***Study Paper***

***On***

# Artificial Intelligence (AI) and Big Data for Telecom

***FN Division, TEC***
***K.L. Bhawan, Janpath, New Delhi-01***

***March 2019***

# Table of Contents

# Abstract

Artificial Intelligence (AI) is the ability of machines and systems to acquire and apply knowledge and carry out intelligent behavior. AI with learning abilities is a revolutionary technology, which the communication industry is exploring, with the aim of introducing it into communication networks to provide new services/ applications and to improve network efficiency and user experience. The telecom industry has been a fertile field of application for AI. The development opportunities created by AI technologies will certainly benefit the entire industry as well as users.

The paper discusses various aspects of AI, its progress and its application to the telecom sector including possible use cases. Explains briefly role of AI in Network monitoring, security and reliability. Also examines the work at ITU on AI such as Focus Group on Machine Learning 5G etc. Finally, identifies possible challenges in AI implementation and need of following certain ethics/ ethical values in doing so.

# 1. Introduction

Artificial Intelligence (AI) is the ability of machines and systems to acquire and apply knowledge and carry out intelligent behavior. AI can be viewed as a set of associated technologies and techniques that can be used to complement traditional approaches, human intelligence and analytics and/or other techniques. In recent years, with the development and enrichment of technologies such as cloud computing, big data and deep learning, the industrialization of artificial intelligence is being developed accordingly. With new developments and worldwide excitement, AI has attracted more and more attention for introducing it into a number of areas.

Communications sector with a variety of consumer demands on individualization requirements, multimedia services and precision management, its network security has become more and more important. With AI's advantages in learning, understanding, reasoning and cooperating and with the invent of software-defined networks (SDN) and network functions virtualization (NFV), technologies of deep packet inspection and service aware networks, the intellectualization of communication networks and services has become possible. Furthermore, operators/industry have a keen interest in AI, which may decrease capital expenditure (CAPEX), and operating expense (OPEX).

# 2. Trends in Communication Networks and Services:

Artificial Intelligence with learning abilities is a revolutionary technology, which the communication industry is exploring, with the aim of introducing it into communication networks to provide new services, to improve network efficiency and user experience. Communication is a sector with heavy ICT use, dealing with a variety of consumer demands on individualization requirements, multimedia services and precision management. Current major trends in communication networks and services are described below: -

## 2.1 Characterized requirements:

With the increasing number of users and the expanding size of the communication networks and services, habits, preferences differences and the information needs of individual users and enterprises are gradually exposed. The customized networks and services now being provided for enterprise users, which makes the demand for specialized businesses stronger. In near future special service package for each user, and even a special network may be prioritizing. Such complex requirements would be unimaginable without an intellectual tool, such as AI.

## 2.2 Multimedia services

Internet users, now have also become information producers, as well as information consumers, and are producing more and more information in multimedia. User-generated content increases Internet traffic exponentially. Under these circumstances, both storage and transmission of data/ information are a great challenge. The inclusion of AI can bolsters the abilities to handle these challenges.

## 2.3 Precision management

The use of smartphones makes it inevitable that the various dimensions and granularities in today's wireless traffic system should be considered in the networks. With the development of the technologies of network function virtualization (NFV) and software-defined networks (SDN), the management of the network has become more precise. Virtualization is not only at the level of network elements, but also at the level of components such as the CPU, memory, port, bandwidth, etc. AI-based technologies allow operators to set up such on-demand networks for special users.

## 2.4 Predictable future

The increasing numbers of users and expansion of business requirements has meant that the gap between the peaks and troughs of network usage is becoming greater. In this case, operators are required to predict the future status of networks more accurately to satisfy users' demand and improve their experience. AI-driven predictive analytics are helping telecoms provide better services by utilizing data, sophisticated algorithms and machine learning techniques to predict future results based on historical data.

