# Trend Reports
# Seminar on Machine Intelligence
# Winter Semester 21/22

Klaus Diepold, Sven Gronauer, Mohamed Ali Tnani, Michael Zwick (Eds.)

April 6, 2022

# Abstract

This book is the product of a one-semester course called *Seminar Machine Intelligence* which was held in the winter term 21/22 at the Technical University Munich. The purpose of the course was to study the intersection between *Machine Intelligence and 6G telecommunication technology* and outline possible future trends in this domain.

Nowadays, not only researchers are enthusiastic about the topic of machine intelligence but also a widespread public. More and more longstanding problems in manifold areas such as natural language and computer vision become tractable, it is evident that machine intelligence as technology will play a crucial role in society, industry, and the environment in the foreseeable future. As we shall expect major changes, we asked ourselves the question: "To what extent do a higher data availability, larger data throughput, and an increased diversity of connected devices affect the future of machine intelligence?"

The students participating in the seminar tried to discuss exactly this question in the winter term 21/22. The students examined the status quo of machine learning methods in the context of 6G and give insights into fields such as federated learning and generalization as well as their applications and the impact on the industry. Current trends are analyzed and projected into the future, which targets the question of how machine intelligence will be affected by the future of 6G.

# Foreword

*by Klaus Diepold*

Dear Reader,

welcome to the Proceedings of the *Seminar on Machine Intelligence* Winter 21/22 edition.

These days the academic community spends significant amount of energy discussing innovations in teaching and learning. In particular, the advent of digital tools causes a frenzy about the introduction of digital innovations in teaching. Such digital innovations include video based teaching materials aka MOOCs (massive open online courses), various concepts for 'inverted classrooms', the use of tablets, clickers, online voting and feedback and other computer-based tools as well as using all sorts of digital media and much more.

I am all for experimenting with new formats of teaching, and a reasonable use of digital tools can be helpful and even inspiring at times. Any new way of teaching, be it digitally supported or based on less technically demanding methods and tools shall be evaluated if they actually help students to earn a better education. This last question taken by itself is already a challenge, because we lack reliable methods to measure the success of education and hence we have a hard time to distinguish between *good* and *better*. Looking at examination results is certainly not enough, just as much as student evaluations are seldom more than an assessment of the students' well-being. These methods are prone to all sorts of secondary effects rendering the results close to useless.

One measure of success that I regard as rather reliable and instructive is to what extend I succeed in activating the students in a class. By activation I mean that students are actually going out on their own acquiring facts and knowledge, digesting and actively discussing the material they found among themselves, without me telling them exactly what they are supposed to be doing. This way they create new knowledge and experiences. And that I would declare a successful education.

The book you hold in hands is the result of one of my educational experiments. The students were set up to collect, acquire, digest and produce new knowledge for themselves. I dearly hope that this seminar also serves for the students as a preparation for choosing a topic for their final project before concluding their Master's degree at TUM. The knowledge students gain this way

may not be new to the world or to the scientific community, but it is new to the students and it is active in their minds by virtue of the process they went through. Besides the new knowledge they pick up, they also gain experience in the process of collecting and digesting information, being critical and constructive as well as experiencing the power of communication and intellectual exchange with their peers and hence turning information into knowledge.

One aspect that I find instructive to measure the success of this course format is the amount of effort and time students invest in the course voluntarily, without me, the instructor, urging or requiring them to work harder. They just do it, because they feel inspired and because they are curious. Funny enough, this extra engagement on the students side earned me an exhorting message from my Dean of Study, who felt that our students were overly burdened by the course. This exhortation was the result of the students' course evaluation, where students indicated that they've worked many more hours than accounted for the by the assigned credits. However, the students also acknowledged that they loved the course in spite of the long hours. To me, this is a strong indicator that we did something right. I am exuberantly happy about the outcome of the course, which is exactly this book and I am proud of the students who proved very convincingly that they are maturing academically and that they can create interesting research-related output way beyond reproducing the content of lecture notes.

In spite of this somewhat personally felt success, I still had to promise to the Dean of Study that next year we will return to a format with reduced work load. I am not sure if the students can keep up to this promise if I succeed to fire them up to a similar amount, possible with one of my next educational experiments.

Munich, March 2022

# Contents


**1 Introduction** **3**

**2 6G and Machine Learning for Industry** **7**
2.1 Introduction . . . . . 8
2.2 Trends . . . . . 8
2.2.1 Edge Computing . . . . . 8
2.2.2 Collaborative Robots (Cobots) . . . . . 11
2.2.3 Digital Twins . . . . . 15
2.2.4 Augmented Reality and Virtual Reality . . . . . 18
2.3 Conclusion . . . . . 20

**3 Federated Learning for Sensitive Data** **29**
3.1 Introduction . . . . . 30
3.2 Trends . . . . . 31
3.2.1 Reducing Communication Cost for Federated Learning . . 31
3.2.2 Federated Learning: Ensuring Fairness and Addressing source of Bias . . . . . 33
3.2.3 Representative Data-Driven Models in Healthcare Systems 36
3.2.4 Reducing the Cost of Countermeasures to Security and Privacy Attacks on Federated Learning . . . . . 39
3.3 Conclusion . . . . . 42

**4 Generalization in Machine Learning and 6G** **49**
4.1 Introduction . . . . . 49
4.2 Trends . . . . . 50
4.2.1 Artificial General Intelligence . . . . . 50
4.2.2 Edge Artificial Intelligence . . . . . 54
4.2.3 Trustworthy Artificial Intelligence . . . . . 57
4.3 Conclusion . . . . . 60

**5 Applications for 6G** **65**
5.1 Introduction . . . . . 65
5.2 Trends . . . . . 66
5.2.1 Extended Reality . . . . . 66

5.2.2 Big Data . . . . . 69
5.2.3 Internet of Things . . . . . 72
5.2.4 The Global Network and Autonomous Driving . . . . . 76
5.3 Conclusion . . . . . 79

# Chapter 1

# Introduction

*by*
*Sven Gronauer,*
*Mohamed Ali Tnani,*
*Micheal Zwick,*
*and Klaus Diepold*

In this introduction chapter, we provide background information about the genesis of this book, why it exists, how it was conceived and how it was finally produced. This account shall also serve to communicate the didactical concept underlying the process that eventually produced the book.

The content of this book represents a snapshot of current thinking about the application of machine intelligence in the domain of telecommunication. As the level of the fifth generation (5G) of telecommunication is steadily advancing, research already focuses on the next level of telecommunication technology: 6G. A plethora of new use cases can be expected due to new technical milestones such as 1 Tb/s peak data rate, 1 ms end-to-end latency and up to 20 years of battery life. The instantaneous availability of data creates a natural playground for artificial intelligence and applications thereof. The role of machine intelligence in the context of 6G and its future perspective is investigated by students who are just about to enter the world of science.

This book is the result of the one-semester *Seminar Machine Intelligence*. The seminar is a course in the curriculum of the Master of Science in Electrical and Computer Engineering, which is offered by the Faculty of Electrical and Computer Engineering of the Technical University of Munich (TUM). The seminar consists mainly of weekly meetings for 2 hours to discuss and work on the subject. The work is organized as group discussions and team work. Students have to read, write, review and present their findings on a weekly basis. To this end, new digital e-learning tools and methods were employed along with discussion styles such as world-cafe or speed-dating discussions and other styles of organized communication. Students do presentations as Pecha Kuchas, a specific presentation format that consists of 20 slides, each shown for 20 seconds.

That makes every presentation to last just 6 minutes and 40 seconds. This format facilitate for highly focused and condensed presentation sessions, while also creating a spontaneous and fun atmosphere. It is tough to be boring under such conditions, and if a presenter is boring, it is quickly over. Throughout the seminar participating students should learn fundamental aspects of scientific research along with honing their skills in oral and written communication in a scientific or technical field. The intention for the students in the course is to develop ideas and paths for future research in the field leading towards insights and methods necessary to design and implement intelligent machines in the broader sense of the word.

The seminar in total was structured in three major stages, which we elaborate a bit here.

**1st Stage: Individual Reading, Writing, Reviewing, Discussing** During the first stage the seminar started out with all students jointly reading a set of fundamental papers or book to set the stage and provide for a shared basis and reference for future discussions. Between subsequent meetings students agreed on a set of chapters to read until the next meeting. Students were also asked to reflect on their reading by writing short essays along some high-level guiding questions. Each of the students' essay had the size of 5000 characters (incl. spaces). The students uploaded their essays before the next meeting using the e-learning platform Moodle. Furthermore, students were randomly assigned essays of their fellow students to read and review. During this stage, the students discussed the content of the book during the weekly meetings, using various forms of discussion, such as world cafe, speed dating discussions, fishbowl discussions, cocktail party discussion. This form of reading, writing, reviewing and discussing generated a shared domain of knowledge to facilitate the later stages in the process. It also conveyed fundamental information about the field of study on intelligent systems as well as some facts on telecommunications and its sixth generation. This first stage took about 4 weeks.

**2nd Stage: Team - Researching, Presenting, Discussing** The second stage started with a workshop where the students tried to identify major fields of science and technology, which were considered essential to push the topic of machine intelligent and its connection to telecommunications into the future. By the end of the workshop, the student agreed on a list containing the dominating fields and domains. Subsequently, students could assign themselves to one of these items on the list to further study the field in more detail. During the next five weeks, the teams of students researched their chosen field compiling information about the state of the art and the major trends. During the weekly contact hours one student per team delivered a Pecha Kucha presentation, highlighting the group's findings during the past week for all others to understand and participate. The presentations were followed by discussions on open points. The one purpose of the presentations is to disseminate the essence of the information collected over the past week to the fellow students. Another

objective is to sharpen the sense of the presenters to think about their target audience and to tailor the amount and the level of detail of the presentations to match the expectation of their target audience.

**3rd Stage: Projecting - Writing - Reviewing** The book is written by students mainly for students. It does not claim to contain and communicate ultimate truths, but rather tries to project current facts and trends into future directions of research based on a intense investigation of trends and possibilities. The book may prove to be a helpful tool to orient students interested in the study and the development of intelligent systems, AI, machine learning and so on as a basis to narrow down on a topic for their Master thesis projects or even beyond. Not least of it, the book may also display interesting ideas and anticipations, which may be helpful even for more seasoned researchers to communicate with young people and transmit the excitement for science and research on intelligent systems using a language and level that students can digest and appreciate.

We hope, you the reader, will find inspiration in the chapters and the material to further lead the discussion about practical uses of machine intelligence to tackle serious societal challenges. If you have any remarks on this book, our process or the course itself, we would love to hear from you.

# Chapter 2

# 6G and Machine Learning for Industry

Djajapermana, Mikhael
Haberhauer, Valentin
Ploch, Noah
Ruano Martinez, Roberto
Tizaoui, Tejennour
Zhao, Ziqing
Zhou, Xiaoming

## Abstract

6G and Machine Learning (ML) are two important pillars supporting the development of many technology trends in the industry. The exponentially growing number of devices will require 6G networks for more efficient and reliable data exchanges. In addition, intelligent data processing, supported by machine learning, will provide new insights for improved industry practices. The industry of the future will be shaped by the integration of multiple technology trends. This report focuses on four industry trends that are expected to emerge or be enhanced by the combined use of 6G and ML: Edge Computing, Collaborative Robots, Digital Twins, and Augmented and Virtual Reality. We start the analysis with the key facts about each trend and then proceed to analyse each trend in terms of its key drivers, challenges and overall impact on the industry. Finally, we compare these four trends and assess their relationship to each other. For this purpose, we use a driver matrix with the features' uncertainty and potential impact. Based on its maturity and its role in enabling and extending existing technologies, we concluded that Edge Computing will have the greatest impact and the least uncertainty in terms of its applicability in the industry.

## 2.1 Introduction

The advances of 6G and Machine Learning (ML) are a major force propelling the industry forward. 6G network is expected to deliver ultra-low latency, high reliability, and high energy efficiency to serve the exponentially growing number of devices. The exponential data growth, when combined with machine learning processing capabilities, provides new insights for improved industry practices and enables the deployment of various new technologies. The development of the future industry will be shaped by the integration and combination of several technology trends.

The future industry will be equipped with a high number of sensors that collect data and provide crucial information. Edge Computing is the enabling infrastructure for the Industrial Internet of Things (IIoT) consisting of sensor-equipped smart devices.

Furthermore, modern production requires the execution of complex multi-stage physical tasks. Collaborative robots (Cobots) are designed to operate collaboratively with humans while adapting to changing environments. This collaboration will increase productivity and efficiency.

Another key concept for the future industry is digital transformation, which is achieved through the integration of existing manufacturing systems with virtual simulation. Digital Twin monitors the real-time status of an object to transform the physical object in its digitized form. The Digital Twin can be used to track performance within the industry, simulate scenarios, and predict failures.

Finally, innovative interfaces are necessary to allow effective human-machine interaction. Virtual Reality (VR) and Augmented Reality (AR) provides users with an intuitive way of machine interaction through gesture control and tactile feedback.

## 2.2 Trends

In this section, each of the four trends named in Section 2.1 is presented in more detail and corresponding key drivers, challenges and the resulting impact are analyzed.

### 2.2.1 Edge Computing

In the near future, one can clearly foresee that industrial production will be awash in an ocean of data. As it becomes increasingly intelligent, there is an urgent need to collect and process large amounts of data from sensors and IoT devices in real-time. Traditional methods such as centralized data centres have shown their limitations in network latency, cost of network bandwidth and data storage, security, and compliance issues [1]. Hence, computing in the cloud no longer fits the extremely tremendously growing data traffic. This leads to

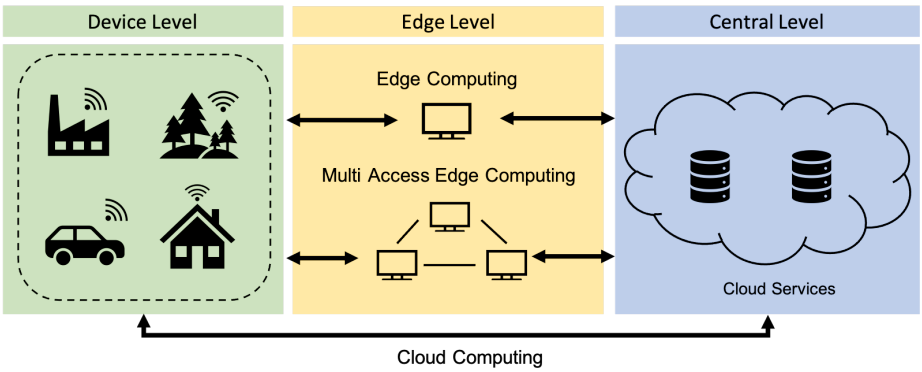


Figure 2.1: An Edge Computing architecture, which consist of three levels: device level, edge level and central level. Three architectual deployment models for 6G networks include cloud computing, Edge Computing and multi access Edge Computing.

the emergence of edge infrastructure which can pre-process and interpret data on-device rather than sending data to the cloud.

According to Karim Arabi's definition [2], Edge Computing can be broadly seen as all computing outside the cloud, which happens frequently at the edge of the network, and more specifically in applications where real-time processing of data is required. In other words, Edge Computing moves some of the storage and computing resources out of the central data centre and closer to the data source itself. Only the results of the Edge Computing work, such as real-time business insights, equipment maintenance predictions, or other actionable answers, are sent back to the main data centre for review and other human-computer interaction [3].

Edge Computing is also one of the key driving forces of enabling the 6G network, as the traditional cloud computing architecture can hardly meet the ultra-low latency as the 6G network would commit. The inherited longer distance from the end-users makes cloud computing have a higher delay, and Edge Computing can overcome this by bringing computing and storage capabilities closer to the end-users [4]. It can be predicted that the evolution of telecom infrastructures towards 6G will consider highly distributed Artificial Intelligence (AI), moving the intelligence from the central cloud to Edge Computing resources [5].

### Facts

- The total amount of data created, captured, copied, and consumed globally is reaching 79 Zettabytes (ZB) in 2021 [6], while the data centre IP traffic is only 20.6 ZB [7]. By the year 2025, the global data sphere will reach 175 ZB, with over 90ZB of data created in IoT devices [6].

- There will be more than 6 billion consumers, or 75% of the world's population, interacting with data every day by 2025. Each connected person will have at least one data interaction every 18 seconds [6].

- More than 150 billion devices will be connected across the globe by 2025, most of which will be creating data in real-time. In 3 years over 6 billion devices will be connected to the Edge Computing solution [6].

- By the year 2028, cumulative capital expenditures of up to 800 billion USD will be spent on new and replacement IT server equipment and Edge Computing facilities [7].

- The potential economic impact of IoT in the factories set could be from 3.9 trillion to 11.1 trillion USD per year in 2025 [8].

**Key Drivers**

- Average prices for IoT sensors decrease from 0.70 USD in 2014 to 0.38 USD in 2020 [9], which makes it cheap enough to support broad industrial applications.

- Over the last two decades, microprocessors' computational power has improved, doubling every three years [9]. The emergence of more powerful edge devices allows for better-distributing computing, processing and storage tasks, enabling the usage of a large amount of sensor data.

- 6G provides new protocols such as end-to-end application protocol to make use of edge infrastructure [10].

- 6G utilizes much broader frequency bands, including sub-terahertz and terahertz (THz) bands as well as visible light communication (VLC) [11], which help IoT systems to maintain with ultra-high data rate and extraordinarily low latency.

- The space-air-terrestrial-sea integrated (SATSI) network architecture and the ultra-massive MIMO communication in 6G will provide sufficient network capabilities, enabling flexible and efficient connection of trillion-level edge devices in multiple domains [11].

- Network and cloud service providers are facing an unprecedented challenge to meet the demand of end-users during the COVID-19 pandemic [12].

- Investment in Edge Computing is still in its preliminary stages. 'Edge Computing' CPC (cost per click) levels are around 70% lower than for 'Cloud Computing' – at 3.94 USD versus 12.98 USD [13].

**Challenges**

- Edge Computing lack standard protocols. IoT systems may have unique programming platforms and frameworks [14], which add difficulty for interoperability between different systems.
- With limited storage, computation, and communication resources in the wireless edge networks, deploying an edge AI system causes a significant scalability issue in terms of latency, energy, and accuracy [15].
- When integrating smart networks into a 6G base station, the robustness of the Edge Computing servers are not yet ensured [16]. The integration between edge devices could affect the availability of the mobile network.
- Integration of Edge Computing and other communication systems raises many challenges about the security and privacy of users and organizations. Its emergence increases the security threats of cyber-attack due to the weak computation power, attack unawareness and heterogeneous OS and protocols [17].

**Impact**

Edge Computing architecture could have great benefits in many industries. These benefits do not solely come to a few network and computing-based industries, but to the vast majority of industries that utilize cloud infrastructures, such as logistics, agriculture, healthcare, manufacturing, oil and gas, retail, and services. For manufacturing, Edge Computing can be used for smart sensing, machine vision, or predictive maintenance [18]; for transportation, it enables the automated vehicles to process the visuals on-device, without data offloading [19]; for retail, it can help predict the interest of customers and enhance the user experience [20].

However, it does not mean that cloud computing is coming to an end, as cloud computing complements Edge Computing in many ways. Combining on-premises Edge Computing infrastructure with private clouds or public clouds may be a "best-of-both-worlds" solution to reap the benefits and advantages of both [21].

### 2.2.2 Collaborative Robots (Cobots)

6G wireless network technology will have a great impact on how industries use robots. Having a high bandwidth, highly reliable wireless connection will allow a shift from pre-programmed fenced-off robots that perform only a single task to flexible and safe to be around collaborative robots (cobots).

In the past robots revolutionized manufacturing by freeing humans from redundant and dangerous tasks. The concept of cobots however focuses on interacting intelligently with both humans and their environment. Cobots will share the same workspace with human operators without the need for any protective devices. Human workers are great at adjusting to changing situations whereas

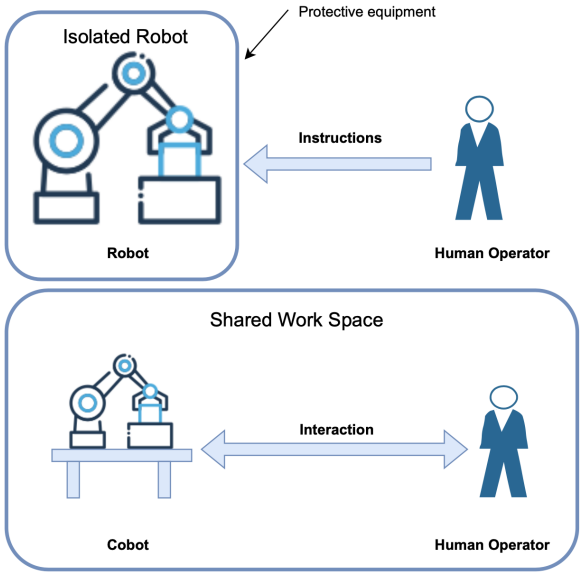


Figure 2.2: Illustration of the difference between traditional robot automation (top half) and cobots (bottom half).

robots are perfect for executing redundant tasks. Combining both entities' advantages of both of them allows the fulfilment of requirements of upcoming Industry 5.0 where flexibility and efficiency are key performance indicators.

