. False-data injection refers to clients purposely adding wrong data to the training sets. On the other hand, workers might unintentionally provide low-quality raw data due to constraints in energy or high-speed mobility.

5. Dependability for MCAs in 6G

One of the primary focus of 6G networks is MCAs. These applications usually require dependable services in terms of latency and error rates, and due to their nature, this must be equivalent to wired networks. The requirements of MCAs are closely related to those of Ultra-Reliable Low-Latency Communications (URLLC) with a target latency of 0.1 ms and a block error rate (BLER) of 10−9

Although these KPI values are not applicable to all use cases, they do have practical relevance in a couple of them. It could mention autonomous driving, remote surgery, and augmented reality [51]. Needless to say, MCAs also mandate high-security communications and resource efficiency. Current 5G networks' approaches for meeting the requirements of MCAs based on tweaking the system design is not scalable, nor efficient. Future 6G networks need to make use of application-domain information in order to predict actual resource requirements. Furthermore, 6G networks need to introduce new parameters that will not only help with characterizing resource needs but will also ease dependability analysis [52].

Due to its performance, edge computing is gaining traction as a viable solution for meeting the requirements of MCAs. The drivers behind the adoption of edge computing in MCAs use cases are the amount of data being transferred between end devices and edge servers, and time taken for data processing at the edge server. Due to the proximity of the edge server to the source of data, the network requirements mentioned at the beginning of this subsection could be met, even in the scenario of a massive amount of data. Furthermore, edge intelligentization eases meeting these requirements, as it is capable of offering micro-interaction with end devices, bringing management much closer to them, thereby reducing the communications overhead due to data fetching and controlling [24].

References

1. Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. IEEE Netw. 2020, 34, 134–142.
2. Giordani, M.; Polese, M.; Mezzavilla, M.; Rangan, S.; Zorzi, M. Toward 6G Networks: Use Cases and Technologies. IEEE Commun. Mag. 2020, 58, 55–61.
3. Ahmad, I.; Suomalainen, J.; Porambage, P.; Gurtov, A.; Huusko, J.; Höyhtyä, M. Security of Satellite-Terrestrial Communications: Challenges and Potential Solutions. IEEE Access 2022, 10, 96038–96052.
4. AbdulRahman, S.; Tout, H.; Ould-Slimane, H.; Mourad, A.; Talhi, C.; Guizani, M. A survey on federated learning: The journey from centralized to distributed on-site learning and beyond. IEEE Internet Things J. 2021, 8, 5476–5497.
5. Peltonen, E.; Bennis, M.; Capobianco, M.; Debbah, M.; Ding, A.; Gil-Castiñeira, F.; Jurmu, M.; Karvonen, T.; Kelanti, M.; Kliks, A.; et al. 6G white paper on edge intelligence. arXiv 2020, arXiv:2004.14850.
6. Sekaran, R.; Patan, R.; Raveendran, A.; Al-Turjman, F.; Ramachandran, M.; Mostarda, L. Survival Study on Blockchain Based 6G-Enabled Mobile Edge Computation for IoT Automation. IEEE Access 2020, 8, 143453–143463.
7. Nawaz, S.J.; Sharma, S.K.; Mansoor, B.; Patwary, M.N.; Khan, N.M. Non-Coherent and Backscatter Communications: Enabling Ultra-Massive Connectivity in 6G Wireless Networks. IEEE Access 2021, 9, 38144–38186.
8. Bariah, L.; Mohjazi, L.; Muhaidat, S.; Sofotasios, P.C.; Kurt, G.K.; Yanikomeroglu, H.; Dobre, O.A. A Prospective Look: Key Enabling Technologies, Applications and Open Research Topics in 6G Networks. IEEE Access 2020, 8, 174792–174820.
9. Ren, J.; Zhang, D.; He, S.; Zhang, Y.; Li, T. A Survey on End-Edge-Cloud Orchestrated Network Computing Paradigms: Transparent Computing, Mobile Edge Computing, Fog Computing, and Cloudlet. ACM Comput. Surv. 2019, 52.
10. Hashima, S.; Fadlullah, Z.M.; Fouda, M.M.; Mohamed, E.M.; Hatano, K.; ElHalawany, B.M.; Guizani, M. On Softwarization of Intelligence in 6G Networks for Ultra-Fast Optimal Policy Selection: Challenges and Opportunities. IEEE Netw. 2022, 1–9.
11. Letaief, K.B.; Shi, Y.; Lu, J.; Lu, J. Edge Artificial Intelligence for 6G: Vision, Enabling Technologies, and Applications. IEEE J. Sel. Areas Commun. 2022, 40, 5–36.