## 2.5 Intellectualization

Networks are becoming more heterogeneous as users often uses a variety of equipment with different wireless access technologies such as 2G, 3G, 4G, and Wi-Fi. Adoption of 5G will further reshape telecommunication networks in the near future. The network management becoming more difficult to maintain with an acceptable quality of service (QoS) due to the increase in network equipment and user terminals, the expansion of network size, the increase in the number of users, and the increasing complexity of the network. As well as expanding capacity by introducing more equipment, the operators are expected to raise their network performance with smart tools and intelligence technologies. This includes introducing more intelligence into networks and management to meet customer needs, make more profits, reduce operating costs, and improve network performance.

## 2.6 More attention to security and safety

As AI develops, security and security will be significant factors for everyone involved in these technologies. Security incidents are growing and becoming more severe. These events have resulted in significant commercial consequences, including broken networks, economic losses, etc. AI can be used to establish strong security protection and behavioral analysis based on machine learning, will significantly improve the ability of network detection attacks, automatic analysis of data, and the identification of relationships between isolated behaviors.

## 2.7 Trends of mobile network

Today, the application of virtualized network functions (NFV) to mobile core networks is in progress. For years, various network functions, such as the conventional Evolved Packet Core (EPC), have been provided in their dedicated hardware (HW) such as Advanced Telecom Computing Architecture (ATCA) hardware. With the introduction of NFV, software will be able to run on a virtualized operating system (OS) of generic Intel architecture (IA) servers and be provided separately from hardware. Furthermore, the NFV architecture enables integrated management and control (orchestration) of network services and resources, interworking with Management and Orchestration. The application of AI will enable to respond to the above-mentioned problems in the planning and maintenance processes quickly and efficiently.

## 2.8 Big data for development and ICT monitoring

Big Data and AI are set of two amazing modern technologies that empower machine learning, continuously reiterate and update the data banks, and taking the help of human intervention and recursive experiments for the same. Data combined with steady advances in the power of computing are leading to the emergence of data-driven innovation: online activity and networked things generate “big data” which feed machine learning that enables AI, which in turn leads to advances in intelligent machines (robotics, automated vehicles) as well as new techniques in science which can spur further innovation. The growth of the volume, variety and velocity of data and the ability to analyze and use it is a significant departure from the past and marks the emergence of a new factor of production that augments traditional capital and labor, but with unique properties of its own.

One of the richest sources of big data is the data captured by the use of ICTs. This broadly includes data captured directly by telecommunication operators as well as by Internet companies and by content providers such as Google, Facebook, Twitter, etc. Big data from the ICT services industry are already helping to produce large-scale development insights of relevance to public policy. Collectively, they can provide rich and potentially real-time insights

to a host of policy domains. In some countries and regions, the use of big data, including big data from the ICT industry, is subject to national regulation.

## 3. Advantages of Artificial Intelligence:

In the communications industry, whether its network operators, equipment manufacturers or solution providers, the industry hopes to take advantage of AI to assist in areas in which they are currently struggling, such as in designing, operating, maintaining and managing communication networks and services. Some of the advantages of AI are as follows:-

### 3.1 Abilities of learning

Operators need intelligent decisions to manage complex resources and dynamic traffic. With capability to describe the network traffic characteristics accurately, AI has entered into the cognitive age, and deep learning can be used, where the machine system can use the existing training data to process large amounts of data through data mining. AI can also learn the characteristics of data traffic, management, controls and other characteristics automatically and master expert experience of operating, managing and maintaining networks. By these efforts, the accuracy of analysis can be enhanced, and the intelligent management and services of communication networks can be realized.

### 3.2 Abilities of understanding and reasoning

Due to the dynamics of the network system, the state information of a resource may have changed when it is transmitted to the network management system. Therefore, the network management can only know the local state information without the knowledge about the system internal state. Machine learning happens to have the strength to deal with this kind of logic and uncertainty reasoning. In order to make the classification or prediction easier, deep learning constructs a multi-hidden layer model and uses the hierarchical network structure to transform the feature representation of the sample into a new feature space layer by layer.