The concept of cobots is further strengthened by taking advantage of Machine Learning and Edge Computing. While Machine Learning allows for predicting movements of humans and general object recognition, Edge Computing reduces communication overhead and lowers computing latency. This allows for faster reaction times and therefore increases safety without taking a performance hit. Both aspects can also be used to interact with other robots and cobots and split tasks up to multiple cobots which can increase efficiency [22].

### Facts

- The market size for cobots grew by more than 10 times from 2016 to 2021 to an estimated total of 1.2 billion USD and is expected to surpass the 10 billion USD mark by 2027 [23, 24]. Another research group predicts a smaller but still impressive annual growth rate of more than 12% from 2020 to 2030 [25].

- Cobots are beneficial for many different applications in a wide variety of fields. These fields include automotive manufacturing, general order picking and packaging [26, 27] but also reach from logistics in hospitals to a helper during surgical procedures [28].

- Generally cobots are way smaller than traditional robots and are light enough to be moved by a single human operator [29]. Combined with reduced operating complexity and no need for a safety barrier cobots allow for a rapid change in the production environment [30].

- Robots are very efficient for repetitive actions and reliable outcomes but not every task is (financially) viable for automation [29]. In these cases close interaction between cobots and humans to solve complex and quickly changing tasks is beneficial.

- Although the concept of cobots has been around for many years, dating back to the last century, industries only accept them at a slow rate. Further development in safety and efficient task splitting between robots have been identified as a necessity [31].

**Key Drivers**

- Advances of AI will allow the robots to interact intelligently with their environment and learn from it and human colleagues, [30]. In addition, we are preparing for the introduction of the next generation communication network (6G). 6G promises lower latency and high reliability. These two technological foundations could enable cobots to learn online. They will also help to increase the accuracy and efficiency of the system [32].

- The use of cobots can improve productivity and flexibility. In addition, cobots do not require safety devices or gates, which leads to savings in the cost of safety equipment [33, 27].

- Future production lines will have to focus on highly customizable products to keep up with Industry 5.0. Traditional robots are not flexible enough to aid in the production of customizable products [27]. Cobots on the other hand can be easily reprogrammed and adjusted to the new product design.

- Robots are great in fulfilling repetitive tasks and cobots therefore can reduce the strain on human workers by offloading certain tasks. Furthermore, the health of workers can be protected by using cobots for handling dangerous operations [33, 34]. This makes cobots a great tool to improve ergonomics for many human workers and thereby fulfil the principles of Industry 5.0.

- Cobots can be programmed and reconfigured by workers with minimal training which enables quick changes in the production environment [35]. This maintains high efficiency while offering more flexibility than conventional robots.

**Challenges**

- The need for extreme performance [36]. Cobots need to be able to process large amounts of data and make decisions in (close to) real-time to sustain new applications. At present, however, there is not yet sufficient computing and communication performance and storage capacity to meet these requirements [32].

- Cobots have to be safe enough to directly interact with humans [32]. Therefore, cobots have to include safety measures that include slower movements and limitations in available power and force [33, 37, 29], which yet can put them at a disadvantage to traditional robots. A way to guarantee safety without restraining the abilities of the cobot is still an ongoing research.

- Human workers have not fully accepted cobots yet. Futhermore, Cobots not only have to be safe but human operators also have to perceive them as being safe. Humans have to accept the interactions with the cobots and realize that they won't be replaced by them [38].

- Cobots should be able to adjust their behaviours according to different workers' behaviours, such that ergonomics can be improved and possible accidents can be reduced [39]. A process still needs to be put in place to enable cobots to recognise different work styles and identify workers.

**Impact**

Cobots are designed to work in close proximity to humans [32]. The use of cobots will have an impact on many areas. First and foremost it will impact the manufacturing landscape by enhancing the flexibility of production lines and improving product quality and customizability of products [40]. In addition, cobots have an overall lower initial cost and a faster return on investment [27] which makes cobots a viable solution even for small and mid-scale businesses. Instead of developing complex machines and processes that consume even more resources, cobots will help use existing capabilities intelligently, as cobots can communicate with every entity on the production floor [22].

On the other hand, it will have an impact on both society and the environment. By building an interactive environment for humans and robots, complex tasks can be completed more sustainably. Furthermore the ease of use of cobots reduces the need for specially trained robot operators therefore enabling every production worker to take advantage of automation which can reduce strain on the humans. On a societal level, cobots will further enhance the automation of processes in the industry, which will free workers from redundant manual tasks and reduce labour costs [27]. We also expect that sensory safety measures in cobots will be used in traditional robots and thereby reducing the required footprint for safety fences.

### 2.2.3 Digital Twins

Nowadays, the pace at which the industry needs to deliver new, reliable and sophisticated products and the level of flexibility in design required by customers is increasing. However, there is still one major setback that many companies have to deal with which is the long production and product design time due to unexpected problems that can come once the hardware and the physical devices are tested. Therefore, digitalization technologies promising more efficient, less error-prone and more flexible production are of high interest for industrial companies. The Digital Twin (DT) represents one of these technologies and explores the opportunity of Digital-Product Definition (DPD) and Digital Manufacturing. Although its meaning has not been completely unified, a compelling definition is the one proposed by Cunbo et al., who define it as *an integrated multi-physics, multi-scale, super-realistic, dynamic probability simulation model that can be used to simulate, diagnose, predict, and control the realization process of physical entities of products in real environments* [41].

The DT concept first appeared in 2003 as part of a Life Cycle Management course [42], and now it is being explored to be used in the automotive, aircraft and spacecraft industry, but also healthcare, energy (smart cities) and in general in the manufacturing industry, shortening the production time to deliver a product and accelerating innovation. Some of the DT enabling technologies include cloud computing, IoT and IIoT (Industrial Internet of Things), Edge Computing, 5G technologies and Artificial Intelligence (AI) [43, 44].

The big role these technologies play in the realization of a DT can be appreciated in Figure 2.3, which shows the working principle of an exemplary DT with the bi-directional data flow. This means, the DT receives real-time data from the physical objects connected to it, but can also influence the physical workflow, depending on the tasks it was designed for. The DT is embedded in a cloud to guarantee quick remote access, e.g. through an online human user interface, and sufficient computing power for running models, e.g., for predictive maintenance. The middle layer captures the local infrastructure needed to run a DT, which consists of an IoT framework capable of collecting data and (if needed) sending commands to the physical objects.

**Facts**

- The interest of the industry for DT technology lies in the increase in competitiveness, productivity and efficiency by improved production planning and control, maintenance and layout planning [45].
- The market for DT technology in the US is currently at 3.1 billion USD with a prospective growth of up to 48.2 billion USD in 2026 [46].
- Most applications of DT technology are found in manufacturing, but there is an increasing interest from healthcare and for smart cities [47].
- Automotive and transport industries held the largest market share in the DT market in 2019 [46].

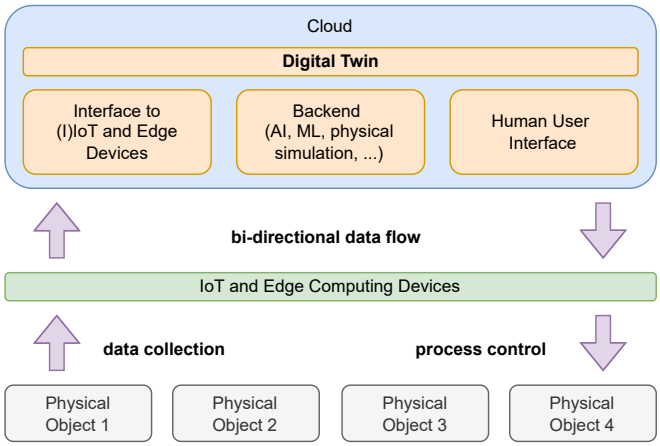


Figure 2.3: Working principle of a Digital Twin. The edge devices and IoT framework collect data from physical objects and pass them to the DT environment, which is embedded in the cloud. Depending on the twin's purpose, different actions can be performed, e.g., control sequences are passed to the physical objects after data analysis.

- Currently, research regarding the DT is still in its beginnings and the concept and types of twins are about to be standardized [45].
- Some of the main efforts in healthcare include creating Digital Twins of human organs or the human as a whole, e.g., to increase the efficacy of treatments [48, 43].

### Key Drivers

- IIoT and IoT are key enablers of DT technology [43]. The number of applications of IoT and IIoT is growing incredibly fast, with more than 50 billion devices connected to the IIoT by 2025 [49].
- AI and ML have been successfully used to analyze large amounts of data yielding patterns and results hidden in data. DTs profit from this technology to cope with the physical system data and provide useful insights, e.g., by predictive maintenance [43].
- Large multinational software and automation companies have started developing integrated solutions to implement DT technology in their products, such as "Mindsphere" by Siemens [43, 50], offering access to Digital Twins to their great amount of customers.
- High connectivity with real-time communication and low latency is key for a DT to work. 5G is the first standard to offer the speed and latency needed for DT implementations [44] and 6G with higher data rates, higher

connectivity, higher reliability and lower latency [51] will push the use of DTs further forward.

- The COVID-19 pandemic has become a strong driver of industry digitalization and thus use of DT technology [46].

**Challenges**

- The expectations lying on DTs and its enabling technologies such as data analytics and AI can quickly create frustration if promised results and cost savings are not directly appreciable [43].
- The required IT infrastructure, physical modelling and software development to produce an accurate replica of the physical system and achieve synchronization between digital and physical manufacturing is a big challenge and multidisciplinary effort. Therefore, the costs to implement it are elevated [52, 42].
- In the medical sector, DTs will still need a long legal process and a worldwide effort to effectively develop more efficient twins [48].
- Since DTs will be used more and more in safety-critical applications, the need to ensure secure archival and retrieval of data through advanced cryptography methods is crucial. There is already research proposing blockchain as a tool to provide maximum security, traceability and transparency [53].
- DT orchestration will be part of the main challenges when several virtual models need to work together to simulate a physical environment (e.g the systems inside a car). This will require a high effort at selecting the right frameworks, tooling and modelling [54].

**Impact**

Digital Twins are at the heart of the digital transformation of industry. They represent the ultimate, bi-directional connection of a physical object or process and a simulation of it, thus opening doors to data-driven production control, predictive maintenance and efficient product redesign [50], among others. These advantages lead to increased efficiency and productivity and a much shorter product design process for the companies using them, resulting in a quickly growing interest of the industry for this technology.

On the other hand, the accessibility to Digital Twins will also become better due to the consolidation and spread of its key enabling technologies, which most importantly are cloud computing, artificial intelligence/machine learning and IoT/IIoT. Furthermore, Digital Twins will pave the way to the industrial application of augmented and virtual reality due to its very own purpose of making physical objects virtually accessible, for instance, an ice cream machine as demonstrated by Karadeniz et al [55]. In addition, the COVID-19 pandemic

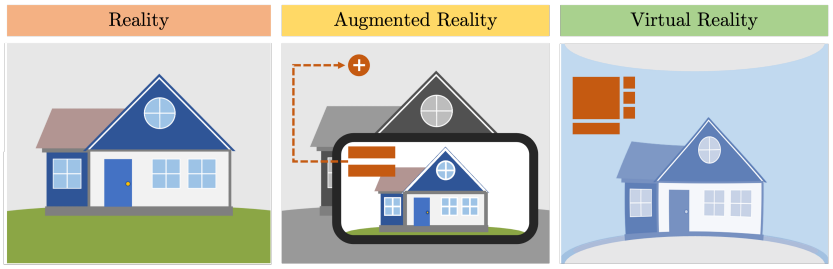


Figure 2.4: Illustration of Augmented Reality and Virtual Reality. In Augmented Reality, virtual objects are overlaid in a real world environment. Virtual Reality immerse the users in a fully digital environments.

has made many companies aware of the advantage of remote availability of digital-twin-enhanced industry [46].

Digital Twins will be a key component of the digital transformation of industry in the area of process automation and virtualization. Taking into account the current pandemic situation, the demand will be even increased due to the added value of remote accessibility [49].

### 2.2.4 Augmented Reality and Virtual Reality

The term augmented reality (AR) refers to a physical environment whose elements are enhanced and supported by virtual input. On the other hand, a virtual reality (VR) is a simulated virtual environment that simulates a physical environment [56].

After attracting huge attention in the gaming industry (e.g. Pokémon Go), AR and VR are rapidly extending into other industries. A perfect illustration of this is the healthcare sector, where AR/VR usage has been experiencing the most change since the COVID-19 pandemic [57]. The increasing use of AR and VR are thanks to the emergence of wearable gadgets such as the Oculus Rift and Microsoft HoloLens.

In the industry, AR and VR can be utilized as a visualization tool to reduce miscommunication and improve spatial perception during design processes [58]. Because of its immersion capabilities, virtual environments can also be used for work training, minimizing risk when working in dangerous areas [59].

**Facts**

- Successful applications of AR and VR can be found in many industries, such as retail [60], education [61], healthcare [62] and production and maintenance [63].
- Worldwide spending on AR/VR is forecast to rise from $12.0 billion in 2020 to $72.8 billion in 2024. The five-year compound annual growth rate (CAGR) for AR/VR spending will be 54.0% [64].

- The global AR/VR market in the healthcare industry is expected to grow and reach $10.82 billion by 2025, representing a compound annual growth rate of 36.1% [65].
- Big Tech companies invest in AR and VR: Google with ARCore, Microsoft with Hololens, Meta with Oculus, and Apple with Akonia Holographics.

**Key Drivers**

- Improved computer vision algorithms to deliver more reliable and immersive experiences.
- Advanced sensing technologies to provide a responsive and intuitive interface through gestures, emotions and gazes [66].
- 6G will provide higher speed and volume of the broadband network, which enables more complex AR applications [67].
- AR systems require a powerful CPU and considerable amount of RAM to process camera images. With the rise of smart-phones technology, a lighter and more sophisticated AR system can be developed [68].
- New holographic technologies and smart contact lenses are being developed, resulting in better integration of AR into industry workflows [69].

**Challenges**

- Lack of feasibility studies examining the actual cost of implementation versus an increase in profit [56].
- The industry is still in the early stages for content [57]. Developers should produce more interactive and immersive content.
- User experience is the top barrier to greater adoption of AR and VR [57]. For example, some people might experience motion sickness when using VR [70].
- High-quality VR graphics needs large computational power which is challenging in mobile devices [71].
- Some applications require devices to be durable, but this has not been a focus of AR/VR research thus far.

**Impact**

VR and AR have the potential to enhance current safety training programs and workers' hazard recognition abilities [59]. They also provide easier access to information for the on-site employees, resulting in increased productivity. As a visualization tool, VR can provide better spatial perception than conventional 2D screens, which helps to decrease the number of errors in the design process

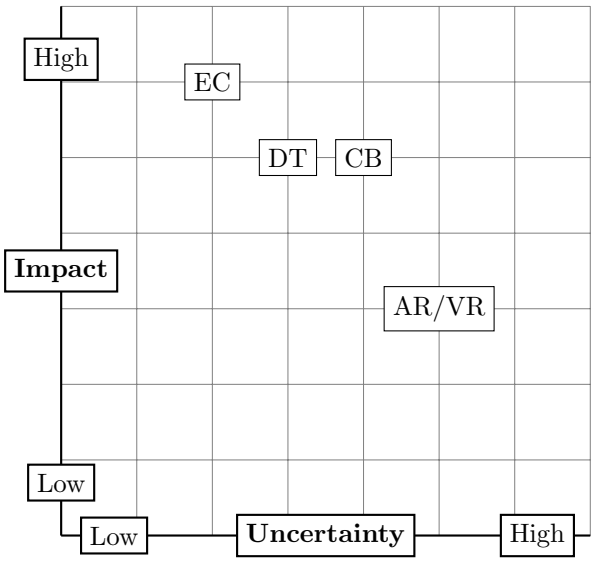


Figure 2.5: Driver matrix. EC stands for Edge Computing, DT for Digital Twin, CB for Cobots, and AR/VR for Augmented and Virtual Reality.

[58]. AR can enhance shopping experiences by providing visually appealing information and assisting potential buyers in better understanding what is being offered [72]. Furthermore, VR has been found to be effective in obtaining user feedback, which serves to increase end-user satisfaction and design [73].

## 2.3 Conclusion

Within the topic of 6G and ML for industry, the four trends presented cover a wide range of applications that are already being implemented or will be realized in the upcoming years in the industry. However, the question of how these trends relate and compare to each other is also of high interest. The driver matrix shown in Figure 5.5 depicts our assessment of that question by arranging the trends in terms of uncertainty and impact.

The analysis of Edge Computing revealed the maturity of this trend and the high impact it is having, as it is a necessary step towards a digital industry. This positions it in the top left corner. The small uncertainty we see regarding the future of this trend arises from some of the challenges identified, such as the need for standardization, but they are more a matter of time to us than a threat to the trend itself.

With slightly less impact and some more uncertainty, the digital twin follows Edge Computing as a technology strongly dependent on the latter. DT technology requires an industrial environment with high digital integration, such as implemented hardware for data collection and device control, thus resulting

in higher uncertainty. On the other hand, DT technology is key to the digital transformation of industry by definition and will therefore be a strongly impacting trend.

We assess cobots to have a similar impact as DT technology, but with a higher uncertainty due to safety and performance issues. Reaching the same performance as current industrial robots, but also fulfilling safety requirements applying to collaborative work with humans is a big challenge this trend faces. Nevertheless, once this challenge is overcome, applications, such as flexible manufacturing, are very promising.

Augmented and virtual reality have the least advantageous rating when compared to the other trends. This is due to the dependence of this technology on all other trends in differing ways and depending on the application, such as serving as an interface to a cobot, as the visualization tool of a digital twin or as an enhanced human-machine interface for an Edge Computing network. We assess this dependence to significantly condition the uncertainty of this trend and also its impact in the industry, since it is not mandatory for a digitalized industry but offers significant advantages once implemented, such as visually appealing training for future machine supervisors.

Looking at the big picture, these four trends will shape the digitalization of industry and play a major role in the next years. The current and projected market size of these trends and the promising answers they offer to pressing industry problems are strong indicators of their importance and the impact they will have.

# References

[1] Wei Yu et al. "A survey on the edge computing for the Internet of Things". In: *IEEE access* 6 (2017), pp. 6900–6919.

[2] Karim Arabi. "Trends, Opportunities and Challenges Driving Architecture and Design of Next Generation Mobile Computing and IoT Devices". MTL Seminar. 2015. URL: `https://www.mtl.mit.edu/seminars/trends-opportunities-and-challenges-driving-architecture-and-design-next-generation-mobile`.

[3] Baotong Chen et al. "Edge computing in IoT-based manufacturing". In: *IEEE Communications Magazine* 56.9 (2018), pp. 103–109.

[4] Mariam Ishtiaq, Nasir Saeed, and Muhammad Asif Khan. "Edge Computing in IoT: A 6G Perspective". In: *arXiv preprint arXiv:2111.08943* (2021).

[5] Ella Peltonen et al. "6G white paper on edge intelligence". In: *arXiv preprint arXiv:2004.14850* (2020).

[6] Phil Marshall et al. *State of the Edge Report*. Tech. rep. The Linux Foundation Whitepaper, 2021.

[7] Cisco Global Cloud Index. *Forecast and Methodology, 2016-2021*. Tech. rep. CISCO Whitepaper, 2018.

[8] James Manyika et al. "The Internet of Things: Mapping the value beyond the hype". In: McKinsey Global Institute New York, NY, USA, 2015, p. 144.

[9] Jonathan Holdowsky et al. "Inside the internet of things (IoT)". In: *Deloitte Insights* 21 (2015).

[10] Xiuquan Qiao et al. "6G vision: An AI-driven decentralized network and service architecture". In: *IEEE Internet Computing* 24.4 (2020), pp. 33–40.

[11] Shangwei Zhang et al. "Envisioning device-to-device communications in 6G". In: *IEEE Network* 34.3 (2020), pp. 86–91.

[12] Yassine Abdulsalam and M Shamim Hossain. "COVID-19 networking demand: an auction-based mechanism for automated selection of edge computing services". In: *IEEE Transactions on Network Science and Engineering* (2020).