12. Ahmed, W.; Wu, Y.W. A survey on reliability in distributed systems. J. Comput. Syst. Sci. 2013, 79, 1243–1255.
13. Avizienis, A.; Laprie, J.C.; Randell, B.; Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable Secur. Comput. 2004, 1, 11–33.
14. Heimann, D.I.; Mittal, N.; Trivedi, K.S. Dependability modeling for computer systems. In Proceedings of the Annual Reliability and Maintainability Symposium, Orlando, FL, USA, 29–31 January 1991; pp. 120–128.
15. Chen, D.; Garg, S.; Kintala, C.M.; Trivedi, K.S. Dependability Enhancement for IEEE 802.11 Wireless LAN with Redundancy Techniques. In Proceedings of the Dependable Systems and Networks, San Francisco, CA, USA, 22–25 June 2003; pp. 521–528.
16. Laprie, J.C. Dependable computing: Concepts, limits, challenges. In Proceedings of the Special issue of the 25th International Symposium on Fault-Tolerant Computing, Pasadena, CA, USA, 27–30 June 1995; pp. 42–54.
17. Gupta, R.; Reebadiya, D.; Tanwar, S. 6G-enabled Edge Intelligence for Ultra -Reliable Low Latency Applications: Vision and Mission. Comput. Stand. Interfaces 2021, 77, 103521.
18. Ahmad, I.; Namal, S.; Ylianttila, M.; Gurtov, A. Security in Software Defined Networks: A Survey. IEEE Commun. Surv. Tutorials 2015, 17, 2317–2346.
19. Banerjee, A.; Venkatasubramanian, K.K.; Mukherjee, T.; Gupta, S.K.S. Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems. Proc. IEEE 2012, 100, 283–299.
20. Raytis, J.L.; Yuh, B.E.; Lau, C.S.; Fong, Y.; Lew, M.W. Anesthetic Implications of Robotically Assisted Surgery with the Da Vinci Xi Surgical Robot. Open J. Anesthesiol. 2016, 6, 115–118.
21. Rim, L.J. Anesthetic considerations for robotic surgery. Korean J. Anesth. 2014, 66, 3–11.
22. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and beyond. IEEE Commun. Surv. Tutor. 2019, 21, 3682–3722.
23. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G security challenges and solutions. IEEE Commun. Stand. Mag. 2018, 2, 36–43.
24. Ahmad, I.; Shahabuddin, S.; Malik, H.; Harjula, E.; Leppänen, T.; Lovén, L.; Anttonen, A.; Sodhro, A.H.; Mahtab Alam, M.; Juntti, M.; et al. Machine Learning Meets Communication Networks: Current Trends and Future Challenges. IEEE Access 2020, 8, 223418–223460.
25. Suomalainen, J.; Juhola, A.; Shahabuddin, S.; Mämmelä, A.; Ahmad, I. Machine learning threatens 5G security. IEEE Access 2020, 8, 190822–190842.
26. Ahmad, I.; Shahabuddin, S.; Sauter, T.; Harjula, E.; Kumar, T.; Meisel, M.; Juntti, M.; Ylianttila, M. The Challenges of Artificial Intelligence in Wireless Networks for the Internet of Things: Exploring

Opportunities for Growth. IEEE Ind. Electron. Mag. 2020, 15, 16–29.

27. Dibaei, M.; Zheng, X.; Xia, Y.; Xu, X.; Jolfaei, A.; Bashir, A.K.; Tariq, U.; Yu, D.; Vasilakos, A.V. Investigating the Prospect of Leveraging Blockchain and Machine Learning to Secure Vehicular Networks: A Survey. IEEE Trans. Intell. Transp. Syst. 2021, 23, 683–700.
28. Zhang, Z.; Xiao, Y.; Ma, Z.; Xiao, M.; Ding, Z.; Lei, X.; Karagiannidis, G.K.; Fan, P. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. IEEE Veh. Technol. Mag. 2019, 14, 28–41.
29. David, K.; Berndt, H. 6G Vision and Requirements: Is There Any Need for Beyond 5G? IEEE Veh. Technol. Mag. 2018, 13, 72–80.
30. Tariq, F.; Khandaker, M.R.A.; Wong, K.K.; Imran, M.A.; Bennis, M.; Debbah, M. A Speculative Study on 6G. IEEE Wirel. Commun. 2020, 27, 118–125.
31. Nezami, Z.; Zamanifar, K. Internet of ThingsInternet of Everything: Structure and Ingredients. IEEE Potentials 2019, 38, 12–17.
32. Wang, X.; Han, Y.; Wang, C.; Zhao, Q.; Chen, X.; Chen, M. In-Edge AI: Intelligentizing Mobile Edge Computing, Caching and Communication by Federated Learning. IEEE Netw. 2019, 33, 156–165.
33. Pham, Q.V.; Fang, F.; Ha, V.N.; Piran, M.J.; Le, M.; Le, L.B.; Hwang, W.J.; Ding, Z. A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art. IEEE Access 2020, 8, 116974–117017.
34. Osorio, D.P.M.; Ahmad, I.; Sánchez, J.D.V.; Gurtov, A.; Scholliers, J.; Kutila, M.; Porambage, P. Towards 6G-enabled Internet of Vehicles: Security and Privacy. IEEE Open J. Commun. Soc. 2022, 3, 82–105.
35. Okwuibe, J.; Haavisto, J.; Kovacevic, I.; Harjula, E.; Ahmad, I.; Islam, J.; Ylianttila, M. SDN-Enabled Resource Orchestration for Industrial IoT in Collaborative Edge-Cloud Networks. IEEE Access 2021, 9, 115839–115854.
36. Zhou, Z.; Chen, X.; Li, E.; Zeng, L.; Luo, K.; Zhang, J. Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing. Proc. IEEE 2019, 107, 1738–1762.
37. Deng, S.; Zhao, H.; Fang, W.; Yin, J.; Dustdar, S.; Zomaya, A.Y. Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence. IEEE Internet Things J. 2020, 7, 7457–7469.
38. Li, C.; Guo, W.; Sun, S.C.; Al-Rubaye, S.; Tsourdos, A. Trustworthy Deep Learning in 6G-Enabled Mass Autonomy: From Concept to Quality-of-Trust Key Performance Indicators. IEEE Veh. Technol. Mag. 2020, 15, 112–121.