### 3.3 Ability of collaborating

Due to the expansion of the network both in scale and size, the structure complexity of communication networks are increasing quickly. Concepts such as distribution and hierarchy are often talked about in the network management. Management tasks and controls are distributed to the entire network. As a result, we have to deal with issues such as tasks' distribution, communication and collaboration between management nodes. If we introduce

the multi-agent collaboration of distributed AI into the network management, we can expect the ability to collaborate between network managers distributed in every layer.

# 4. Artificial Intelligence: Progress & possible uses in Communications

Innovative telecom operators use AI and machine learning to increase network reliability, improve customer satisfaction & retention, optimize their business processes for higher profit, and much more. The most visible use case for AI in telecoms is enhanced customer service. Other than customer service, telecoms use artificial intelligence in network maintenance. Top AI use cases are shown in Figure 1.

SDN, NFV, network slicing and other technologies, coupled with integrated network management systems have been able to directly issue orders which can be executed by network equipment, and DPI systems can be deployed on network equipment, and it is possible to realize real-time monitoring of networks and services and intelligent management.

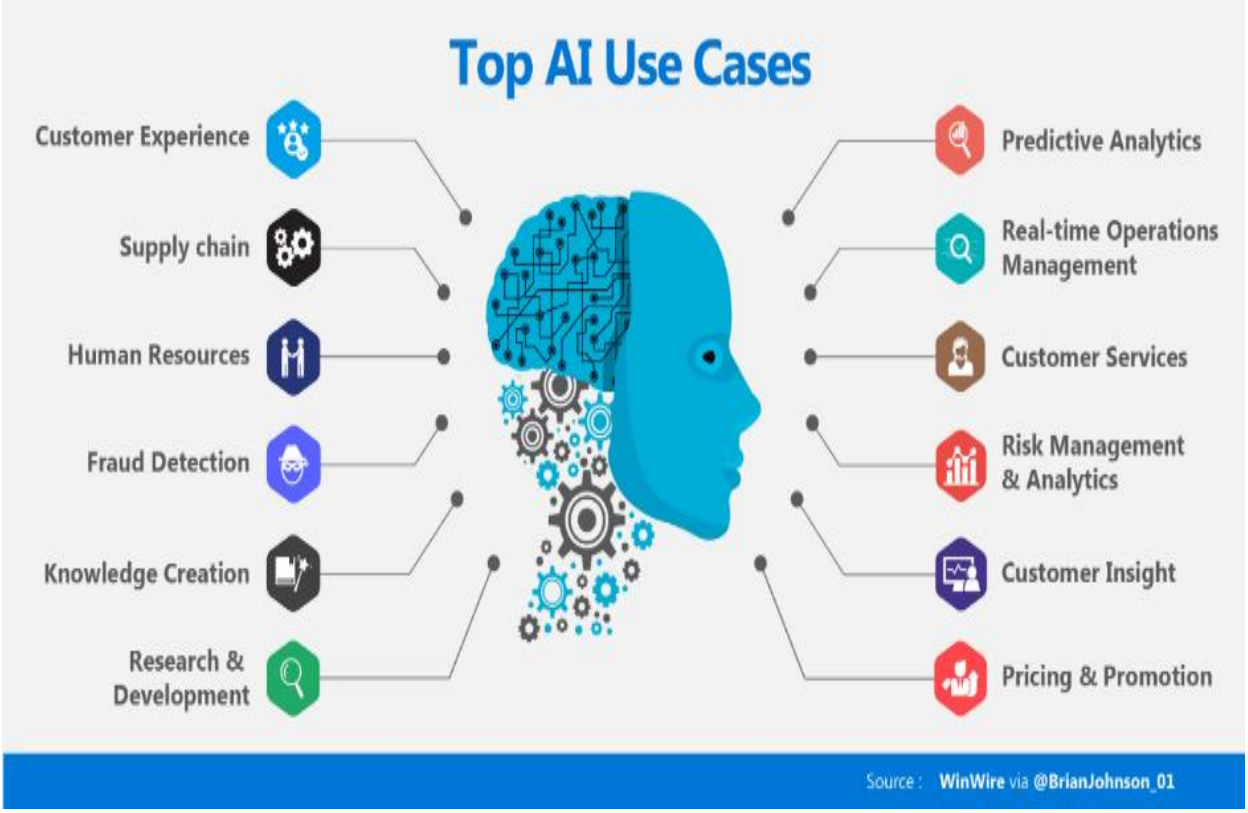



**Figure 1: AI use cases**

## 4.1 AI in SDN

Software defined networking (SDN) represents a promising networking architecture that combines central management and network programmability. SDN separates the control plane