[13] STL Partners$^{TM}$. *Edge computing investments are just beginning*. `https://stlpartners.com/articles/edge-computing/edge-computing-investments-are-just-beginning/`. Accessed: 06.02.2022.

[14] Ejaz Ahmed and Mubashir Husain Rehmani. *Mobile edge computing: opportunities, solutions, and challenges*. 2017.

[15] Khaled B Letaief et al. "Edge Artificial Intelligence for 6G: Vision, Enabling Technologies, and Applications". In: *IEEE Journal on Selected Areas in Communications* 40.1 (2021), pp. 5–36.

[16] Ahmed Al-Ansi et al. "Survey on intelligence edge computing in 6G: characteristics, challenges, potential use cases, and market drivers". In: *Future Internet* 13.5 (2021), p. 118.

[17] Yinhao Xiao et al. "Edge computing security: State of the art and challenges". In: *Proceedings of the IEEE* 107.8 (2019), pp. 1608–1631.

[18] Wazir Zada Khan et al. "Edge computing: A survey". In: *Future Generation Computer Systems* 97 (2019), pp. 219–235.

[19] Shaoshan Liu et al. "Edge computing for autonomous driving: Opportunities and challenges". In: *Proceedings of the IEEE* 107.8 (2019), pp. 1697–1716.

[20] Abhiraj Biswas, Ayush Jain, et al. "Survey on Edge Computing–Key Technology in Retail Industry". In: *Computer Networks and Inventive Communication Technologies*. Springer, 2021, pp. 97–106.

[21] EQUINIX. *An Examination of the Global Impact and Future of Edge Computing*. Tech. rep. EQUINIX, 2020.

[22] Hexa-X$^{TM}$. *6G Vision, use cases and key societal values*. `https://hexa-x.eu/wp-content/uploads/2021/02/Hexa-X_D1.1.pdf`. Accessed: 09.03.2022.

[23] Yuval Cohen et al. "Deploying cobots in collaborative systems: major considerations and productivity analysis". In: *International Journal of Production Research* 0.0 (2021), pp. 1–17. DOI: 2021Deploying. eprint: https://doi.org/10.1080/00207543.2020.1870758. URL: https://doi.org/10.1080/00207543.2020.1870758.

[24] MarketsandMarkets™. *Collaborative Robot Market with COVID-19 Impact Analysis, Component, Payload (Up to 5 Kg, 5-10 Kg, and Above 10 Kg), Application (Handling, Processing), Industry (Automotive, Furniture & Equipment), and Region - Global Forecast to 2027*. https://www.marketsandmarkets.com/Market-Reports/collaborative-robot-market-194541294.html. Accessed: 06.03.2022.

[25] Research and Markets™. *Collaborative Robot Market by Payload, by Components, by Application, by Industry - Global Opportunity Analysis and Industry Forecast 2021-2030*. https://www.researchandmarkets.com/reports/5519703/collaborative-robot-market-by-payload-by. Accessed: 17.01.2022.

[26] Wim Lambrechts et al. "Human Factors Influencing the Implementation of Cobots in High Volume Distribution Centres". In: *Logistics* 5.2 (2021). ISSN: 2305-6290. DOI: 10.3390/logistics5020032. URL: https://www.mdpi.com/2305-6290/5/2/32.

[27] Richard Bloss. "Collaborative robots are rapidly providing major improvements in productivity, safety, programing ease, portability and cost while addressing many new applications". In: *Industrial Robot: An International Journal* 43.5 (Jan. 2016), pp. 463–468. ISSN: 0143-991X. DOI: 10.1108/IR-05-2016-0148. URL: https://doi.org/10.1108/IR-05-2016-0148.

[28] Richard Bloss. "Robotic innovations that address a wide spectrum of medical applications". In: *Industrial Robot: An International Journal* 39.4 (Jan. 2012), pp. 329–334. ISSN: 0143-991X. DOI: 10.1108/01439911211227881. URL: https://doi.org/10.1108/01439911211227881.

[29] Iñaki Maurtua et al. "Human–robot collaboration in industrial applications: Safety, interaction and trust". In: *International Journal of Advanced Robotic Systems* 14.4 (2017), p. 1729881417716010. DOI: 10.1177/1729881417716010. eprint: https://doi.org/10.1177/1729881417716010. URL: https://doi.org/10.1177/1729881417716010.

[30] KUKA™. *Cobots: the intelligent robot as a colleague*. https://www.kuka.com/en-de/future-production/human-robot-collaboration/cobots. Accessed: 10.03.2022.

[31] Iina Aaltonen and Timo Salmi. "Experiences and expectations of collaborative robots in industry and academia: barriers and development needs". In: *Procedia Manufacturing* 38 (2019). 29th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM 2019), June 24-28, 2019, Limerick, Ireland, Beyond Industry 4.0: Industrial Advances, Engineering Education and Intelligent Manufacturing, pp. 1151–

1158. ISSN: 2351-9789. DOI: https://doi.org/10.1016/j.promfg.2020.01.204. URL: https://www.sciencedirect.com/science/article/pii/S2351978920302055.

[32] Chamitha De Alwis et al. "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research". In: *IEEE Open Journal of the Communications Society* 2 (2021), pp. 836–886.

[33] Ana C. Simões, António Lucas Soares, and Ana C. Barros. "Drivers Impacting Cobots Adoption in Manufacturing Context: A Qualitative Study". In: *Advances in Manufacturing II*. Ed. by Justyna Trojanowska et al. Cham: Springer International Publishing, 2019, pp. 203–212. ISBN: 978-3-030-18715-6.

[34] Ashwin P. Dani et al. "Human-in-the-Loop Robot Control for Human-Robot Collaboration: Human Intention Estimation and Safe Trajectory Tracking Control for Collaborative Tasks". In: *IEEE Control Systems Magazine* 40.6 (2020), pp. 29–56. DOI: 10.1109/MCS.2020.3019725.

[35] Mary Doyle-Kent and Peter Kopacek. "Collaborative Robotics Making a Difference in the Global Pandemic". In: *Digitizing Production Systems*. Ed. by Numan M. Durakbasa and M. Güneş Gençyılmaz. Cham: Springer International Publishing, 2022, pp. 161–169. ISBN: 978-3-030-90421-0.

[36] Walid Saad, Mehdi Bennis, and Mingzhe Chen. "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems". In: *IEEE network* 34.3 (2019), pp. 134–142.

[37] Mary Doyle Kent and Peter Kopacek. "Social and Ethical Aspects of Automation". In: *Digital Conversion on the Way to Industry 4.0*. Ed. by Numan M. Durakbasa and M. Güneş Gençyılmaz. Cham: Springer International Publishing, 2021, pp. 363–372. ISBN: 978-3-030-62784-3.

[38] Tobias Kopp, Marco Baumgartner, and Steffen Kinkel. "Success factors for introducing industrial human-robot interaction in practice: an empirically driven framework". In: *The International Journal of Advanced Manufacturing Technology* 112.3 (Jan. 2021), pp. 685–704. ISSN: 1433-3015. DOI: 10.1007/s00170-020-06398-0. URL: https://doi.org/10.1007/s00170-020-06398-0.

[39] Olatz De Miguel Lázaro et al. "An Approach for adapting a Cobot Workstation to Human Operator within a Deep Learning Camera". In: *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*. Vol. 1. 2019, pp. 789–794. DOI: 10.1109/INDIN41052.2019.8972238.

[40] Danica Kragic et al. "Interactive, Collaborative Robots: Challenges and Opportunities." In: *IJCAI*. 2018, pp. 18–25.

[41] Z. Cunbo et al. "The connotation, architecture and development trend of product digital twins". In: *Computer Integrated Manufacturing System* (2017), pp. 753–768.

[42] J Wu et al. "The Development of Digital Twin Technology Review". In: *2020 Chinese Automation Congress* (2020).

[43] Aidan Fuller et al. "Digital Twin: Enabling Technologies, Challenges and Open Research". In: *IEEE Access* (2020). DOI: 10.1109/ACCESS.2020.2998358.

[44] Adil Rasheed, Omer San, and Trond Kvamsdal. "Digital Twin: Values, Challenges and Enablers From a Modeling Perspective". In: *IEEEAccess* (2020). DOI: 10.1109/ACCESS.2020.2970143.

[45] Werner Kritzinger et al. "Digital Twin in manufacturing: A categorical literature review and classification". In: *IFAC-PapersOnLine* 51 (11 Jan. 2018), pp. 1016–1022. ISSN: 2405-8963. DOI: 10.1016/J.IFACOL.2018.08.474.

[46] MarketsandMarkets™. *Digital Twin Market Size Global forecast to 2026*. https://www.marketsandmarkets.com/Market-Reports/digital-twin-market-225269522.html. Accessed: 06.02.2022.

[47] Tolga Erol, Arif Furkan Mendi, and Dilara Dogan. "Digital Transformation Revolution with Digital Twin Technology". In: *4th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2020 - Proceedings* (Oct. 2020). DOI: 10.1109/ISMSIT50672.2020.9254288.

[48] Lindsay James. "Digital Twins will revolutionise healthcare". In: *E&T Magazine* 16 (2021), pp. 50–53.

[49] McKinsey & Company. *The top technology trends*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-top-trends-in-tech. Accessed: 07.02.2022.

[50] Maulshree Singh et al. "Digital Twin: Origin to Future". In: *Applied System Innovation* (2021). DOI: 10.3390/asi4020036. URL: https://doi.org/10.3390/asi4020036.

[51] Takehiro Nakamura. "5G Evolution and 6G". In: *Digest of Technical Papers - Symposium on VLSI Technology* 2020-June (June 2020). ISSN: 07431562. DOI: 10.1109/VLSITECHNOLOGY18217.2020.9265094.

[52] B. Sousa et al. "ELEGANT: Security of Critical Infrastructures With Digital Twins". In: *IEEE Access* (2021).

[53] A Rasheed, O San, and T Kvamsdal. "Digital Twin: Values, Challenges and Enablers From a Modeling Perspective". In: *IEEEAccess* (2020).

[54] M. van den Brand et al. "Models Meet Data: Challenges to Create Virtual Entities for Digital Twins". In: *2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)* (2021).

[55] Ahmet Mert Karadeniz et al. "Digital twin of egastronomic things: A case study for ice cream machines". In: *Proceedings - IEEE International Symposium on Circuits and Systems* 2019-May (2019). ISSN: 02714310. DOI: 10.1109/ISCAS.2019.8702679.

[56] Mojtaba Noghabaei et al. "Trend analysis on adoption of virtual and augmented reality in the architecture, engineering, and construction industry". In: *Data* 5.1 (2020), p. 26.

[57] Perkins Coie. *2021 XR Survey: Industry Insights Into the Future of Immersive Technology*. Tech. rep. Perkins Coie, 2021.

[58] Vahid Balali et al. "Improved stakeholder communication and visualizations: Real-time interaction and cost estimation within immersive virtual environments". In: *Construction Research Congress 2018*. American Society of Civil Engineers Reston, VA. 2018, pp. 522–530.

[59] Xiao Li et al. "A critical review of virtual and augmented reality (VR/AR) applications in construction safety". In: *Automation in Construction* 86 (2018), pp. 150–162.

[60] Francesca Bonetti, Gary Warnaby, and Lee Quinn. "Augmented reality and virtual reality in physical and online retailing: A review, synthesis and research agenda". In: *Augmented reality and virtual reality* (2018), pp. 119–132.

[61] Scott W Greenwald et al. "Technology and applications for collaborative learning in virtual reality". In: *CSCL*. Philadelphia, PA: International Society of the Learning Sciences., 2017.

[62] Wee Sim Khor et al. "Augmented and virtual reality in surgery—the digital surgical environment: applications, limitations and legal pitfalls". In: *Annals of translational medicine* 4.23 (2016).

[63] Wolfgang Vorraber et al. "Assessing augmented reality in production: Remote-assisted maintenance with HoloLens". In: *Procedia CIRP* 88 (2020), pp. 139–144.

[64] IDC. *Worldwide Spending on Augmented and Virtual Reality Forecast to Deliver Strong Growth Through 2024, According to a New IDC Spending Guide*. `https://www.idc.com/getdoc.jsp?containerId=prUS47012020`. Accessed: 05.02.2022. 2021.

[65] Research and Markets. *Global Healthcare Augmented Reality and Virtual Reality Market by Technology, Offering, Device Type, Application, End-user, and Region 2019-2026: Trend Forecast and Growth Opportunity*. Tech. rep. Research and Markets, 2019.

[66] Thorsten Wild, Volker Braun, and Harish Viswanathan. "Joint design of communication and sensing for beyond 5G and 6G systems". In: *IEEE Access* 9 (2021), pp. 30845–30857.

[67] Harish Viswanathan and Preben E Mogensen. "Communications in the 6G era". In: *IEEE Access* 8 (2020), pp. 57063–57074.

[68] Liang Gong, Åsa Fast-Berglund, and Björn Johansson. "A framework for extended reality system development in manufacturing". In: *IEEE Access* 9 (2021), pp. 24796–24813.

[69] Mojo Vision. *Mojo Lens: The World's First True Smart Contact Lens.* `https://www.mojo.vision/mojo-lens/`. Accessed: 07.02.2022. 2021.

[70] Umer Asghar Chattha et al. "Motion sickness in virtual reality: an empirical evaluation". In: *IEEE Access* 8 (2020), pp. 130486–130499.

[71] Yaping Sun et al. "Communications, caching, and computing for mobile virtual reality: Modeling and tradeoff". In: *IEEE Transactions on Communications* 67.11 (2019), pp. 7573–7586.

[72] Tseng-Lung Huang, Shane Mathews, and Cindy Yunhsin Chou. "Enhancing online rapport experience via augmented reality". In: *Journal of Services Marketing* (2019).

[73] Arsalan Heydarian et al. "Towards user centered building design: Identifying end-user lighting preferences via immersive virtual environments". In: *Automation in Construction* 81 (2017), pp. 56–66.

# Chapter 3

# Federated Learning for Sensitive Data

Ciritci, Yasin
Erhard, Johann
Hamzaoui, Soumaya
Khouni, Ahmed Haroun
Lee, Zach Ren
Ruidisch, Robert Michael
Tian, Ruiying

## Abstract

Since the world is becoming more connected, Internet users are subconsciously feeding the network with a tremendous amount of data. Meanwhile, many researchers and institutions are concerned and calling for more protection of sensitive data circulating in the network. For instance, the traditional centralized approach for training Artificial Intelligence (AI) models faces major challenges related to efficiency and security. On one side modern communication industry is looking for way to process and distribute sensitive data across the network, on the other hand maintaining a high level of security and data streaming is also essential to achieve our goal. Lately, a new Machine Learning (ML) distributed approach is considered to be a promising solution to empower and integrate safely AI in 6G, which is Federated Learning (FL). FL is a distributed AI approach that provides data, solution functions, and training models in heterogeneous and large-scale networks. In this report, we start with some facts about effective communication in federated learning. Then, we give four trends as a vision of how FL will impact the future network with respect to sensitive data. We review some methods for ensuring fairness and addressing sources of bias. Next, we use the healthcare system as a source of sensitive data and see how it is represented in data-driven models. Finally, we see how the costs of

security and privacy attacks on FL and centralized learning differ.

## 3.1 Introduction

Since internet and connected devices became more affordable and accessible, the usage of smartphones and the number of systems integrated with sensors has grown exponentially. As a result, a tremendous amount of data is daily generated. This phenomenon represents a big opportunity to solve many problems and cases. However, it is challenging to manipulate this large datasets in terms of efficiency and security. Therefore, researchers are currently on the run to find a new alternative to 5G: eventually 6G. For instance, 6G will be supported by a new era of AI: a new framework, in which the human intelligence is embedded inside the network. The integration of ML across wireless communication systems is appealing since the already existing ML models are working only on large scale centralized environment. The main problem in these systems is that the data rates of each single node are relatively identical, which does not allow us to adapt to the need of each user in the new wireless networks. Due to the delay constraints, limited bandwidths and poor network reliability, the centralized ML systems are not capable of supporting these new applications. In addition, data privacy and confidentiality in the centralized ML Systems is not guaranteed. Especially towards sensitive data such as social security numbers, health information, bank accounts, private images and locations etc. As many researchers and institutions [1] are calling for regulations and procedures to protect sensitive data circulation in the network, sensitive data should not be circulating online [2] [1].

This increases the need for exploring new machine learning methods that can efficiently handle distributed datasets. Traditional centralized ML schemes are not good candidates for such cases because they require the data to be transferred and processed in a central entity, which may not be possible to implement in practice due to the restrictions on sensitive data.

Therefore, it is now becoming primordial to find new machine learning solutions that can efficiently handle distributed datasets and models. This new strategy will tremendously diminish the computation power and the resource allocation, since the data streaming will be adapted to each user based on his specific needs. In addition, decentralized ML can significantly reduce the bandwidth and energy consumption by a better resource allocation to each channel [3]. Under these conditions, FL happens to be a potential candidate that can respond to these new challenges.

For instance, FL has a new approach, which consists of distributing the training process of the global model through local multiple data silos and entities. This helps to build a global ML model without necessarily oversharing the training data with the rest of the network nodes and users. Based on these facts, FL has a potential of building a wide range of applications related to wireless communication while maintaining a high level of security. In this report, we will go extensively through the challenges and open research topics of FL related to

wireless communication and the possible fields, where this new process can be implemented.

## 3.2 Trends

In this section, we will describe several trends that have an impact on federated learning with sensitive data.

### 3.2.1 Reducing Communication Cost for Federated Learning

Edge devices such as mobile phones are typical devices used in the training process of FL. Implementing FL efficiently on heterogeneous devices with different states such as network connectivity and stability is a challenge. While the computing power of the device increases rapidly, the delay caused by communication will become the bottleneck of training. Improving the communication efficiency of FL has been an active area of research. With the development of 6G services in the future, FL has the potential to be applied on a larger scale, facing an even more complex network environment [4] [5].

In recent years, several approaches have been proposed to reduce communication costs, some of which are inspired by the techniques applied to other ML methods. They can be categorized into two types:

i) Reducing communication overhead
Updates can be compressed by model compression methods, e.g., sparsification, quantization, or subsampling [6] [7]. In addition, the federated dropout is also considered in which a certain number of activation functions at a fully-connected layer are designed to be removed. The edge Stochastic Gradient Descent (eSGD) algorithm [8] is proposed. Only important gradients are selected to be transmitted to the server during each communication round.

ii) Reducing communication rounds
More local updates are performed using the Federated Averaging algorithm [9]. The communication cost can be further reduced by adding an intermediate server [10]. The convergence could be accelerated through learning also from other clients with a fixed global model[11]. The two-stream model introduced this technique.

**Facts**

- In internet connection, the download speed is faster than the upload speed. The uploads by the clients can be delayed [6].
- In the training progress that involves complex models, e.g., CNN, millions of parameters are comprised in each update [15].

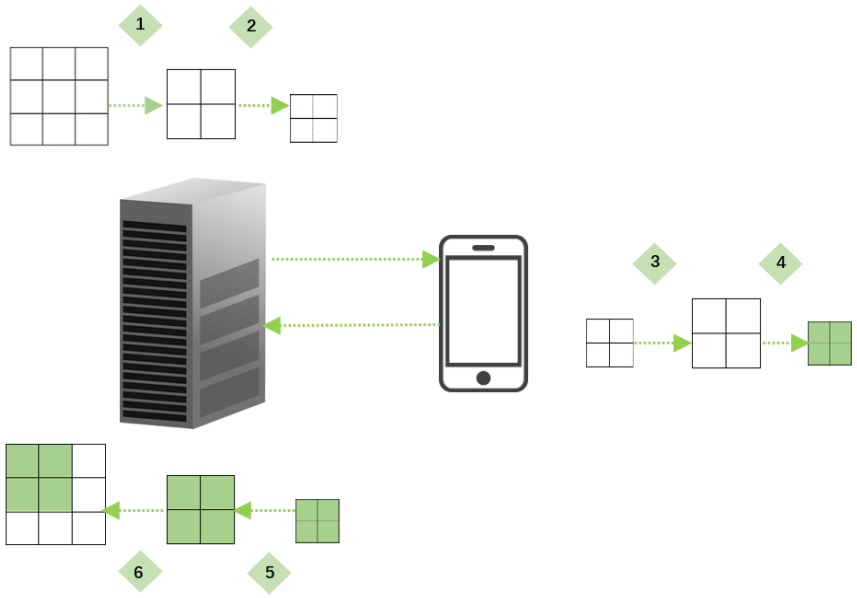


Figure 3.1: The figure above summarized the compression techniques proposed by the authors in [12]. (1) The size of the model is reduced via federated dropout (2) The model is compressed lossily (3) The model is sent to the client and decompressed (4) The participant updates are compressed (5) The model is decompressed (6) The model is aggregated into the global model.[13, 14]

- For MNIST CNN simulations using Independent and Identically Distributed (IID) data, the communication rounds can be reduced by more than 30 times with the FedAvg algorithm [9].
- The simulation results using both IID and non-IID data show that more aggregations at the edge server before the global aggregation in the cloud reduces more computation overhead compared to the FedAvg algorithm [10]. This intermediate server technique can be applied on top of the Federated Averaging algorithm.
- Model compression is commonly applied in distributed learning [15].
- Two-stream model is commonly applied in domain adaption [16] and transfer learning.