39. Harjula, E.; Karhula, P.; Islam, J.; Leppänen, T.; Manzoor, A.; Liyanage, M.; Chauhan, J.; Kumar, T.; Ahmad, I.; Ylianttila, M. Decentralized IoT edge nanoservice architecture for future gadget-free computing. IEEE Access 2019, 7, 119856–119872.
40. Herlich, M.; Maier, C. Measuring and Monitoring Reliability of Wireless Networks. IEEE Commun. Mag. 2021, 59, 76–81.
41. Bhagwan, R.; Savage, S.; Voelker, G.M. Understanding availability. In Proceedings of the International Workshop on Peer-to-Peer Systems, Berkeley, CA, USA, 21–22 February 2003; Springer: Berlin/Heidelberg, Germany; pp. 256–267.
42. Young, W.; Leveson, N.G. An integrated approach to safety and security based on systems theory. Commun. ACM 2014, 57, 31–35.
43. Ahmad, I.; Lembo, S.; Rodriguez, F.; Mehnert, S.; Vehkaperä, M. Security of Micro MEC in 6G: A Brief Overview. In Proceedings of the 2022 IEEE 19th Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022; pp. 332–337.
44. Ma, J.; Shrestha, R.; Adelberg, J.; Yeh, C.Y.; Hossain, Z.; Knightly, E.; Jornet, J.M.; Mittleman, D.M. Security and eavesdropping in terahertz wireless links. Nature 2018, 563, 89–93.
45. Song, F. A note on quantum security for post-quantum cryptography. In Proceedings of the International Workshop on Post-Quantum Cryptography, Waterloo, ON, Canada, 23 September 2014; pp. 246–265.
46. Omolara, A.E.; Alabdulatif, A.; Abiodun, O.I.; Alawida, M.; Alabdulatif, A.; Alshoura, W.H.; Arshad, H. The internet of things security: A survey encompassing unexplored areas and new insights. Comput. Secur. 2022, 112, 102494.
47. Khan, L.U.; Pandey, S.R.; Tran, N.H.; Saad, W.; Han, Z.; Nguyen, M.N.H.; Hong, C.S. Federated Learning for Edge Networks: Resource Optimization and Incentive Mechanism. IEEE Commun. Mag. 2020, 58, 88–93.
48. Mittal, M.; Kumar, K.; Behal, S. Deep learning approaches for detecting DDoS attacks: A systematic review. Soft Comput. 2022, 1–37.
49. Mwase, C.; Jin, Y.; Westerlund, T.; Tenhunen, H.; Zou, Z. Communication-efficient distributed AI strategies for the IoT edge. Future Gener. Comput. Syst. 2022, 131, 292–308.
50. Liu, Y.; Yuan, X.; Xiong, Z.; Kang, J.; Wang, X.; Niyato, D. Federated learning for 6G communications: Challenges, methods, and future directions. China Commun. 2020, 17, 105–118.
51. Mahmood, N.H.; Böcker, S.; Munari, A.; Clazzer, F.; Moerman, I.; Mikhaylov, K.; López, O.L.A.; Park, O.; Mercier, E.; Bartz, H.; et al. White Paper on Critical and Massive Machine Type Communication Towards 6G. arXiv 2020, arXiv:2004.14146.

52. She, C.; Dong, R.; Gu, Z.; Hou, Z.; Li, Y.; Hardjawana, W.; Yang, C.; Song, L.; Vucetic, B. Deep Learning for Ultra-Reliable and Low-Latency Communications in 6G Networks. IEEE Netw. 2020, 34, 219–225.

Retrieved from https://encyclopedia.pub/entry/history/show/98275