from the data plane and moves the network management to a central point, called the controller that can be programmed and used as the brain of the network, which greatly promote the capabilities of network-automated management and control. A typical SDN framework is composed of three layers: infrastructure layer, control layer and application layer. The infrastructure layer includes some network elements which can provide network traffic, acting as the object controlled by the SDN controller, as well as a data source of the network resource. The control layer has the SDN controller, which is the core component of the SDN network carrying out important tasks of controlling network traffic. The application layer includes various applications. The southbound interface D-CPI (Data-Controller Plane Interface) is responsible for exchanging data between the SDN controller and the network element. The northbound interface A-CPI (Application-Controller Plane Interface) is responsible for providing the upper-level application with the channel exchange to obtain the underlying network resource information and send data to the lower-level network. SDN provides a good interface with its programmability to introduce AI into the communication networks. This is SDN's biggest advantage. SDN uses the application-programming interface to send powerful programming instructions to the network device.

With AI, network managers can not only schedule an automated intelligent business orchestrator, but also program the AI-optimized network strategy and automatically compile them into the task script, then assign them into the network allocation tasks with the application-programming interface (API). Network managers can also automatically collect network statistics information to lay a solid foundation for continuous network optimization. If necessary, some new functionalities can also be added intelligently through the SDN application for the network environment.

### 4.2 AI in NFV

With virtualization technology, Network Functions Virtualization (NFV) can divide network-level functions and applications, such as routing, customer premises equipment (CPE), mobile core, IP Multimedia Subsystems (IMS), content delivery networks (CDN), switching elements, mobile network nodes, home routing operations, set-top box business, tunnel gateway elements, traffic analysis, service assurance, service level agreement (SLA) monitoring, testing and diagnosis, next generation network (NGN) signal, aggregation and network range functions, application optimization, security policy, etc., into several functional blocks, and run them in software mode respectively. This means that they are no longer limited to the hardware architecture.

The typical NFV reference architecture includes three layers of the complete infrastructure layer, the resource management layer, and the business flow orchestrator layer. NFV helps ISV and telecommunication operators to achieve virtual network functions by deploying hypervisor at the infrastructure layer to virtualize infrastructure resources such as commercial general computing, storage and network resources and others. The resource management layer is in charge of the NFV infrastructure's management, configuration and collaboration. The business flow orchestrator layer is a key part of the NFV network function for network operating; it is used to organize and orchestrate the functions of the NFV network. It is also in charge of managing and monitoring the global resources across the data center or the resource pool.

With the virtualization of network functions NFV can realize an on-demand dynamic network configuration separated from the underlying architecture. As key issues have been solved, AI can play its full role in critical network management.