**Key Driver**

- Communication is a primary bottleneck of FL due to the characteristic of its framework. The network connection between such a large number of heterogeneous end devices is not as stable as the connection between data

centers involved in the distributed training. The reliability and the speed of the network connection are not guaranteed, and it can be potentially expensive. Reducing communication costs can be an effective method to improve training efficiency and scalability. Furthermore, the communication cost is often a more serious problem compared to computation cost [9].

**Challenges**

- In addition to the methods mentioned above, there are several other ways to reduce communication overhead. But many of them sacrifice on the accuracy or increase computation cost [17]. Weak process power of the edge devices can lead to a straggler effect. The convergence also needs to be considered. For example, when too many local updates are implemented between the communication rounds, the convergence is significantly delayed [18]. The tradeoff between these sacrifices and communication cost needs further evaluation.
- The combination of the methods mentioned above requires further exploration [18]. For example, the combination of the model compression and the edge server technique. The feasibility of this kind of combination needs to be evaluated.
- The non-IID data exacerbates the convergence issue. Multi-model methods such as multi-task learning can be solutions, which need future work [17].

**Impact**

- Reducing the communication cost can alleviate the efficiency bottleneck of the training caused by the unstable network connection by the clients.
- Reduced communication overhead makes the implementation of FL on a large scale more feasible.
- The author of [19] proved that compressed gradient can defend against gradient leakage attacks. The combination with the privacy methods can solve the user privacy issues at the same time.

### 3.2.2 Federated Learning: Ensuring Fairness and Addressing source of Bias

In the last decade, the variety of applications using ML and the importance of these applications has increased significantly. Today, ML is not only used in spam filtering or video recommendation, but also to make life-changing decisions in a variety of areas, ranging from hiring recommendations to courts decisions [20]. As ML invades our lives and can change our future, it is imperative to ensure that the created models are trustworthy and fair. Otherwise, they can cause harm and lead to discrimination.

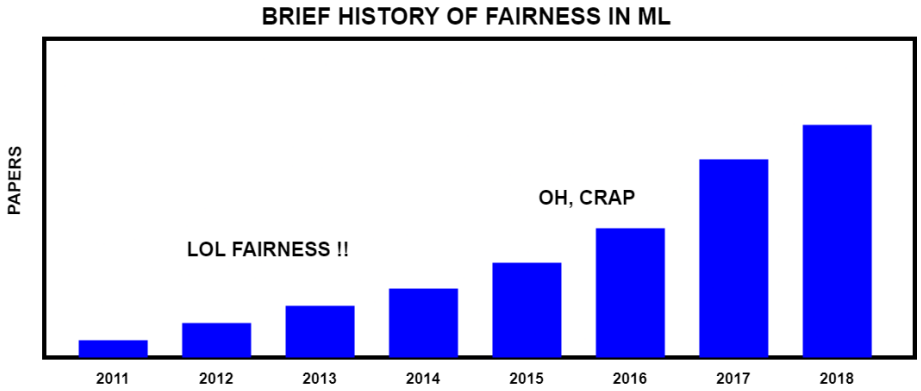


Figure 3.2: Fairness has become one of the most popular branches of ML in recent years. It has received a lot of attention from the research community.

Generally, fairness refers to avoiding biasing or favouring an individual or group based on their inherent or acquired characteristics. By analogy, an unfair algorithm is an algorithm whose decisions are biased in favour of a particular group of people [21].

ML algorithms depend heavily on training data and can be inadvertently susceptible to biases that lead to discriminatory and unfair incidents towards underrepresented group or minorities. Achieving fairness in the application of FL is still a major opportunity for research, as most existing work focuses on the interests of the central controller in FL and neglects the interests of clients. This "discourages clients from actively participating in the learning process and sustainability of the whole system" [22].

For instance, fairness in ML/FL requires access to personal and sensitive data. However, this is in contradiction with privacy notion, which FL normally guarantees to its users. For this reason, approaches and methods, that achieve fairness without access to sensitive data, need to be also explored. Furthermore, a trade-off between fairness and privacy needs to be found.

**Facts**

- Some ML algorithms used in well-known companies and government institutions show unfair and unethical behaviour. COMPAS, for example, a software used in American courts to help judges make decisions, shows discrimination against African-Americans [20].
- Latency can be a reason of bias in FL: datasets groups with powerful devices and networks maybe over-represented [22].
- Socioeconomic conditions can be a source of bias: populations without

devices or access to network are neglected in FL models.

- The idea of fairness is in opposition to the notion of privacy that FL claims to guarantee. Therefore, it is very challenging to find a compromise between them.

**Key Drivers**

- To achieve fairness without access to sensitive data, Distributed Robust Optimization (DRO) and calibration methods have been applied in the non-federated algorithms. DRO aims to optimize the outcome across all individuals in the training data and multicalibration, as the name suggests, calibrates subsets of data to obtain fair models [23].

- Research suggests to give fairness another definition so that it does not refer anymore to equalizing the probability of an outcome, but to equal access to effective models.

- In order to hide individual private data and realizing fairness at the same time, some techniques are applied in not federated settings such as personalization and hybrid differential privacy, which is based on the data donations of users with lesser privacy guarantees [24].

**Challenges**

- Studying the extent to which biases in the process of data generation can be detected or reduced is a challenging problem for research in the field of federal learning [24].

- As mentioned before, there is an intention to redefine fairness as an equitable model performance without access to sensitive data. However, providing equitable model performance in FL is still challenging.

- To reduce the tension between fairness and unavailability to sensitive data, DRO and multicalibration are used in the classical ML methods. However, they are inefficient in FL models. They cannot handle large-scale and high-dimensional data because they suffer from data scaling problem. For this reason, an improvement in these methods is required.

- To balance between privacy and fairness, more researches must take place. For instance, differentially private optimization algorithms must be improved so that performance of under-represented datasets is preserved [22].

**Impact**

- By achieving fairness without access to their private and sensitive data, FL models becomes trusted and used in a real population of customers. For example, they can be embedded in the 6G industry.

- By achieving fairness, companies and state institutions will increasingly rely on FL/ML models. In this way, bureaucracy will decrease noticeably.
- Achieving fairness in FL ensures that serious decisions are made without discrimination or favouritism, which can be achieved by human beings.
- Realizing fairness in the FL accelerates its integration in various fields such as the 6G network

### 3.2.3 Representative Data-Driven Models in Healthcare Systems

Data-driven algorithms such as ML and Distributed Learning (DL) have become a significant tool in many fields such as image classification in the computer vision field, speech recognition and machine translation in the natural language processing. Ideally, these algorithms would be widely used in all sectors, as they are promising methods in solving large and complex problems. However, this is not the case as some data such as medical, military and financial records are highly sensitive and cannot be used without the owner's consent.

For instance, in the healthcare industry, medical data are sensitive to privacy and security issues thus directly collect them in one location to train a generalized global model is infeasible. This becomes the bottleneck of intelligent healthcare systems, as the local data are not enough to represent the global data distribution, which results in a model that does not generalize well.

FL is a viable solution to train a sensitive data-driven model without conceding confidentiality. In this learning framework, only information such as model parameters and gradients are shared, but not the confidential raw data itself. As a result, it opened the door to ample of research, especially in the healthcare sector. FL also shows promising potential in realizing intelligent healthcare system by including various sources of medical information (Fig. 3.3).

**Facts**

- Real world healthcare data is available in the form of the Electronic Health Record (EHR) and has been used for an amalgamation of important biomedical research [33].
- Numerous FL-based researches in healthcare systems have been done and show a comparatively better performance than the traditional ML models [25].
- ML-based approaches have the potential to revolutionize the field of medicine and help in the development of precision medicine [34].
- Obermeyer et al. [35] found evidence of racial biases in a commonly used health algorithm against African Americans, assigning the same level of risk to healthier Caucasian patients.

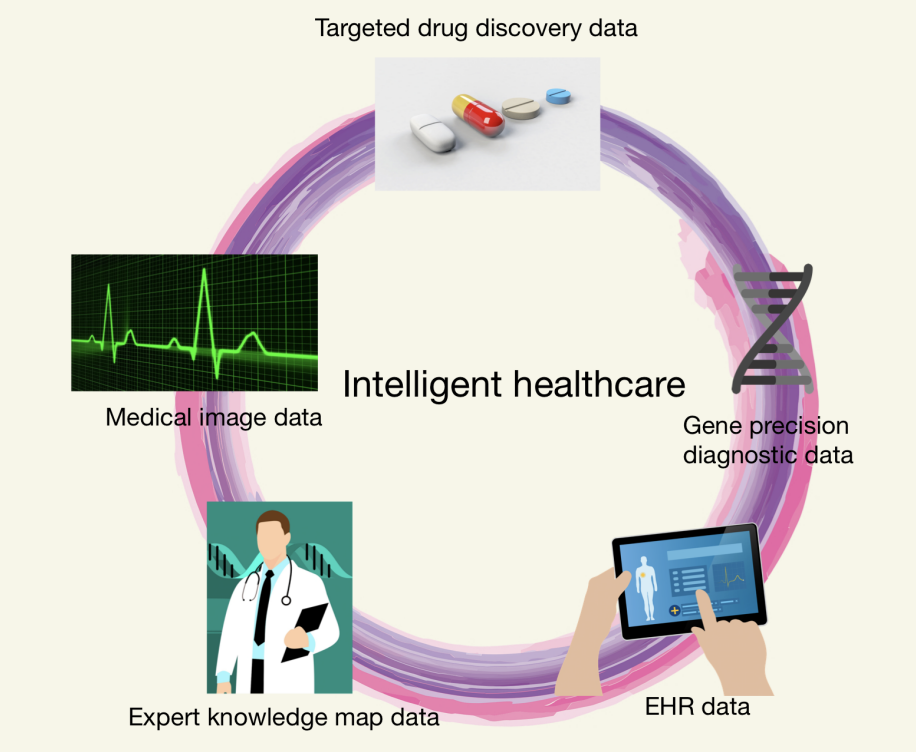


Figure 3.3: Federated smart diagnosis in the healthcare [25, 26] [27, 28, 29, 30, 31, 32].

**Key Drivers**

- DL is decentralized in FL by eliminating the necessity to pool data into a solitary place.
- Increasing concerns on user's privacy. According to the Internet Society and Consumers International, 69% of consumers are concerned about how personal data is collected in 2019 [36].
- Various data privacy laws and regulations such as GDPR in European Union, HIPAA/CCPA in the United States of America, and PIPDEA in Canada limit the performance of conventional ML and DL models.
- Various medical data like symptoms of diseases, medicinal reports as well as gene structures in a single institution are often not representative and prone to demographical, geographical and racial biases.
- With the development of wearable technology, smartphone, wristbands, and smart glasses provide easy access to user's daily activities and health information [37].

- More and more healthcare data are becoming readily available from clinical institutions, patients, insurance companies and pharmaceutical industries due to rapid development of computer software and hardware technologies [38].

### Challenges

Despite promising results of FL in healthcare systems, it does not solve all inherent issues from learning on medical data. Realizing and integrating it in real world applications is faced with following challenges [39, 38]:

- Data
  Data heterogeneity: Certain sources of bias may be addressed by FL, but inhomogeneous data distribution poses a hindrance for FL algorithms and strategies due to the assumption that the data are identically distributed across all the participants. Besides, data heterogeneity may also lead to situations where global optimal solution are suboptimal for the local participants.
  Data Quality: Although FL has the potential to connect isolated data from medical institutions, hospitals or devices, these data from multiple different sources are uneven and there is no uniform data standard. This results in data clutter and efficiency problems.

- Privacy and Security
  It is crucial to know that FL does not solve all the privacy and security issues from conventional Machine Learning approaches, as data-driven algorithms in general always carry some risks. There are multiple privacy preserving techniques in FL, but they come with a performance trade-off, for example in the accuracy of the final model [40].

- Traceability and Accountability
  Application of FL in healthcare systems is safety-critical, thus reproducibility of the systems is at utmost importance. Due to the nature of decentralized training in FL, traceability of all system assets including data access history, training configurations, and hyperparameter tuning throughout the training processes is thus difficult. This issue should be further researched to increase explainability and interpretability of the global model.

- Incentive Mechanism
  During FL training process, clients (especially owners of wearable devices) suffer from additional communication and computation overhead. A well-designed incentive mechanism has to be implemented to attract clients to participate and contribute in the FL system.

**Impacts**

FL provides a promising approach in adopting data-driven algorithms and realizing intelligent healthcare systems. This brings huge impacts to all the stakeholders in the FL ecosystems [25, 39].

- Clinicians
  Clinicians are usually only exposed to a certain subgroup of populations, depending on the demographic and location of their working environment. This leads to biased assumptions while making clinical decisions. By using FL-based systems, this problem can be alleviated given a large enough and representative training data. Besides, FL-based systems has the potential to be more sensitive to rare cases as it is exposed to a more complete data distribution.

- Patients
  Establishing a FL-based healthcare systems can ensure high quality medical diagnosis and treatment regardless of the patients' location.

- Hospitals and Practices
  Hospitals and Practices have full control in the usage of patients' data, thus limiting the risk of misuse by third parties. Furthermore, small hospitals can also benefit from the expert-level AI techniques resulting from the globally trained FL model.

- Researchers and AI Developers
  Researchers and developers can focus on solving clinical needs and associated technical problems without relying on limited open-sourced data.

### 3.2.4 Reducing the Cost of Countermeasures to Security and Privacy Attacks on Federated Learning

The FL framework seems like a secure method for ML by design. In any scenario, edge devices, that produce the data, are also responsible for training the model on their own device. Then, the produced local model updates, e.g., gradient information, are shared between the peers to generate a global model. (Fig. 3.4) In centralized FL, this is typically done by a model manager, i.e., server, but general attacks on the framework can be adapted to other frameworks [41]. Attacks can be generalized into two categories: security attacks, and privacy attacks. Security attacks are designed to influence the training process itself to prevent the global model from converging. This is possible by utilizing the Byzantine and poison attack models (Fig. 3.4 C) [42]. Attacks on privacy aim to extract personal information about contributors and datasets by inferring memberships and properties (Fig. 3.4 A, B) [43, 44]. To counteract those flaws, many protection algorithms were developed to be applied to FL. However, they also take a toll on the model and device performance, which leads to longer convergence times and therefore more communication costs. [41] Reducing the cost of those countermeasures and balancing them against security and privacy

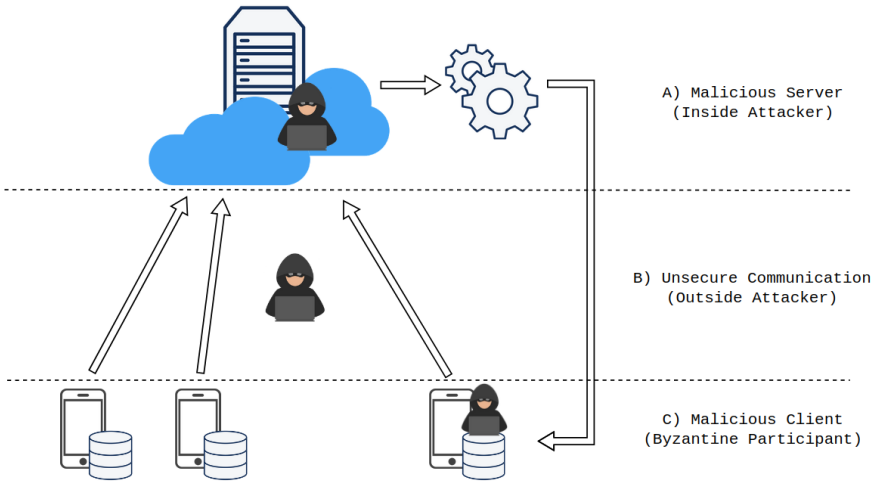


Figure 3.4: Overview over possible attackers in a centralized FL framework [45] [13, 46, 47, 48]

aspects will be a future trend to bringing the framework back to its original motivation of providing a scalable and secure ML framework to the community.

**Facts**

- The FL framework is vulnerable to security attacks by design. Because the model manager only knows parameters without their related data, it cannot decide if a client is malicious or not. Countermeasures against security attacks are therefore necessary [42].

- Countermeasures against security attacks, e.g., increasing the size of epochs and clients, including good client selection, and detecting malicious clients via model metrics and update statistics, can require significant additional computation and communication costs, and reduce the model accuracy [41].

- Although only parameters are shared, FL can still be attacked by inferring parameters to properties and memberships. Countermeasures against privacy attacks are therefore necessary, i.e., Secure Multiparty Protocol (SMC), and Differential Privacy (DP) [41].

- SMC is an encryption-based secret sharing protocol that protects the individual's privacy in a lossless manner. However, significant extra communication cost is needed. Countermeasures against Poison and Byzantine attacks become ineffective [41].

- DP distorts client updates to protect the individual's privacy by adding controlled noise to the input or the output of the training process. However, DP significantly affects the accuracy of the global model [41].

### Challenges

Until now, there are many countermeasures against attacks on FL. However, most of them do not take others into account or shift the problem to other fronts. This makes reducing the cost of countermeasures of each one very challenging. To solve the problem of achieving a framework that is secure against both security and privacy attacks, there are many challenges to overcome [5, 17, 41].

- Ensuring privacy and security at the same time: Many protocols developed for protecting against attacks are focused on one major aspect alone and disregarding their effects on others. This makes their combination into a united protection strategy difficult. Finding such a united protection protocol is one of the key challenges [41].
- The solution to an effective aggregation strategy could be the use of a performant anonymous communication protocol. However, such a protocol, similar to SMC is still yet to be successfully designed [41].
- Reducing communication cost: Ultimately, most algorithms protecting against attacks raise the communication cost, between server and client, and between client and client. However, reducing the cost of communication is not a trivial task, that is part of research on its own [17, 41] (Chap. 3.2.1).

### Key Drivers

To reduce the cost of countermeasures, a unified framework against attacks on FL could be the solution. There are a few key drivers that are part of the current research in this field to solve this problem.

- Peer-to-Peer multi-hop forwarding protocol: Such a protocol aims to create an anonymous communication channel between client and server. Because in FL, attacks originating from a malicious server cannot be excluded, a truly secure end-to-end communication would not be helpful. However, utilizing a server to share and compute the global model is a useful tool in ensuring edge device independence. Therefore, a peer-to-peer forwarding mechanism has been proposed that uses multiple random hops to a peer before forwarding the parameters to the server. This way, a lossless and secure channel between client and server renders attacks on both sides ineffective [41].
- Incentive system: To make such a protocol viable, it is suggested to add artificial incentives for peers to share their data. This way, a client with

a good reputation is more likely to forward the data of other peers to the server. However, such metrics have not been designed successfully yet [41].

- Communication cost: Similar to the SMC protocol, peer-to-peer multi-hop protocols require additional communication between peers. However, the communication overhang of this approach is significantly lower than that of SMC. Still, this motivates to reduce the communication cost to ensure such protocols can work effectively [17, 41] (Chap. 3.2.1).

**Impact**

A solution to reducing the cost of countermeasures against attacks on FL is part of the current research. However, it is also important to look at its place and impact on the overall future development of FL.

- Reducing the cost of countermeasures requires implementing a unified system against both security and privacy attacks. This renders many other developed protocols and algorithms unused.

- Most methods discussed in this chapter focus on the implementation of centralized FL with a model manager. However, there are also other approaches, e.g., fully decentralized FL that are discussed. The algorithms above would not be applicable in such a scenario.

- Overall, if FL is to be implemented in a server-client-based approach, the usage of a performant anonymous communication protocol that unifies protection against privacy and security is essential. Only then can the extent of the cost of countermeasures against protection algorithms be rated and solved completely.

## 3.3 Conclusion

Throughout this report, we demonstrated how FL can be used to leverage the challenges in the future wireless communication networks through four different trends that can have an impact on the future networks and sensitive data. We started off with the importance of the communication cost in FL and the urge of reducing the costs. The challenge here is to balance between the costs and efficiency and many factors. Distributed or centralized, ML has always been under the loop when it comes to fairness due to several incidences of segregation and racism. Many techniques are used to prevent these problems, such as DRO. However, they are not effective in FL, since they are destinated to large scaled data.

Next, we study the impact of FL on the modern healthcare system. Despite all the advantages of FL, privacy is still an issue that needs to be discussed. Considering that FL started to get attention in the medical research field only

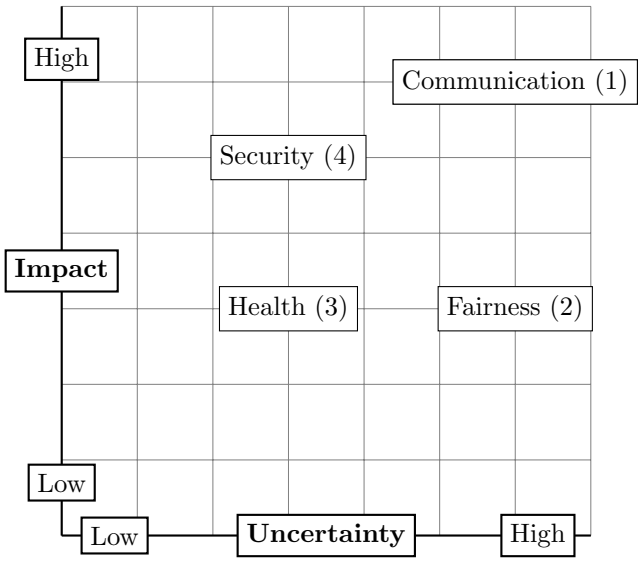


Figure 3.5: Driver matrix

since 2016, it is too early to make assumptions about the performance. However, experts estimate a good global benefit for the health care system from FL.

We highlighted the costs and unification of countermeasures to security and privacy attacks on centralized federated learning. We introduced many classical strategies to counteract attacks on security and privacy, such as byzantine and poison attack models, cannot resist against the actual cyberattacks. Therefore, The alternative is using a unified anonymous communication protocol based on Peer2Peer forwarding, which will guarantee an anonymous communication, more security and feasibility in the future.

Throughout the Driver matrix, we summarized the different direction, which FL can take in the future and plotted them impact-wise. You can see for every trend how likely it will be implemented and how much impact it will have. In terms of uncertainty, Communication and Fairness need to be searched further. On the other hand, the impact of Security and Healthcare is relatively low, while the impact of Security is more severe. However, all these trends will have definitely a good impact on the future network, namely for Communication and Security.

# References

[1] Emmanuel Femi Gbenga Ajayi. “Challenges to enforcement of cyber-crimes laws and policy”. In: *Journal of Internet and Information Systems* 6.1 (2016), pp. 1–12.

[2] Graham Greenleaf. "Global data privacy laws 2019: 132 national laws & many bills". In: (2019).

[3] Solmaz Niknam, Harpreet S Dhillon, and Jeffrey H Reed. "Federated learning for wireless communications: Motivation, opportunities, and challenges". In: *IEEE Communications Magazine* 58.6 (2020), pp. 46–51.

[4] Z Yang et al. "Federated Learning for 6G: Applications, Challenges, and Opportunities. arXiv 2021". In: *arXiv preprint arXiv:2101.01338* ().

[5] Yi Liu et al. "Federated learning for 6G communications: Challenges, methods, and future directions". In: *China Communications* 17.9 (2020), pp. 105–118.

[6] Jakub Konečn et al. "Federated learning: Strategies for improving communication efficiency". In: *arXiv preprint arXiv:1610.05492* (2016).

[7] Song Han, Huizi Mao, and William J Dally. "Deep compression: Compressing deep neural networks with pruning, trained quantization and huffman coding". In: *arXiv preprint arXiv:1510.00149* (2015).

[8] Zeyi Tao and Qun Li. "esgd: Communication efficient distributed deep learning on the edge". In: {*USENIX*} *Workshop on Hot Topics in Edge Computing (HotEdge 18)*. 2018.

[9] Brendan McMahan et al. "Communication-efficient learning of deep networks from decentralized data". In: *Artificial intelligence and statistics*. PMLR. 2017, pp. 1273–1282.

[10] Lumin Liu et al. "Client-edge-cloud hierarchical federated learning". In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.

[11] Xin Yao, Chaofeng Huang, and Lifeng Sun. "Two-stream federated learning: Reduce the communication costs". In: *2018 IEEE Visual Communications and Image Processing (VCIP)*. IEEE. 2018, pp. 1–4.

[12] Sebastian Caldas et al. "Expanding the reach of federated learning by reducing client resource requirements". In: *arXiv preprint arXiv:1812.07210* (2018).

[13] IO-Images. *smartphone-mobile-phone*. [Online; accessed 04-February-2022]. URL: `https://pixabay.com/images/id-1132675/`.

[14] OpenClipart-Vectors. *server-computer-mainframe*. [Online; accessed 04-February-2022]. URL: `https://pixabay.com/images/id-146615/`.

[15] Kaiming He et al. "Deep residual learning for image recognition". In: *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2016, pp. 770–778.

[16] Mingsheng Long et al. "Learning transferable features with deep adaptation networks". In: *International conference on machine learning*. PMLR. 2015, pp. 97–105.

[17] Wei Yang Bryan Lim et al. "Federated learning in mobile edge networks: A comprehensive survey". In: *IEEE Communications Surveys & Tutorials* 22.3 (2020), pp. 2031–2063.

[18] Yang Liu et al. "A communication efficient collaborative learning framework for distributed features". In: *arXiv preprint arXiv:1912.11187* (2019).

[19] Ligeng Zhu, Zhijian Liu, and Song Han. "Deep leakage from gradients". In: *Advances in Neural Information Processing Systems* 32 (2019).

[20] Jeff Larson et al. "How We Analyzed the COMPAS Recidivism Algorithm". In: (2016).

[21] Ninareh Mehrabi et al. "A survey on bias and fairness in machine learning". In: *ACM Computing Surveys (CSUR)* 54.6 (2021), pp. 1–35.

[22] Peter Kairouz et al. "Advances and open problems in federated learning". In: *arXiv preprint arXiv:1912.04977* (2019).

[23] Tatsunori B. Hashimoto et al. *Fairness Without Demographics in Repeated Loss Minimization*. 2018. arXiv: 1806.08010 [stat.ML].

[24] Brendan Avent et al. "BLENDER: Enabling Local Search with a Hybrid Differential Privacy Model". In: *Journal of Privacy and Confidentiality* 9.2 (Sept. 2019). ISSN: 2575-8527. DOI: 10.29012/jpc.680. URL: http://dx.doi.org/10.29012/jpc.680.

[25] Yogesh Kumar and Ruchi Singla. "Federated Learning Systems for Healthcare: Perspective and Recent Progress". In: *Federated Learning Systems*. Springer, 2021, pp. 141–156.

[26] Songtao Lu et al. "Learn electronic health records by fully decentralized federated learning". In: *arXiv preprint arXiv:1912.01792* (2019).

[27] mcmurryjulie. *ehr-emr-electronic-medical-record*. [Online; accessed 04-February-2022]. URL: https://pixabay.com/images/id-1476525/.

[28] qimono. *pill-capsule-medicine-medical*. [Online; accessed 04-February-2022]. URL: https://pixabay.com/images/id-1884775/.

[29] mcmurryjulie. *gene-icon-genetics-icon-dna-icon*. [Online; accessed 04-February-2022]. URL: https://pixabay.com/images/id-3184531/.

[30] PublicDomainPictures. *pulse-trace-healthcare-medicine*. [Online; accessed 04-February-2022]. URL: https://pixabay.com/images/id-163708/.

[31] mohamed_hassan. *analysis-hospital-doctor-medical*. [Online; accessed 04-February-2022]. URL: https://pixabay.com/images/id-3707159/.

[32] rldkridel. *watercolor-circle-paint-artistic*. [Online; accessed 04-February-2022]. URL: https://pixabay.com/images/id-4525735/.

[33] Riccardo Miotto et al. "Deep learning for healthcare: review, opportunities and challenges". In: *Briefings in bioinformatics* 19.6 (2018), pp. 1236–1246.

[34] Zeeshan Ahmed et al. "Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine". In: *Database: The Journal of Biological Databases and Curation* 2020 (2020).

[35] Ziad Obermeyer et al. "Dissecting racial bias in an algorithm used to manage the health of populations". In: *Science* 366.6464 (2019), pp. 447–453.

[36] A Goswami. *The rising concern around consumer data and privacy.* 2020.

[37] Yiqiang Chen et al. "Fedhealth: A federated transfer learning framework for wearable healthcare". In: *IEEE Intelligent Systems* 35.4 (2020), pp. 83–93.

[38] Jie Xu et al. "Federated learning for healthcare informatics". In: *Journal of Healthcare Informatics Research* 5.1 (2021), pp. 1–19.

[39] Nicola Rieke et al. "The future of digital health with federated learning". In: *NPJ Digital Medicine* 3 (2020).

[40] Tian Li et al. "Federated learning: Challenges, methods, and future directions". In: *IEEE Signal Processing Magazine* 37.3 (2020), pp. 50–60.

[41] Alberto Blanco-Justicia et al. "Achieving security and privacy in federated learning systems: Survey, research challenges and future directions". In: *Engineering Applications of Artificial Intelligence* 106.September (2021), p. 104468. ISSN: 09521976. DOI: 10.1016/j.engappai.2021.104468. URL: https://doi.org/10.1016/j.engappai.2021.104468.

[42] Eugene Bagdasaryan et al. "How To Backdoor Federated Learning". In: 108 (2018). arXiv: 1807.00459. URL: http://arxiv.org/abs/1807.00459.

[43] Mathias Parisot, Balázs, and Dayana Spagnuelo. "Property inference attacks on convolutional neural networks: Influence and implications of target model's complexity". In: *Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021* (2021), pp. 715–721. DOI: 10.5220/0010555607150721. arXiv: 2104.13061.

[44] Reza Shokri et al. "Membership Inference Attacks Against Machine Learning Models". In: *Proceedings - IEEE Symposium on Security and Privacy* (2017), pp. 3–18. ISSN: 10816011. DOI: 10.1109/SP.2017.41. arXiv: 1610.05820.

[45] Nguyen Truong et al. "Privacy preservation in federated learning: An insightful survey from the GDPR perspective". In: *Computers and Security* 110 (2021), p. 102402. ISSN: 01674048. DOI: 10.1016/j.cose.2021.102402. arXiv: 2011.05411. URL: https://doi.org/10.1016/j.cose.2021.102402.

[46] 200degrees. *download-upload-cloud-internet.* [Online; accessed 04-February-2022]. URL: https://pixabay.com/images/id-1745473/.

[47] Hnnng. *hacker-hacking-theft-cyber-malware*. [Online; accessed 04-February-2022]. URL: `https://pixabay.com/images/id-5151533/`.

[48] OpenClipart-Vectors. *computer-data-database-diagram*. [Online; accessed 04-February-2022]. URL: `https://pixabay.com/images/id-1294359/`.

# Chapter 4

# Generalization in Machine Learning and 6G

Chaabouni, Zeineb
Fuchs, Florian
Gan, Lisa
Klama, Tobias
Krug, Tobias
Schölles, Alexander Hoàng
Stümke, Daniel

## Abstract

What is Love? That question is still to be answered by R.E.M. Pun aside, humanity as a whole places an increasingly high hope into the beneficial use of AI to solve arbitrary problems. This is largely promoted by the positive impact many people experience in their lives on a daily basis: smoke-detectors, image quality enhancement and chess training software may be some of the examples that might come to one's mind. Current-era communication technology on the other hand largely relies on conventional approaches. This trend report sets out to uncover the role Generalization could play to pave the way for AI in the emerging communication standard 6G. As we will show, Generalization might be looming closer on the horizon than expected, could have direct access and impact on end-users and should strive to improve equitable technology access for everyone—and everything.

## 4.1 Introduction

Commonly, there are two definitions for the term generalization which are most often employed:

1. Expected performance of an AI model on unseen data different from training data.

2. Capability of an AI model to devise new, useful actions on unseen data.

While the former is easier to grasp, the latter introduces more severe problems. Therefore literature usually discusses the former: "Does my apple detector understand oranges are no apples?", "Is my automated car able to distinguish a marketing flag from a traffic light?" or "Will my robo vacuum try to vacuum my baby?" are questions that express the concerns of the first definition.

The second definition includes more abstract problems, that could read like "Will my automated car be able to detect my desire to buy me a PS5 while I sleep during the drive to work? Will it be able to avoid scalpers when buying one? Can it arrange a route to collect the delivery? Can it inform Joe to visit in the evening for an often discussed game night?" This class of problems is notably more vague, while incorporating a large number of involved parties, actions and interfaces.

In the subsequent section, we set out to close the information gap on the current state of affairs of the broader definition of generalization. We will put a special focus on the interdependence of generalization and the evolving 6G technology. In general, additionally to 6G, all application areas benefit from better generalization. Further 6G enables much more broader and numerous data collection activities to help the whole field in developing better and more broadly applicable AI solutions.

## 4.2 Trends

Generalization is one of the long-term aspirations of (computer) scientists. As early as 1950, the great Alan Turing proposed "The Imitation Game" [1, p. 1] as a test to assess the generalization capabilities of a "machine". Nowadays, the question is covered in an array of papers and allows a specific view with an application-specific perspective. Our perspective shall be the emerging field of 6G and its prospective ML constituents. Inspired by surveys with a broader scope on the challenges and solutions to 6G ([2], [3]) we will present a number of specific trends that emphasize the importance of research into generalization to make 6G a worthwhile undertaking.

### 4.2.1 Artificial General Intelligence

This trend on Artificial General Intelligence (AGI) considers the quest to build a system, which shows a capability to solve problems beyond a narrowly scoped area. Different minds tackle it differently. According to [4], such a system would be required to mimic his system of four pillars of human learning—namely Attention, Active Engagement, Error Feedback and Consolidation—to get even close to human level intelligence.

Judea Pearl on the other hand points to two other perspectives when he says he believes "that the software package that can give a thinking machine the benefits of agency would consist of at least three parts: a causal model of the world; a causal model of its own software, however superficial; and a memory that records how intents in its mind correspond to events in the outside world." [5, p. 367] and that "It means that we should equip thinking machines with the same cognitive abilities that we have, which include empathy, long-term prediction, and self-restraint, and then allow them to make their own decisions." [5, p. 370].

### Facts

To assess the use cases and impacts of AGI in 6G, we first give an insight into recent developments in the direction of AGI. Research groups such as Google Brain or Deep Mind, who are specialized in Machine Intelligence research, are working towards AGI solutions and recently introduced new forms of Neural Networks, namely *Capsule Network (CapsNet)* and *Ponder Net (PN)*. Both are a step towards a more generalized AI approach.

Current amibtions to implement AGI are eg. done by the OpenCog Foundation which tries to provide an open-source software platform for AGI. The project launched in 2008 and according to its website aims "to create a thinking machine with human level intelligence and beyond" with the ultimate goal of artificial general intelligence [6] [7]. OpenCog uses a so called atomspace which is a knowledge base built out of (hyper)graphs. The OpenCog architecture consists of different specialised algorithms which are working together. These are logic reasoner, genetic program learner, pattern matcher and natural language subsystem, which use Neural Networks (NNs) and Reinforcement Learning (RL) to achieve features like attention, creativity and action selection. Since the human brain also uses different specialised areas for different tasks this approach seems promising. Since August 2021 the development of a new version started, the OpenCog Hyperon which tries to exceed its predecessor particularly in scalability [7].

OpenCog is aimed to be the core AI of SingularityNet, a decentralized AI-platform to allow AIs to interoperate with the goal to create a system with broader capabilities [8].

### Key Drivers

### Capsule Networks

CapsNets, introduced by Hinton et al.[9], are an extension to conventional Convolutional Neural Networks (CNNs) and focus on robustness to spatial relations between different objects and therefore try to increase data efficiency through improved data exploitation.

Similar to standard NNs, which are built from layers of neurons, CapsNets are built from layers of *'capsules'*. Each of these capsules consists of a group

of neurons and therefore has vectors as inputs and outputs. Each vector encodes various properties of some entity that is present in the image. Here, the vector's orientation represents the properties of the entity, while the vector's norm expresses the confidence that the entity is present. Further, this vectorized form allows using a powerful *'dynamic routing by agreement'* mechanism for the forward pass through the network [9].

Other than the distinct architectural difference to conventional CNNs, CapsNets focus on equivariance instead of invariance. This means that no matter what rotation, position, etc. an object has in an image, the network outputs the same.

According to Hinton et al. [9], CapsNets deliver state-of-the-art performance on the MNIST data set. Moreover, in a more recent work of Keselj et al. [10] the authors stated that based on their experiments, CapsNets are still very new and unlikely to work on tasks other than digit classification. But there is significant potential for them to be improved and made useful [10]. An example for a communication network application could be to use the CapsNet idea to be more robust against different mobile phone brands and software systems when building ML models, such that no extra training data for different types of phones and software is required. This could reduce the overall effort for data collection and training, while maintaining performance.

**Ponder Net**

The idea behind PN is to expand a NN to learn to adapt the amount of computation based on the complexity of the input [11]. In essence, more (computational) resources are allocated to inputs that are more complex to process. This process of *'pondering'* is already employed by NN researchers daily when choosing the number of hidden layers and neurons, or when deciding on how many Graphics Processing Units (GPUs) to use depending on the problems' complexity.

The PN environment is a supervised setting that modifies the forward pass and defines a new loss function for training. It is based on previous work of Adaptive Computation Time (ACT), where the algorithm automatically learns to scale the required computation time via a halting probability [12].

PNs' architecture requires a step function $y_n, h_{n+1}, \lambda_n = s(x, h_n)$ [11]. It can process the input to a NN multiple times, where in each pass it outputs the prediction $y_n$, the halting probability $\lambda_n$ for step n, and an updated hidden state $h_{n+1}$. To decide whether to *'halt'* or *'continue'* it then samples from the halting Bernoulli random variable $\lambda_n$. If a *halt* outcome is sampled, the final prediction of the network becomes $y = y_n$. Note that during training a bound on the pondering steps is required, but during interference, no explicit bound is needed (but still advisable). The results in Banino et al. [11] show highest accuracy in different complex domains.

An advantage of PN is to use the network's ability to ponder, to reduce the amount of computation and energy usage at inference time. Especially devices with a limited amount of resources, such as mobile phones, can profit from this feature [11]. Additionally, the authors in [11] identified that PNs bring

a performance gain in real-world problems due to their ability to adapt their computational complexity. Lastly, it is fairly easy to adapt existing networks to work with PN.

### SingularityNET

The SingularityNET is a framework based on blockchain and is designed to serve AI agents that are interacting with each other and with external customers. It allows the AIs to interoperate in order to create a more synergistic and general intelligence that is broadly applicable. The framework can be thought of as a mesh of disparate elements into a collective intelligence, much like the human brain [8].

### Challenges

One big, maybe the biggest, challenge for AGI is computational feasibility. There are already theoretical solutions for AGI systems and Hutter already defined a kind of optimal solution for an arbitrary reward function in a random environment [13]. However this so-called AIXI cannot be practically implemented since this solution is not computable. Altogether there are a few approaches for AGI but there still is no consensus for an accepted definition in the field [14]. It is necessary to find feasible approximations and algorithms to theoretical solutions such that implementations with current hardware and data limitations become viable.

Due to the complexity and variety of tasks and problems at hand, an AGI agent must be able to learn from fewer data than conventional NNs. This leads to many challenges which have to be dealt with. Where

- bias of small, incomplete data patches,
- distinction between causality and correlation in limited data,
- identification of most important features

are just a few of them.

A whole different class of challenges is, premised the implementation difficulties are overcome, the ethics aspect of an AGI. There are already several dystopian science fiction stories like [15] which show potential evolution of AGIs. The insight that humans are all-destroying parasites on earth which have to be extinguished to guarantee existence of life on earth seems, climate-change and menacing nuclear warfare at hand, not too far-fetched. Who knows what potentialities an AGI can find to achieve this?