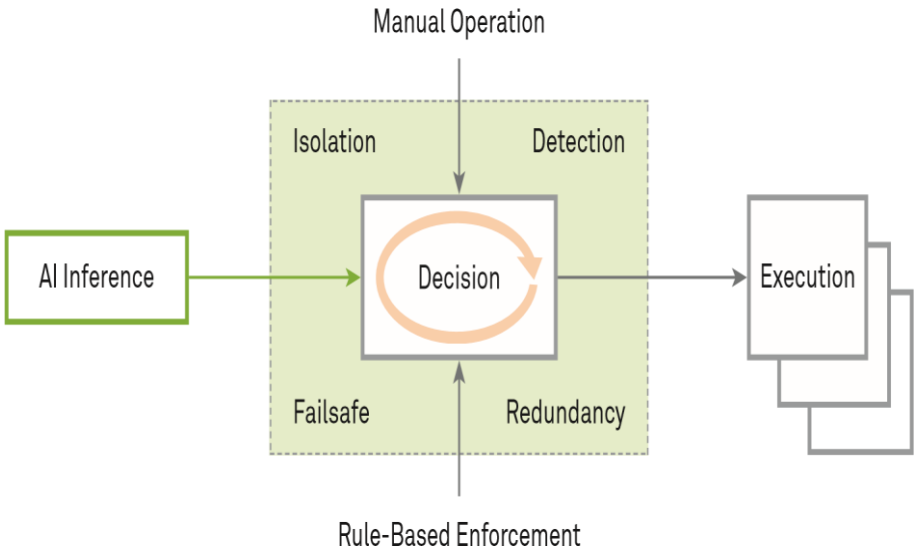
### 4.3 AI and Network monitoring, security and reliability:

To master the real-time information of the communication network, the network must have the function of initiative uploading. Currently there are many DPI systems. With inspectors, the deep packet inspection (DPI) system can collect the information such as the running state of network equipment, the usage of resources and the quality of services. With the big data obtained from the DPI system, the AI system can rapidly analyse and find if there are or will be abnormity within the information. For example, if the AI system finds a burst a continuous traffic, it can doubt a distributed denial of service (DDoS) attack in the network and analyse the package characteristics immediately, then orchestrate an inspector collaboration task to drop all packages with the characteristics to avoid the damage. It could write a new record in the security database in case of the appearance of unknown hack attacks or new virus flooding.

While developing AI systems, attention must be paid to the potential security risks; strengthen prevention mechanisms and constraint conditions; minimize risks; and ensure AI's secure, reliable, and controllable development. When applying AI models, it needs to analyze and determine the risks in using AI technology based on the characteristics and architecture of specific services, and design a robust AI security architecture and deployment solution using security mechanisms involving isolation, detection, failsafe, and redundancy (Figure 2).

By detecting unusual network activity at every level of the network, an AI-enabled platform can accurately detect existing and day-zero threats. In addition, location technology can be

used to accurately locate accidental or malicious rogue devices and provide location-based access to resources.




(Source: Huawei)

**Figure 2 Security architecture for AI with business decision making**

**i) Isolation:**

To ensure stable operation, an AI system analyzes and identifies the optimal solution and sends it to the control system for verification and implementation. Generally, the security architecture must isolate functional modules and setup access control mechanisms between modules. The isolation of AI models can reduce the attack surface for AI inference, while the isolation of the integrated decision module can reduce attacks on the decision module. The output of AI inference can be imported into the integrated decision module as an auxiliary decision-making suggestion, and only authorized suggestions can enter the decision module.

**ii) Detection:**

Adopting continuous monitoring and with an attack-detection model in the main system architecture, it is possible to comprehensively analyze the network security status and estimate the current risk level. When the risk is high, the integrated decision system can reject the suggestion coming from the automatic system and hand over control to a person to ensure security under attacks.

**iii) Failsafe:**

When a system needs to conduct critical operations such as AI-assisted autonomous driving or medical surgery, a multi-level security architecture is required to ensure the entire system

security. The certainty of the inference results provided by the AI system must be analyzed. When the certainty of the result is lower than a certain threshold, the system falls back to conventional rule-based technologies or manual processing.

**iv)Redundancy:**

Many business decisions and data are associated with each other. A feasible method to ensure the security of AI models is to analyze whether the association has been ruined. A multi-model architecture can be set up for critical applications, so that a mistake in one model does not keep the system from reaching a valid decision. In addition, the multi-model architecture can largely reduce the possibility of the system being fully compromised by a single attack, thereby improving the robustness of the entire system.

## 4.4 AI and QoS:

The AI module consists of two different parts. The first one is a classifying part, which detects the type of traffic that is sent through the network. The second part is an estimator that informs the SDN controller on which kind of action should be executed to guarantee the Quality of Service (QoS) and Quality of Experience (QoE). Results show that with the actions performed by the network, problems like jitter and losses can be reduced.