### Impact

The previous analysis of the AGI trend leads us to assume that meaning could be a relevant quality of any AGI system, which is also supported by Hashagen

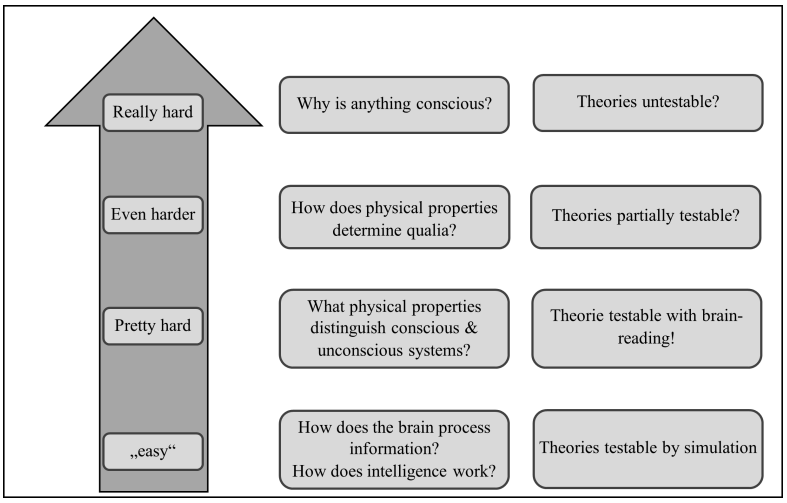


Figure 4.1: Problem hierarchy to uncover the mind [19, p. 285]

et al. [16, pp. 167-175] This is especially obvious when considering the negative impacts powerful technology like AGI could have, e.g. potentially causing a dystopian caste system. [17] If meaning is considered, AGI could improve the lives of many people by providing better communication infrastructure, solutions to unknown problems and overall more fair and equitable access to life-augmenting systems. Furthermore, the future could see the advent of man-machine teams bound to surpass each one's individual performance. [18, pp. 227ff.]

For the time being, the question of Max Tegmark dating back to 2017 is still unanswered, though: "[...] why is anything conscious?" [19, p. 286] To answer it, we will likely need to climb the ladder he proposed in Figure 4.1.

### 4.2.2 Edge Artificial Intelligence

The availability of Edge Artificial Intelligence (EdgeAI) capabilities will mark one of the major differences between current 5G and future 6G networks [20]. While the AI-based applications of today majorly rely on centralized intelligence, future AI models will reside not too far away from the user. Autonomous driving vehicles for example, will not request a central server in order to make lane change decisions or to recognize road signs but they will be capable to do those tasks locally with their own computational power. This transition will be made for a variety of reasons, ranging from technical aspects like scalability and power consumption to novel concepts for connected intelligence which will enhance prediction performance and generalization abilities.

In order to arrive at a fully functional EdgeAI, many novel ideas are being researched. The combination of self-learning techniques and EdgeAI [21] or the usage of Reconfigurable Intelligent Surfaces [22] are just two interesting

examples out of many more research topics in that area.

**Facts**

- It is estimated that the 6G network will have to support over 125 Billion devices by 2030 [21].
- A differentiation into AI for edge (intelligence-enabled edge computing) and AI on edge (artificial intelligence on edge) can be made [23].
- According to a prediction, 45% of the global Internet data will be generated by the Internet of Things (Iot) devices in 2024, so offloading is intractable [23].
- Machine learning methods can be split and deployed on numerous devices in different ways (data splitting, model splitting, federated learning) [23].

**Key Drivers**

- Many key technologies like the Intelligent Internet of Things (IIot), autonomous vehicles or Augmented Reality (AR) are based on AI and have high requirements in terms of latency, accuracy and security [24].
- Case studies show applicability of EdgeAI for semantic tasks [25] and Simultaneous Localization and Mapping (SLAM) [26].
- Digital twins will be an essential part of smart manufacturing systems. Edge AI can be used to model and deploy digital twins in IIot networks [27].
- Wireless communication networks will no longer just provide a connection but will bring the need to properly authenticate parties, guarantee the security of data fluxes (maybe via blockchain), and recognizing in real time abnormal behavior which leads to increased demands for wireless networks, more data transfer and processing [20].

**Challenges**

- Building a standardized edge AI management and orchestration framework may not be feasible [27].
- Limited storage, computation and communication resources in wireless networks require a paradigm shift. Data oriented communication has to be replaced with task oriented communication in order to achieve fast and accurate intelligence at the network edge [27].
- EdgeAI is by design decentralized and distributed, but most modern AI methods are not suited for such architectures yet or they are just in an early stage of adoption [24].

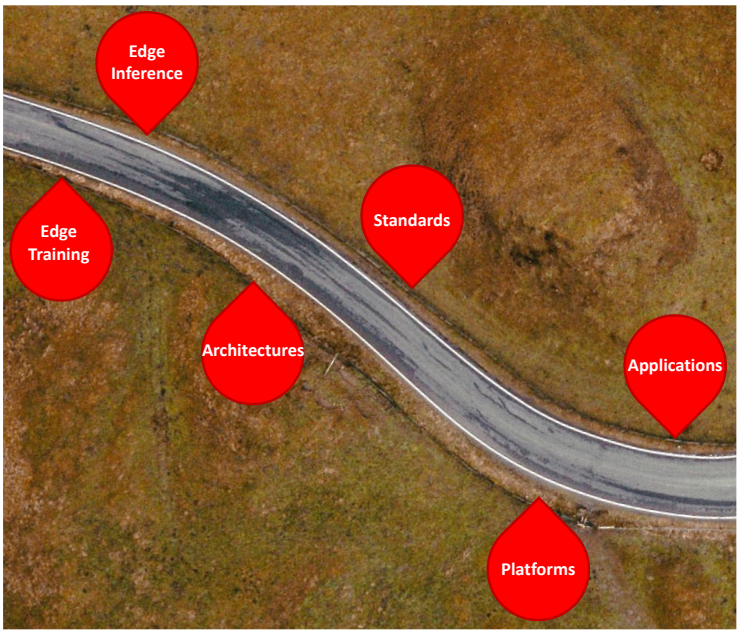


Figure 4.2: Roadmap to EdgeAI for 6G [27]

- AI on Edge, Data Availability: A proper incentive mechanism may be necessary for raw data provisioning from the mobile users. But raw data could be biased for different users [23].

### Impact

To build powerful and widely available AI systems it is clear that the centralized approach is a dead end. But especially for the realization of the 6G network the availability of AI capabilities is needed to achieve the proposed performance. EdgeAI will therefore provide a fundamental building block which enables high security, reliability, resiliency as well as yet unseen efficiency for the 6G network. Among other applications we expect this to have a huge impact on the progression of IIot, because it requires all those mentioned aspects.

The connected intelligence which emerges from EdgeAI is likely going to enhance the generalization abilities of AI. This will enable the deployment of large scale intelligent smart city services as shown by Xiao et. al. [21]. We think that applications which require the cooperation of many geographically distant heterogenous devices, to solve complex tasks like earthquake prediction, are going to benefit enormously by EdgeAI.

### 4.2.3 Trustworthy Artificial Intelligence

In the beginning of the 2010s, major advancements were achieved in the field of machine learning. This has caused several groups to become aware of the risks and challenges of AI. They quickly agreed that in the advancement of AI, the benefits of AI should be maximized, while its risks and dangers are to be minimized. Various guidelines regarding the use and development of AI were published, focusing on ethical aspects. The concept of ethical AI quickly gained traction which led to the term and research field of trustworthy AI [28]. Nowadays, due to the growing interest in and dependence on AI, Trustworthy Artificial Intelligence (TAI) has become an extensive research field with increasing relevance.

Trust is the foundation of societies, economies, and sustainable development. Therefore, we will only be able to realize the full potential of AI if trust can be established in it. For this matter, the EU has proposed an ethical guideline. TAI systems should follow four ethical principles: respect for human autonomy, prevention of harm, fairness and explicability [29]. These four principles are based on the human perception of trust and should be met when building AI to ensure its trustworthiness.

#### Facts

#### COMPAS

- COMPAS is a criminal risk assessment tool, which was developed in 1998. Since the year 2000, the recidivism risk scale has been in use. It predicts a defendants risk of committing a crime of felony, after being released [30].
- COMPAS has been used to assess over 1 million offenders, until ProPublica discovered a bias against african-american defendants within its recidivism component [30].
- Through analysing over 7000 individuals arrested in Broward County, Florida, ProPublica found out that that COMPAS overpredicting recidivism for black defendants, while underpredicting their white counterparts [30].
- Black defendants were incorrectly predicted to reoffend at a rate of 44.9%, while white defendants had a rate of 23.5%. Simultaneously, white defendants who did reoffend after release were falsely predicted to not recidivate at a rate of 47.7%, almost twice as high as their black counterparts (28.0%) [30].

#### Key Drivers

Researchers have proposed several approaches to define and quantify trustworthiness. Going through several papers, we decided to choose the most elaborate

definition out of them [31]. The article covers 8 key drivers, which are a requirement for trustworthy AI. The following paragraphs explain each key driver in detail according to the paper. Fulfilling these key drivers, the AI will meet the four ethical principles, proposed by the European Union (EU). In detail, figure 4.3 shows how the different key drivers are applied and directly linked to each principle.

Interestingly, generalization is a key driver (spoiler alert) and crucial, in order to successfully develop TAI. At the same time, when it comes to generalization, the AI system must be trustworthy. Therefore, these two concepts are deeply connected and mutually dependant on each other.

**Robustness** Robustness describes how well a system copes with erroneous inputs and execution errors. In realistic situations, the environment surrounding a system can be very stressful. Even then, the AI system should not falter in its performance. A lack of robustness could potentially harm and damage the system, decreasing its trustworthiness.

**Generalization** Generalization refers to the ability of TAI systems to extract information from a limited set of data, which they utilize to make accurate predictions on new, unseen data during training. Our introduction elaborates on this concept in detail.

**Explainability and Transparency** Explainability means being able to understand how an AI makes its decisions. Black box algorithms do not offer insight into their systems, which creates distrust. A transparent system allows humans to comprehend the inner process of the system and its risks as well as defects. By being transparent, an AI becomes trustworthy.

Transparency focuses on information disclosure of a system. In the AI industry, it is required to disclose the life cycle of an AI system by providing documentation. Information on its design purpose, data source, hardware and more should always be displayed and made available. This allows stakeholders to examine and verify the integrity of AI systems.

**Reproducibility** Research results should be reproducible. Being able to reproduce the results verifies the system and its reliability. Making one's code and data public for other experts to test out and verify increases the legitimacy of the system. Given reproducibility, the AI system as well as the whole AI industry become more trustworthy to the general public.

**Fairness** Bias in any part of the AI system can lead to detrimental, potentially discriminating results. Therefore, it is crucial for researchers to be aware of fairness in AI. They should detect and diminish biases to ensure fairness. Otherwise, it can greatly decrease trustworthiness in AI. There are three principles of fairness:

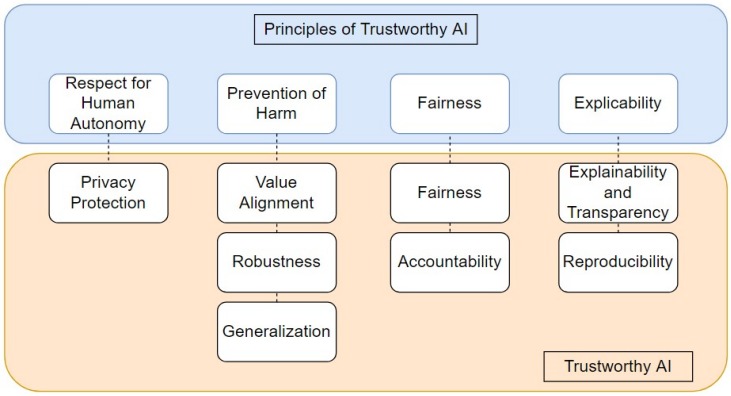


Figure 4.3: Principles of Trustworthy AI and Trustworthy AI

- **Independence** The system outcome is statistically independent of sensitive variables. The admission rate of female and male candidates is equal.
- **Separation** Independence principle stands depending on the underlying ground truth which correlates with a sensitive attribute. If the advertised position requires certain qualifications, the qualified men and women should have equal admission rates.
- **Sufficiency** Considers ground truth and requires the same ratio of qualified candidates among two groups. The chances of males and females being qualified enough given the admission decision should be equal.

**Privacy Protection** Privacy protection describes the ability to protect oneself against unauthorized use of data, which could leak personal information. People value privacy, even regarding it as a human right. Therefore, AI systems need to prioritize privacy protection in order to gain trust.

**Alignment** The purpose of AI systems should be to help us humans and improve our lives without violating our values. Abusing AI to achieve unethical and harmful goals destroys trust in the general AI industry. So, it is crucial to align the life cycle and development of AI with the values of humans to create TAI.

**Accountability** When it comes to regulating AI systems, the responsible persons must be held accountable. Since AI will have a growing impact on our lives, stakeholders of AI systems should be obligated to justify their decisions to align with human values. Furthermore, accountability also includes auditability, which means the ability to review and assess a system.

**Challenges**

Numerous challenges persist in attaining trustworthy AI:

- Every key driver needs to be quantified, in order to serve as a reliable and internationally accepted measures for TAI. Regarding 6g, an approach to define and measure trust has been made [32].
- Complex and powerful AI systems like deep neural networks usually come in black box models. Black box models are opaque to the outsider. Hence, the explainability of these systems is very low. This reduces the trustworthiness. The challenge lies in increasing explainablity in opaque AI systems while not compromising its usability [32].
- According to research, increasing robustness of an AI system can lead to a decrease in its generalization ability [31]. Since both key drivers are crucial to build TAI, this apparent trade-off needs to be solved in order to create trust.

**Impact**

Billions of data points need to be exchanged and processed every second in real time. While higher speed and larger capacity of the network for new internet applications are required, fairness of the packet transmission is an important goal. In consequence, the urge for perpetual development of 5G/6G technologies is increasing.

The scientific community is aware of these risks and intends to tackle them with the 6G network generation currently under development. To explicitly tackle the fairness concern a novel field was merged into a novel a discipline: The TAI for wireless networks. Implementing trustworthiness in the next generation communication system will solve the problem of low transparency in processing logics.

Our enlarged dependance on massive, autonomous data transmission prompts the need for common trust metrics. In fact, mission-critical tasks and general security will legitimately require translucent AI decision processes and quantifiable Quality-of-Trust (QoT) metrics for a range of users. Moreover, the data used when training the model used in data-queuing may enclose private or confidential information that influences data privacy in 6G communication. Therefore trustworthy algorithms are needed. Another important use of trustworthiness in 6G is the fair routing of packages.

## 4.3 Conclusion

To conclude, the future of Generalization evolves in three main fields. Firstly, a broader application scope and increased autonomy is in the making. Secondly, EdgeAI will reduce the entry barrier for such systems and allow them to operate closer to the user. The third and final dimension is fairness, which ensures

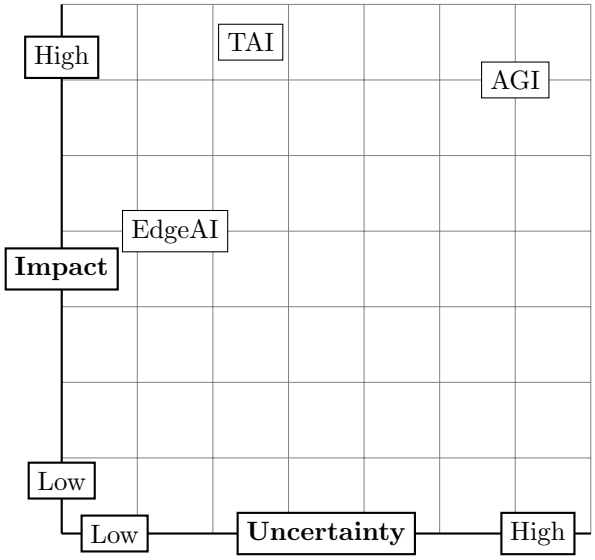


Figure 4.4: Trend matrix

equitable access to the beneficial results of increasingly capable AI systems in the daily life of communication technology users. This is emphasized by the trend matrix in Figure 5.5.

AGI is poised to pave the way for new, currently unimaginable applications. So far we neither know when these applications appear, nor what their impact to the daily life will be. Hence, we assume a very high impact of AGI but acknowledge the haziness of the current state of research.

With the ever increasing amount of data and traffic occuring at all network stages, the deployment of EdgeAI will be a necessity to not overwhelm network capacity. Even taking into account existing challenges like regulation, EdgeAI is waiting in the wings, alongside the rollout of 6G networks.

What is Love? Love is trust. TAI possesses the highest impact, as it directly affects how the world views and deals with intelligent technology. Building untrustworthy AI systems can have detrimental effects on political, economical and societal aspects. Since TAI is already an established field of research, we are certain that milestones and advancements will be achieved in the future. Nonetheless, some of the challenges are tough to solve and require international cooperation, which is not readily available. Therefore, a certain level of uncertainty persists.

# References


[1] A. M. Turing. "Computing Machinery and Intelligence". English. In: *Mind*. New Series 59.236 (1950), pp. 433–460. ISSN: 00264423. URL: http://www.jstor.org/stable/2251299.

[2] Syed Agha Hassnain Mohsan et al. "6G: Envisioning the Key Technologies, Applications and Challenges". In: *International Journal of Advanced Computer Science and Applications* 11.9 (2020). DOI: 10.14569/IJACSA.2020.0110903. URL: http://dx.doi.org/10.14569/IJACSA.2020.0110903.

[3] Haitham Hassan H. Mahmoud, Amira A. Amer, and Tawfik Ismail. "6G: A comprehensive survey on technologies, applications, challenges, and research problems". In: *Transactions on Emerging Telecommunications Technologies* 32.4 (2021), e4233. DOI: https://doi.org/10.1002/ett.4233. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/ett.4233. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4233.

[4] Stanislas Dehaene. *How we learn*. London, UK: Allen Lane, Jan. 2020.

[5] Judea Pearl and Dana Mackenzie. *The book of why*. Harlow, England: Penguin Books, May 2019.

[6] 2019. URL: https://wiki.opencog.org/w/Vision.

[7] Andre' Senna Ben Goertzel Alexey Potapov. *Toward a New Improved OpenCog – Preliminary Design Ideas*. 2020. URL: https://wiki.opencog.org/wikihome/images/7/77/OpenCog_Hyperon.pdf.

[8] SingularityNET. *White paper 2.0: SingularityNET - A Decentralized, Open Market and Network for AIs*. Tech. rep. SingularityNET, February, 2019. URL: https://public.singularitynet.io/whitepaper.pdf.

[9] Sara Sabour, Nicholas Frosst, and Geoffrey E Hinton. *Dynamic Routing Between Capsules*. 2017. arXiv: 1710.09829 [cs.CV].

[10] Prem Nair, Rohan Doshi, and Stefan Keselj. *Pushing the Limits of Capsule Networks*. 2021. arXiv: 2103.08074 [cs.CV].

[11] Andrea Banino, Jan Balaguer, and Charles Blundell. *PonderNet: Learning to Ponder*. 2021. arXiv: 2107.05407 [cs.LG].

[12] Alex Graves. *Adaptive Computation Time for Recurrent Neural Networks*. 2017. arXiv: 1603.08983 [cs.NE].

[13] Marcus Hutter. *Universal Artificial Intelligence: Sequential Decisions based on Algorithmic Probability*. Springer, 2005.

[14] Ben Goertzel. "Artificial General Intelligence: Concept, State of the Art, and Future Prospects". In: *Journal of Artificial General Intelligence* 5.1 (2014), pp. 1–46.

[15] Frank Schätzing. *Die Tyrannei des Schmetterlings*. Kiepenheuer & Witsch, 2018.

[16] Anne Carina Hashagen, Riccardo Manzotti, and Büchner-Verlag. *Ich denke, aber wer ist Ich? Ein Essay über den Sinn des Lebens*. 1st ed. Marburg an der Lahn, Germany: Büchner-Verlag, 2021.

[17] Yuval Noah Harari. *Homo Deus*. New York, USA: Harper, Feb. 2017.

[18] Erik Brynjolfsson and Andrew McAfee. *The Second Machine Age*. de. Kulmbach, Germany: Plassen Verlag, Oct. 2014.

[19] Max Tegmark. *Life 3.0*. London, UK: Allen Lane, Aug. 2017.

[20] Ella Peltonen et al. "6G white paper on edge intelligence". In: *arXiv preprint arXiv:2004.14850* (2020).

[21] Yong Xiao et al. "Toward Self-Learning Edge Intelligence in 6G". In: *IEEE Communications Magazine* 58.12 (2020), pp. 34–40. DOI: 10.1109/MCOM.001.2000388.

[22] Jinghe Wang et al. "Interplay Between RIS and AI in Wireless Communications: Fundamentals, Architectures, Applications, and Open Research Problems". In: *IEEE Journal on Selected Areas in Communications* 39.8 (Aug. 2021), pp. 2271–2288. ISSN: 1558-0008. DOI: 10.1109/jsac.2021.3087259. URL: http://dx.doi.org/10.1109/JSAC.2021.3087259.

[23] Shuiguang Deng et al. "Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence". In: *IEEE Internet of Things Journal* 7.8 (2020), pp. 7457–7469. DOI: 10.1109/JIOT.2020.2984887.

[24] Anastasia Yastrebova et al. "Airborne-terrestrial integrated architecture for self- driving vehicles realization". In: (Oct. 2019). DOI: 10.1109/ICUMT48472.2019.8970960.

[25] Jingao Xu et al. "Edge Assisted Mobile Semantic Visual SLAM". In: *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*. 2020, pp. 1828–1837. DOI: 10.1109/INFOCOM41043.2020.9155438.

[26] Ali J. Ben Ali, Zakieh Sadat Hashemifar, and Karthik Dantu. "Edge-SLAM: Edge-Assisted Visual Simultaneous Localization and Mapping". In: *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*. MobiSys '20. Toronto, Ontario, Canada: Association for Computing Machinery, 2020, pp. 325–337. ISBN: 9781450379540. DOI: 10.1145/3386901.3389033. URL: https://doi.org/10.1145/3386901.3389033.

[27] Khaled B. Letaief et al. "Edge Artificial Intelligence for 6G: Vision, Enabling Technologies, and Applications". In: *IEEE Journal on Selected Areas in Communications* 40.1 (2022), pp. 5–36. DOI: 10.1109/JSAC.2021.3126076.

[28] Scott Thiebes, Sebastian Lins, and Ali Sunyaev. "Trustworthy artificial intelligence". In: *Electronic Markets* 31.2 (June 2021), pp. 447–464. DOI: 10.1007/s12525-020-00441-. URL: https://ideas.repec.org/a/spr/elmark/v31y2021i2d10.1007_s12525-020-00441-4.html.

[29] Haochen Liu et al. *Trustworthy AI: A Computational Perspective*. 2021. arXiv: 2107.06641 [cs.AI].

[30] Julia Dressel and Hany Farid. "The accuracy, fairness, and limits of predicting recidivism". In: *Science Advances* 4.1 (2018), eaao5580. DOI: 10.1126/sciadv.aao5580. eprint: https://www.science.org/doi/pdf/10.1126/sciadv.aao5580. URL: https://www.science.org/doi/abs/10.1126/sciadv.aao5580.

[31] Bo Li et al. *Trustworthy AI: From Principles to Practices*. 2021. arXiv: 2110.01167 [cs.AI].

[32] Chen Li et al. "Trustworthy Deep Learning in 6G-Enabled Mass Autonomy: From Concept to Quality-of-Trust Key Performance Indicators". In: *IEEE Vehicular Technology Magazine* 15.4 (2020), pp. 112–121. DOI: 10.1109/MVT.2020.3017181.

# Chapter 5

# Applications for 6G

Putra, Stephen Lowis
Amami, Hazem
Chen, Wenwen
Chen, Zhen
Gan, Fengrui
Kong, Tianyuan
Nie, Yuliang

## Abstract

The motivation of approaching futuristic networks that combine an extreme high reliability with a significant connection density as well as an extreme high data rate or capacity has been pushing the research in the telecommunication field ever since it came to existence. This ever-awaited goal is getting closer to being in the realm of possibilities as 6th Generation wireless technology has been gaining momentum recently. As it seems, the aforementioned premise of the 6G technology is not only beneficial as a powerful structure for networking, but rather, and arguably more important, as infrastructure for more sophisticated applications that require an efficient network at their core. In this trend report, we present trends based on a review of state-of-art available documentation of the topic "Applications for 6G". Furthermore, we incorporate our own research and assessment to closely examine the facts, key drivers and challenges of each trend mentioned. Eventually, a conclusion is made to shed light on the comparison of these trends by analysing the uncertainty and impact of each.

## 5.1 Introduction

The growing interest for fast, reliable wireless networks with low latency have resulted in a huge research motivation to further introduce more designs to the innovations we already achieved in telecommunication. For the past decade, it

has been believed by many that 5th Generation wireless technology is somewhere near the peak of this research revolution. Nevertheless, this technology has created even more need for improvement as more and more sectors and applications are looking for an integration with reliable networks. At this point, it seems like more and more new use cases are demanding networking environment that are more sophisticated which makes the innovation of 6th Generation almost inevitable.

In essence 6G promises a massive upgrade to every aspect of its predecessors. The extreme high data rate/capacity is set to multiply 100 times for the next decade. [1] At the same time, extreme high reliability is growing with a target of up to 99% in order to ensure security, privacy and resilience. [1] Moreover, researchers project massive connected devices (10Million/$km^2$) combined with high sensing capabilities and high-precision positioning. [1] Another aspect that has been gaining momentum recently is the extreme coverage to engulf the whole globe (including sky and sea).

As one can clearly see, 6G is tackling a list of challenges that, if all solved, an upgrade, not only limited to our networks but rather to all aspects of our lives, is to be expected. This upgrade represents the core of this report as we are trying to define the emerging applications that are likely to take place short after the implementation of 6G.

## 5.2 Trends

In the following, we will focus on the potential future trends that 6G is likely to reshape and revolutionize. This varies from the evolution of Extended Reality and the improvement of Big Data, to the global adoption of Internet of Things and the introduction of Global Networks. Each trend will be accompanied with a rational discussion that explains the potential impact and application that might arise from the addition of the new technology. This includes corresponding facts, relevant key drivers as well as a highlight on the challenges that come along with it. Towards the end of the report, we assess and present the discussed trends in a "Trend Matrix" rated by their impact and uncertainty.

### 5.2.1 Extended Reality

Extended Reality (XR) is the family that includes Virtual Reality (VR), Augmented Reality (AR) and Mixed Reality (MR) either utilized individually or together (Figure 5.1). During the last 10 years, we have seen more and more new technologies involving XR. Starting from the popular game Pokemon Go, until some popular camera-based calculator or language translator. The trend of XR is predicted to continue growing in upcoming years, and accelerate with the presence of the 6G network. [2]

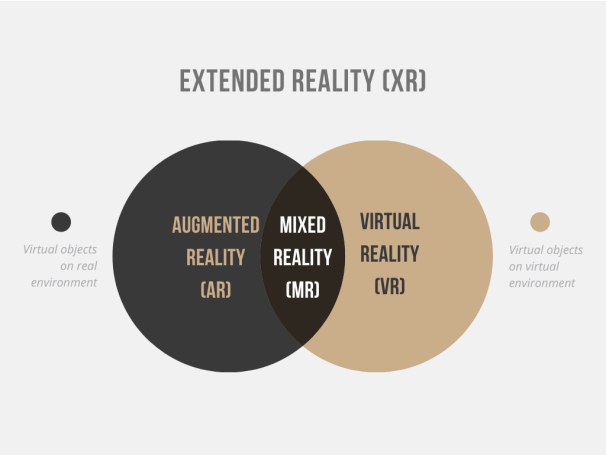


Figure 5.1: XR and its segmentation

**Facts**

- Expanding fields of applications. We can see more applications of XR in more fields of industries. Ranging from education, medical, industrial, entertainment, and still a lot more to come. This proves that XR will play a strategic role in the future world. [3]
- Companies entering the world of XR. In 2014, Oculus was dominating the VR market with its Oculus Rift and was chosen as the winner of the official Best of CES Award for 2014. This led to Facebook acquiring Oculus for $2 billion. Today, we have big companies entering the XR market. Major companies such as HTC, Amazon, Google, Apple, Microsoft, Sony, Samsung, and many others are currently developing XR headsets. [4]
- XR Market Demand is expanding. The accelerated trend of XR is closely related to its market demand. Rental of Google XR has seen an increased of 158%, and XR hardware inquiries have increased by 384% between the year 2016 to 2018. [4]

**Key Drivers**

- Improvement on Hardware. XR requires a high-quality display, various sensors, which then need higher computing power, while at the same time needing to stay within the power and thermal constraints of sleek XR glasses. During the last 10 years, research and developments conducted are able to overcome this challenge step by step, leading to the current state of the art of XR devices. [5]
- Increase in network speed. Roughly every 10 years we adopted a new generation of mobile networks. The boost in the network speed is signif-

icant. Each new generation offers on average 10x more speed compared to the previous generation. Therefore, more XR-based innovations can be enabled. [5]

- Image Processing Techniques. During the last 10 years, we have seen many advancements in image processing techniques. Thanks to the hype of artificial intelligence, more algorithms are being researched so that image processing becomes more advanced and efficient than before. [6]

**Challenges**

- Technological Challenges. Not only hardware computing power which needs to keep up with bigger processing power demands, massive adoption of XR technology also demands an ultra high-speed network. As a reference, in order to be able to do a realistic 3D holographic teleconference, a raw hologram, without any compression, with colors, full parallax, and 30 fps, would require 4.32 Tb/s and latency at sub-millisecond. [7] Within this perspective, the assumption of 5G millimeter-wave (mmWave) is not an option, and therefore research on 6G XR has shifted to the High-rate and High-reliability low latency communications (HRLLC) over the Terahertz frequency. [8] [9] [10]

- Privacy and Security. Like any other technology, the protection of users' sensitive data is also a challenge. Threats are visible in several aspects such as data collection and illegal usage of it. [11]

- Social and Economy. XR massive implementation also needs to take care of ethical problems, so that applications are right on target and beneficial. In addition, the benefits that can be offered should also be taken into consideration, whether or not it is worth the investment. [12]

**Impact**

- In Field of Communication. The successful implementation of 6G will enable holographic telepresence. If you ever watched a movie where the characters have a meeting with 3D holograms of people, it is a teleconference. With this, long-distance communication will be more realistic, as we can see much more details in 3D. [13] [14]

- In Field of Education. XR will enable various new learning methods. Learning processes will be safer and more interactive than before. In school, students can learn about things without having to explore the real world, for example, learning about the river environment which is quite dangerous. In University, students, especially engineers and designers, will be helped when modeling a new product. Also, practical training involving heavy machines, which is relatively dangerous, can be substituted with an XR-based simulator. This way, learning will be more risk-free,

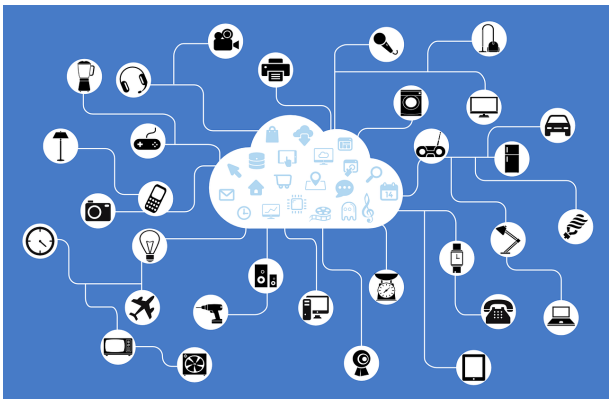

Figure 5.2: Large number of devices and various data type

and learners can even try to explore anything they want to try with the machines/environment. [15]

- In Field of Industry. The use of XR such as Digital Twin will enable workers to prototype and simulate systems easier and more interactively. In addition, this will also allow collaborative 3D prototyping or simulation with other people remotely around the world. [16]

- In Field of Healthcare. XR can be used for 3D visualization. This helps the medical team to understand the patient's condition better and therefore can plan a better strategy. This also enables touch-free interfaces that can be used in sterile environments. [17]

### 5.2.2 Big Data

5G technology is already successfully used in many applications. But communication networks are expanding and new communication technologies are emerging, that lead to clogs in communication networks. [18] Throughout the potential applications, huge amounts of data will become a trend. In smart factories and smart cities, many devices that in conventional situations do not receive information, will be deployed into the communication network. In smart healthcare, big data makes everyone's data be part of the communication network. The development of hardwares and sensory technology makes advanced communication methods possible. Communication networks will deal with massive data with the emergence of these applications. 5G technology will eventually become very limited. [19] Applications will rely on 6G communications, because the requirements for communication accuracy in various applications are getting higher and higher. 6G will provide much higher density of connections, much higher frequency bandwidth, much higher mobility and extremely large network scale. [18]

### Facts

Massive data is mainly generated by the following reasons.

- More communication devices. The communication network enables individual devices to interact with each other. The number of devices in the network continues to grow. This number exceed 50 billion in 2020. [20] In the further this number will get bigger. More devices inevitably lead to more data.

- Non-Traditional data type. The development of hardware devices enables the transmission of data types that are not limited to text and images and sounds. It is possible to transmit new data types such as holograms and tactile information to restore realistic scenes. [21] They have a much higher information volume than traditional data types. Accordingly, the amount of data will be larger.

- Smart to intelligent devices. The smart devices will be replaced by intelligent devices. [21] The intelligent devices will be able to make predictions and decisions by interacting with the environment. Devices are able to determine target motions by themselves. These decision-making processes inevitably require a large data base.

### Key drivers

- Edge computing. A very efficient way of processing data nowadays is cloud-based computing. All data is transmitted to a cloud center, computed and stored in the cloud. But as the volume of data increases and the number of data types continues to grow, the transmission will occupy too much channel bandwidth. This can cause communication delays and even loss of information. [22] Besides, the cloud computing power is not enough to deal with so much data.

  Equipments generate large amounts of data, much of which is unstructured and needs to be run through a robust analytical program. An edge computing framework will help prioritize which data needs to be kept on the edge and processed by the on-board computing power, and which data should be forwarded back to the data center for analysis, acting as a relay station and providing additional computing power for mission-critical analysis. [23]

  Traffic flow prediction timely and accurate access to traffic flow information is an essential part of making high precision maps that help facility sense the complex information in advance. Edge intelligence can combine AI with advanced edge computing technology. Computational resources can be scaled to edge servers to enable state-of-the-art performance for learning hierarchical features from high-dimensional datasets and meeting real-time requirements for time-consuming tasks. [23]

- Deep learning algorithms. Deep learning algorithms coupled with advanced computing hardware, play a critical role in big data processing. [24] Deep learning networks learn from empirical data to discover its intricate structures. By building computational models that include multiple processing layers, deep learning networks can create multiple levels of abstraction to represent data. Therefore, the trained model will have more samplings and be more effective if the amount of data is large . With efficient deep learning algorithms, useful data as well as the framework of the data can be extracted from large amounts of data. This avoids the transfers of large amounts of data and instead only transfer the framework of data and corresponding model parameters. Deep learning for massive data has been successful in speech recognition, collaborative filtering and computer vision.

**Challenges**

- The scale of big data. The scale of big data is the first thing that comes to mind for most people. Managing large and rapidly growing amounts of data has always been a difficult task. Data volumes are growing faster than computing resources, and CPU speeds are static. Future power constraints may make it impossible to use all of a system's hardwares at the same time, and data processing systems may have to actively manage processor power consumption. These unprecedented changes necessitate a complete rethinking of how data processing components are designed, built, and operated. [25]

- Data security and privacy. Data security and privacy concerns are critical in many application areas of big data, because the mobile device data to be processed and inferred may contain much privacy-sensitive information that is not desired to be captured. If the data is sent directly to the edge server for processing, the privacy of the users may be jeopardized. This issue can arise in model training and inference in general. To address this issue, it appears that performing simple processing on the device first, and then uploading intermediate functions to the edge server, is a viable solution. [23]

**Impact**

Big data technology can not only improve the efficiency of the use of data, but also realize the reuse of data, thus greatly reducing transaction costs and enhancing the space for people to develop their own potential. People can carry out holographic vertical historical comparison and horizontal reality comparison of things. Big data technology can not only be rapidly derived into a new information industry, but also can be linked with cloud computing, Internet of Things, and intelligent engineering technology to support a new era of information technology.
First: the production scene. The impact of big data on the production scene

will be clearly reflected in the industrial Internet era, specifically in three areas, one is the data of production materials; the second is the data of operation management; the third is the data of personnel management. The application of big data in the production scene requires a large ecosystem, and this ecosystem cannot be separated from the support of cloud computing and the Internet of Things, and artificial intelligence will also become an important export of big data applications in the future. Second: the consumer scene. The application of big data in the consumer scene has accumulated some application experience in the Internet field, and is covering from online to offline. The coverage of the consumption scene is very large, so the application boundary of big data itself is also very large, which is an important reason why big data has received wide attention. From the big level, big data itself can open up more space for innovation in the field of consumption, and "data consumption" will also become a new consumption trend. Third: learning scenario. With the rapid development of online education, big data will improve the learning experience of online education to a certain extent.

### 5.2.3 Internet of Things

The Internet of Things (IoT) describes the network of physical objects "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. The IoT has been implemented in many application fields, such as smart home, smart city, smart medical care, autonomous driving, smart industrial control, and so on, which is shown in Figure 5.3.
Under the dilemma of the pandemic, IoT paves the way for telemedicine, COVID-19 symptom monitoring, and even disinfection. [26] We expect to see more healthcare organizations continue to innovate systems and processes in the coming years. Some cities are now using the Internet of Things to connect utilities, parking meters, and traffic lights. More and more governments are investing in smart city technology and it is able to improve financial, social, and environmental aspects of urban life. Thus it is envisaged that more and more Research and Development (R&D) capital and professionals will pour into the field and prosper the applications of IoT.

**Facts**

- With the development of IoT technology, many IoT applications such as smart cities, smart factories, and autonomous driving, which are massive in number, data-intensive, computation-intensive, and delay-sensitive, are continuously booming. It is estimated that 50 billion devices in the field of IoT have emerged by the end of 2020, reflecting the large marketing demands and commercial value of this area. [27]
- The main goal of 5G is to meet the needs of communication with lower delay and higher reliability. However, for 2030 and further, the upper limit

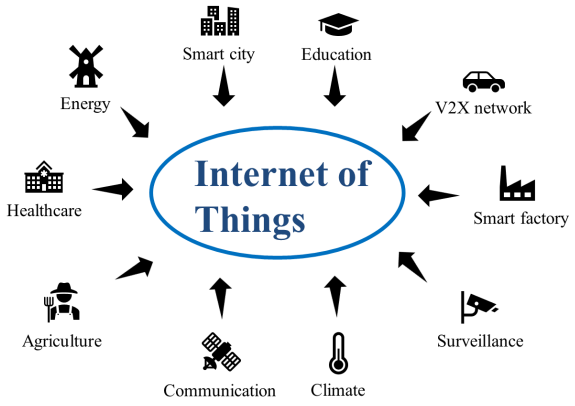


Figure 5.3: Applications of IoT

of 5G technology still cannot meet the needs of IoT coverage and application. [28] In contrast, 6G wireless communication networks are expected to provide global coverage, improved spectral/energy/cost efficiency, higher intelligence level and security, etc. To meet more requirements of IoT applications, 6G networks should rely on new technologies, i.e., air interface and transmission technologies and novel network architecture, such as waveform design, multiple access, channel coding schemes, multi-antenna technologies, network slicing, cell-free architecture, and cloud/fog/edge computing. [29]

- As more and more sensing devices are used in industry, 6G will provide full automation with its ultra-large-scale connectivity and super reliability. Intelligent production is achieved by transferring data to the cloud or edge cloud and analyzing the data to make intelligent decisions. In this process, 6G guarantees error-free data transmission. 6G also enables remote maintenance. In this process, remote experts and field staff can cooperate to solve problems in a timely manner, thus increasing efficiency and reducing costs. Another service refers to remote control, which enables the remote control of machines to ensure worker safety and reduce costs. This requires strictly low-latency, wideband and reliable 6G transmission. [30]

### Key Drivers

- Communication technology. Compared with 5G, 6G is able to achieve IoT in a much more advanced way. Firstly, it enables widespread internet connections. 6G will make full use of the low, medium, and high full spectrum resources to drive seamless global coverage of the integration of

sky and earth. [31] Secondly, the network performance is evolving. IoT requires a 6G data rate to reach terabit magnitude. In surveying and mapping, precision agriculture, Internet of vehicles, deformation monitoring, and other scenarios, Communication technology that can support ultra-high precision positioning of less than $1m$ or even sub-meter is required. It is often required that the communication technology has such technical characteristics as ultra-low delay, swarm intelligence perception, super-large antenna array, and good integration with satellite communication and other communication systems. [32] Thirdly, 6G has Pronounced technological convergence. The highly autonomous and intelligent super flexible network is one of the most obvious features of 6G. 6G intelligence will be implemented in every link of the network from end to end. Artificial intelligence, blockchain, big data, and other technologies will be integrated into the network architecture to realize the autonomy of the network. [33]

- Data Value. Due to the explosion of intelligent devices in recent years, a large number of data is generated every day. It is meaningful to utilize these data and produce more application opportunities and improve the quality of service in IoT. The data sources are becoming more diversified and the scale of data connectivity is greatly increased, pushing industries, cities, and society towards the target of digital twins. At the same time, the introduction of AI, blockchain, and other technologies has changed the way data is collected, prioritized, and shared, further optimizing the value of data for different objects. At the same time, AI, blockchain, and other technologies provide intelligent privacy security guarantee mechanisms. [34]

- Artificial Intelligence. Artificial intelligence is expert in realizing high-level intelligent applications of information technology, such as data mining, semantic understanding, intelligent reasoning, and intelligent decision making. Therefore, AI has become an effective tool to solve the bottleneck of IoT technology, the Internet of Things is responsible for collecting information (through sensors that connect countless devices and carriers, including home appliances) and the dynamic information collected is uploaded to the cloud. The information is then analyzed and processed by AI systems to generate the practical technology needed by humans. In addition, AI helps humans to reach deeper long-term goals by learning from the data itself. [35]

**Challenges**

- Outlier detection in sensor data. Sensors, the foundation of the IoT, are critical to decision making, so it is important to ensure the reliability and accuracy of sensed data. As IoT sensors are vulnerable to malicious attacks, it is critical to detect outliers to ensure data quality. Machine learning has proven to be an effective tool for detecting outliers in sensor

data, but how to efficiently use machine learning for outlier detection in sensor data is still being explored. [36]

- Incomplete Data Set. Almost all machine learning methods require data for training and testing, such as supervised learning, unsupervised learning, reinforcement learning, etc. The data can be obtained or collected in many ways. Furthermore, the larger the data sample, the more accurate the machine learning algorithm will be. However, it is not easy to obtain the large number of perfect data samples required. Firstly, unpredictable link delays and radio interference can lead to slow responses or missing. Secondly, there are privacy issues involved, with some private data often held by different companies, making it difficult to aggregate the data. [33]

- Security and privacy protection. IoT applications require the analysis and mining or integration of collected data, which requires the integration of data from distributed and autonomous IoT devices. Cloud-edge hybrid processing, either locally or with edge servers, may also violate the privacy of the data owner and risk data theft, misuse, and abuse. [37]

- Computing power. The computing ability and resources of terminal devices in IoT systems are limited, and AI algorithms, especially data mining and deep learning algorithms, usually require strong computing power. Therefore, it is difficult to deploy The AI model, and the delay problem of AI-based data mining and intelligent decision making leads to poor application effect in real-time interaction scenarios. [38]

**Impact**

- Smart city. Enhanced maps, autonomous vehicles, mobile ticketing, and passenger counting in transport or logistics have been successfully achieved [39]. Continuous improvement of these technologies is also currently in practice. Similarly, telemedicine in the areas of remote patient monitoring, smart biosensors, smart ambulances, wearable devices, and IoT healthcare benefits society. Not only has the country's infrastructure been enhanced, but citizens also benefit from the concept of smart homes and smart cities, which are cost-effective and convenient. Smart healthcare effectively manages consumer health. The smart gym enables users to monitor their exercise schedules on a regular basis. The automatic update of social activities on social media is also required for humans today.

- Scenario application. The future application value of 6G is mainly reflected in the extensive and large-scale data collection, real-time interaction, and convenience of acquisition, so as to obtain a more accurate digital model, which enables many applications of IoT. The essence of the twin factory, twin medical treatment, twin city, and so on is based on simulation technology, comprehensive application of AI, and other technologies, which is the realization of the physical system to information space digital model mapping, monitoring, analysis, optimization, management. [31]

### 5.2.4 The Global Network and Autonomous Driving

The airborne-integrated communications (combination of terrestrial and non-terrestrial networks) have drawn the attention of both academia and industry. Many organizations recognize non-terrestrial networks (NTNs) as a key component to provide cost-effective and high-capacity connectivity in the future. As defined by the 3rd Generation Partnership Project (3GPP), an NTN (shown in figure 4) is a network where spaceborne or airborne vehicles(Satellites or HAPs) act either as a relay node or as a base station.[40]
Autonomous driving is a knowledge-intensive field. In this sub-section, we base our discussion on the aspect of networking, which refers to airborne-integrated communications. Autonomous driving places very stringent requirements on the network, such as low latency, high throughput, and wide range of network connectivity.[41] Existing networks, including the recently emerged 5G networks, do not fully meet these conditions. The need for ubiquitous connectivity is the main problem. Because the deployment of base stations (BS) in the remote area is challenging. The integration of non-terrestrial and existing networks will also bring additional benefits such as throughput improvement and latency reduction.[42] A growing number of companies, such as Starlink, OneWeb, have joined the competition of NTN and autonomous driving and their combination have great potential.

**Facts**

- Non-terrestrial networks are attracting the attention of academia and industry today[43] and have great potential to meet the requirements of autonomous driving[41]. There are a lot of companies that are deploying non-terrestrial networks, such as Starlink, One Web.

- More than one million subscribers have already subscribed to the Starlink service.[44]

- Autonomous driving has been receiving a lot of attention in recent years, and its concrete implementation has yet to be studied. During the last few years, there are more and more self-driving enabled cars entering the market. I.e. Tesla, Nio.[41]

**Key Drivers**

- Nano-satellites. Traditional satellites weigh about 120 kg, and we can send 60 satellites in one launch. But with the nano-satellite, which weighs only 8 kg. We can deploy 10 times more satellites compared to the traditional method which enhances the flexibility.[45]

- Advanced waveforms and modulation schemes. Non-terrestrial devices have typically been operated in frequency bands below 6 GHz which may not satisfy the data rate requirements of future services. Solutions are

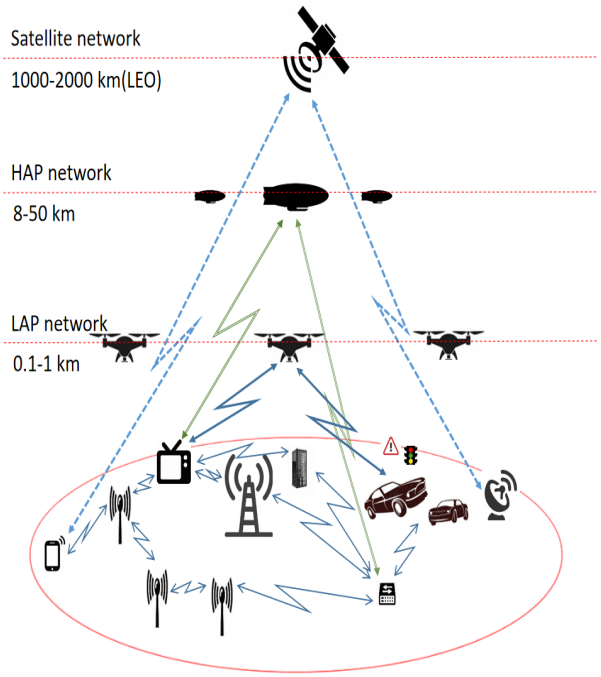


Figure 5.4: General airborne communication architecture to support terrestrial networks.[41]

being proposed toward the development of new waveforms and modulation schemes, i,e, impulse-based ultra-wideband (UWB) modulation.[43]

- Achievability of worldwide coverage. It is more realistic to achieve broader network with non-terrestrial networks coverage than terrestrial networks. This enables to remote control a car in remote areas which can reduce the cost of transportation.[41]

**Challenges**

- Positioning and sensing. The positioning and sensing are very important for Connected and autonomous vehicles (CAV). Traditional Global Positioning System (GPS) satellite positioning methods have low positioning accuracy and not very high performance. Using 6G networks with terahertz in CAVs can reduce cost, improve accuracy, and thus reliability. However, a major challenge is how to design terahertz antennas, increase communication range and handle high CAV mobility. [46]

- Integration between exiting network and non-terrestrial network. Relying on NTN networks alone to support autonomous driving is unwise in terms

of economics and efficiency, so it makes sense to work in conjunction with existing networks.[41]

- Low latency promise. This requirement is obvious to autonomous driving, but how to reach this goal with NTNs is still on discussing.[42] One of the possible solution is the usage of Multi-access Edge Computing (MEC) technology which provides localized computing and storage resources for non-real time and real time services, depending on network conditions. This mechanism provides great possibilities for delay-critical services by performing service-related processing tasks on the cellular customer side, reducing network congestion and latency[41]

- High data throughput requirement. The real-time transmission of high-definition video or uncompressed images from LiDAR sensors for high definition map construction is very bandwidth-consuming. So it is quite essential that the used network can achieve a very high data throughput to support the transmission missions. According to the plan, NTNs can meet this requirement [41]

- Seamless and ubiquitous connectivity. For delay-critical applications, especially remotely controlled, it is important to provide seamless and ubiquitous connectivity. For example, a self-driving truck delivering goods to a remote area cannot be shortly disconnected by driving through the edge of a city and it also should be always connected even in remote area.[42][41]

- The implementation of non-terrestrial networks requires a large number of satellites, which affects the research of other disciplines, such as astronomical observations through the usage of broadband frequency.[42]

**Impact**

Non-terrestrial networks have a very large potential as network infrastructure. Its many features, such as a wide range of network services, high throughput, and low latency can provide Internet access in rural and remote areas, make XR services available in those areas, and even make remote surgery possible.[43][42] For autonomous driving, a stable and good network is an integral part. By using non-terrestrial networks we can make up for the shortcomings of today's networks, extending the range of autonomous driving and contributing to its early realization.[41]
NTNs also make two technologies of autonomous driving possible. First is Vehicle-to-everything (V2X). V2X includes vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle-to-network (V2N), vehicle to the pedestrian. In self-driving mode, it can automatically select the best route for road conditions by analyzing real-time traffic information, thus greatly reducing traffic congestion and accidents. By using NTNs we can keep the constant connection of the vehicle to the network. So that we can do continuous monitoring and accident report. The other is Connected and autonomous vehicles (CAV). CAV combines

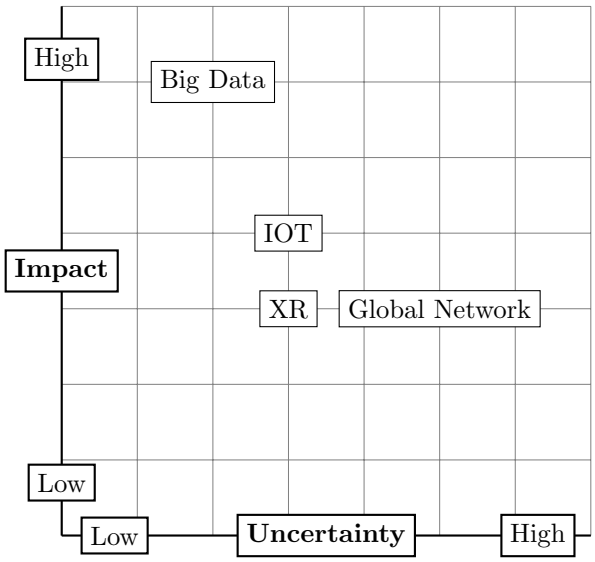


Figure 5.5: Driver matrix

connectivity and automated technologies to assist or replace humans in the task of driving. This can be through a combination of advanced sensor technology, onboard and remote processing capabilities, GPS, and telecommunications systems.[46]

## 5.3 Conclusion

After assessing each trend, we conclude that big data would be the most affecting trends in the future, as we agree that more and more data will be generated and data will be the key ingredients to many other applications and innovations. IoT will also bring significant impacts in the future, as we can already see current implementations and developments on this field, however, how the trends will develop and whether it will be massively adopted is still uncertain, especially when we are talking about the global IoT, where every devices in the world is connected.
XR and The Global Network would also bring a big impact, but would not be as significant as compared to the other two. However, there is a higher uncertainty regarding the future development of the global network compared to the XR, because we can already see that more companies have jumped into the XR field, while only a few has started its way on the global network. The main reason for this is probably due to the development cost, where the research and development for the global network is way more costly than on XR. In addition, the market of XR is proven to be more rapidly expanding compared to the other one. These four trends discussed are able to be described in the following driver

matrix.

# References


[1] INC. NTT DOCOMO. "White Paper 5G Evolution and 6G". In: (Feb. 2021).

[2] Perkins Coie. *2020 AR and VR Survey: Industry Insights Into the Future of Immersive Technology*. Tech. rep. Perkins Coie, 2020.

[3] "Toward 6G Networks: Use Cases and Technologies". English (US). In: *IEEE Communications Society Magazine* 58.3 (Mar. 2020), pp. 55–61. ISSN: 0163-6804. DOI: 10.1109/MCOM.001.1900411.

[4] Perkins Coie. *2018 AR and VR Survey: Industry Insights Into the Future of Immersive Technology*. Tech. rep. Perkins Coie, 2018.

[5] *Extended reality XR: Immersive VR*. Aug. 2021. URL: https://www.qualcomm.com/research/extended-reality.

[6] Ning-Ning Zhou and Yu-Long Deng. "Virtual reality: A state-of-the-art survey". In: *International Journal of Automation and Computing* 6.4 (Nov. 2009), pp. 319–325. ISSN: 1751-8520. DOI: 10.1007/s11633-009-0319-9. URL: https://doi.org/10.1007/s11633-009-0319-9.

[7] Xuewu xu et al. "3D holographic display and its data transmission requirement". In: (Oct. 2011). DOI: 10.1109/IPOC.2011.6122872.

[8] Christina Chaccour et al. *Can Terahertz Provide High-Rate Reliable Low Latency Communications for Wireless VR?* 2021. arXiv: 2005.00536 [cs.IT].

[9] Romano Fantacci and Bendetta Picano. "Edge-Based Virtual Reality over 6G Terahertz Channels". In: *IEEE Network* 35.5 (2021), pp. 28–33. DOI: 10.1109/MNET.101.2100023.

[10] Christina Chaccour et al. "Risk-Based Optimization of Virtual Reality over Terahertz Reconfigurable Intelligent Surfaces". In: *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. 2020, pp. 1–6. DOI: 10.1109/ICC40277.2020.9149411.

[11] Jaybie A. de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. "Security and Privacy Approaches in Mixed Reality: A Literature Survey". In: *CoRR* abs/1802.05797 (2018). arXiv: 1802.05797. URL: http://arxiv.org/abs/1802.05797.

[12] Stephanie Hui-Wen Chuah. "Why and Who Will Adopt Extended Reality Technology? Literature Review, Synthesis, and Future Research Agenda". In: (Dec. 2018).

[13] P.-A. Blanche et al. "Holographic three-dimensional telepresence using large-area photorefractive polymer". In: *Nature* 468.7320 (Nov. 2010), pp. 80–83. DOI: 10.1038/nature09521. URL: https://doi.org/10.1038/nature09521.

[14] Ermal Dreshaj. "Holosuite : an exploration into interactive holographic telepresence". PhD thesis. Jan. 2015.

[15] Sanika Doolani et al. "A Review of Extended Reality (XR) Technologies for Manufacturing Training". In: *Technologies* 8.4 (2020). ISSN: 2227-7080. URL: https://www.mdpi.com/2227-7080/8/4/77.

[16] Jakub Matišák, Matej Rábek, and Katarına Žáková. "Use of Holographic Technology in Online Experimentation". In: *2019 Federated Conference on Computer Science and Information Systems (FedCSIS)*. 2019, pp. 921–924. DOI: 10.15439/2019F179.

[17] Christopher Andrews et al. "Extended reality in medical practice". In: *Current Treatment Options in Cardiovascular Medicine* 21.4 (2019). DOI: 10.1007/s11936-019-0722-7.

[18] Fengxiao Tang et al. "Survey on Machine Learning for Intelligent End-to-End Communication Toward 6G: From Network Access, Routing to Traffic Control and Streaming Adaption". In: *IEEE Communications Surveys Tutorials* 23.3 (2021), pp. 1578–1598. DOI: 10.1109/COMST.2021.3073009.

[19] Ying Loong Lee et al. "6G Massive Radio Access Networks: Key Applications, Requirements and Challenges". In: *IEEE Open Journal of Vehicular Technology* 2 (2021), pp. 54–66. DOI: 10.1109/OJVT.2020.3044569.

[20] Keyan Cao et al. "An Overview on Edge Computing Research". In: *IEEE Access* 8 (2020), pp. 85714–85728. DOI: 10.1109/ACCESS.2020.2991734.

[21] Sabuzima Nayak and Ripon Patgiri. "6G Communication Technology: A Vision on Intelligent Healthcare". In: (Apr. 2020).

[22] Jianli Pan and James McElhannon. "Future Edge Cloud and Edge Computing for Internet of Things Applications". In: *IEEE Internet of Things Journal* PP (Oct. 2017), pp. 1–1. DOI: 10.1109/JIOT.2017.2767608.

[23] Bo Yang et al. "Edge Intelligence for Autonomous Driving in 6G Wireless System: Design Challenges and Solutions". In: *IEEE Wireless Communications* 28.2 (2021), pp. 40–47.

[24] Xue-Wen Chen and Xiaotong Lin. "Big Data Deep Learning: Challenges and Perspectives". In: *IEEE Access* 2 (2014), pp. 514–525. DOI: 10.1109/ACCESS.2014.2325029.

[25] Divyakant Agrawal et al. "Challenges and opportunities with Big Data 2011-1". In: (2011).

[26] Zaheer Allam and David S Jones. "On the coronavirus (COVID-19) outbreak and the smart city network: universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management". In: *Healthcare*. Vol. 8. 1. Multidisciplinary digital publishing institute. 2020, p. 46.

[27] Walid Saad, Mehdi Bennis, and Mingzhe Chen. "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems". In: *IEEE network* 34.3 (2019), pp. 134–142.

[28] Zhengquan Zhang et al. "6G wireless networks: Vision, requirements, architecture, and key technologies". In: *IEEE Vehicular Technology Magazine* 14.3 (2019), pp. 28–41.

[29] Xiaohu You et al. "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts". In: *Science China Information Sciences* 64.1 (2021), pp. 1–74.

[30] Cheng-Xiang Wang et al. "6G wireless channel measurements and models: Trends and challenges". In: *IEEE Vehicular Technology Magazine* 15.4 (2020), pp. 22–32.

[31] Walid Saad, Mehdi Bennis, and Mingzhe Chen. "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems". In: *IEEE Network* 34.3 (2020), pp. 134–142. DOI: 10.1109/MNET.001.1900287.

[32] Yunchou Xing and Theodore S Rappaport. "Propagation measurement system and approach at 140 GHz-moving to 6G and above 100 GHz". In: *2018 IEEE global communications Conference (GLOBECOM)*. IEEE. 2018, pp. 1–6.

[33] Mingzhe Chen et al. "Artificial neural networks-based machine learning for wireless networks: A tutorial". In: *IEEE Communications Surveys & Tutorials* 21.4 (2019), pp. 3039–3071.

[34] Yuji Roh, Geon Heo, and Steven Euijong Whang. "A survey on data collection for machine learning: a big data-ai integration perspective". In: *IEEE Transactions on Knowledge and Data Engineering* 33.4 (2019), pp. 1328–1347.

[35] Murat Kuzlu, Corinne Fair, and Ozgur Guler. "Role of artificial intelligence in the Internet of Things (IoT) cybersecurity". In: *Discover Internet of things* 1.1 (2021), pp. 1–14.

[36] Jihong Park et al. "Wireless network intelligence at the edge". In: *Proceedings of the IEEE* 107.11 (2019), pp. 2204–2239.

[37] Xinghua Li et al. "Smart Applications in Edge Computing: Overview on Authentication and Data Security". In: *IEEE Internet of Things Journal* 8.6 (2021), pp. 4063–4080. DOI: 10.1109/JIOT.2020.3019297.

[38] Ali Hassan Sodhro et al. "Toward 6G Architecture for Energy-Efficient Communication in IoT-Enabled Smart Automation Systems". In: *IEEE Internet of Things Journal* 8.7 (2021), pp. 5141–5148. DOI: 10.1109/JIOT.2020.3024715.

[39] Kinza Shafique et al. "Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios". In: *IEEE Access* 8 (2020), pp. 23022–23040. DOI: 10.1109/ACCESS.2020.2970118.

[40] Federica Rinaldi et al. "Non-Terrestrial Networks in 5G & Beyond: A Survey". In: *IEEE Access* 8 (2020), pp. 165178–165200. DOI: 10.1109/ACCESS.2020.3022981.

[41] Anastasia Yastrebova et al. "Airborne-terrestrial integrated architecture for self- driving vehicles realization". In: (Oct. 2019). DOI: 10.1109/ICUMT48472.2019.8970960.

[42] Sastri Kota and Giovanni Giambene. "6G Integrated Non-Terrestrial Networks: Emerging Technologies and Challenges". In: (2021), pp. 1–6.

[43] Marco Giordani and Michele Zorzi. "Non-Terrestrial Networks in the 6G Era: Challenges and Opportunities". In: *IEEE Network* 35.2 (2021), pp. 244–251. DOI: 10.1109/MNET.011.2000493.

[44] *Starlink Homepage. https://www.starlink.com/, 2022.* URL: http://www.starlink.com/.

[45] Vicente Almonacid and Laurent Franck. "Extending the coverage of the internet of things with low-cost nanosatellite networks". In: *Acta Astronautica* 138 (May 2017). DOI: 10.1016/j.actaastro.2017.05.030.

[46] Jianhua He, Kun Yang, and Hsiao-Hwa Chen. "6G cellular networks and connected autonomous vehicles". In: *IEEE Network* (2020).