## 4.5 ITU Work/ Focus Group on Machine Learning 5G:

ITU-T under its Study Group 13 has established a Focus Group on Machine Learning for Future Networks including 5G, to draft technical reports and specifications for machine learning (ML) for future networks, including interfaces, network architectures, protocols, algorithms and data formats. The major objectives of FG-ML5G includes:

- To help adoption of ML in future networks including architecture, interfaces, use cases, protocols, algorithms, data formats, interoperability, performance, evaluation, security and protection of personal information;
- To study, review and survey existing technologies, platforms, guidelines and standards for ML in future networks;
- To recognize and highlight the various perspectives for the future of networks and computing systems involving ML;
- To identify aspects enabling safe and trusted use of ML frameworks;
- To identify possible requirements on network functionality, interfaces and capabilities to use ML;
- To identify challenges in the standardization activities for ML in communications;

- To establish liaisons and relationships with other organizations which could contribute to the standardization activities for ML.

## 5. AI Challenges and Opportunities:

With humans and machines joining forces now, more than ever before, AI is no longer confined to innovation labs and is being hailed for its immense transformational possibilities. However, businesses including telecom need to overcome certain challenges before they can realize the true potential of this emerging technology. The key lies in leveraging the right opportunities in AI.

### (i) Provability:

Organizations involved in AI cannot demonstrate clearly, why it does and what it does. No wonder AI is a "black box" as of now. People are skeptical about it, as they fail to understand how it makes decisions. Provability – the level of mathematical certainty behind AI predictions – remains a grey area for organizations. There is no way they can prove or guarantee that the reasoning behind the AI system's decision-making is clear. The solution lies in making AI explainable, provable, and transparent. Organizations must embrace Explainable AI as a best practice.

### (ii) Data privacy and security:

As AI develops, Privacy and security will be significant factors for everyone involved in these technologies. Most AI applications rely on huge volumes of data to learn and make intelligent decisions. Machine Learning systems use/ depend heavily on data, often sensitive and personal in nature, to learn from them and enhance themselves. This makes it vulnerable to serious issues like data breach and identity theft. Besides, an emerging method – 'Federated Learning', which is a machine learning setting where the goal is to train a high-quality centralized model with training data distributed over a large number of clients each with unreliable and relatively slow network connections– is all set to disrupt the AI paradigm. It will empower data scientists to develop AI without compromising users' data security and confidentiality.

### (iii) Algorithm bias

An inherent problem with AI systems is that they are only as good – or as bad – as the data they are trained on. Bad data is often laced with racial, gender, communal or ethnic biases. Proprietary algorithms are used to determine who is called for a job interview, who has granted bail, or whose loan is sanctioned. If the bias lurking in the algorithms that make vital decisions

goes unrecognized, it could lead to unethical and unfair consequences. For instance, Google Photos service uses AI to identify people, objects and scenes. However, there is a risk of it displaying wrong results, such as when a camera missed the mark on racial sensitivity, or when a software used to predict future criminals showed bias against black people.

In the future, such biases will probably be more accentuated, as many AI systems will continue to be trained using bad data. Hence, the need of the hour is to train these systems with unbiased data and develop algorithms that can be easily explained.

**(iv) Data scarcity**

It is true that organisations have access to more data today than ever before. However, datasets that are relevant for AI applications to learn are indeed rare. The most powerful AI machines are the ones that are trained on supervised learning. This training requires labeled data – data that is organised to make it ingestible for machines to learn. Labeled data is limited. In the not-so-distant future, the automated creation of increasingly complex algorithms, largely driven by deep learning, will only aggravate the problem. There is a ray of hope though. As a trend that is fast catching up, organisations are investing in design methodologies, trying to figure out how to make AI models learn despite the scarcity of labeled data. 'Transfer learning', 'Unsupervised/Semi-Supervised Learning', 'Active Learning', and so on are just a few examples of the next-generation AI algorithms that can help resolve this.

## 6. Ethical use of AI

Artificial Intelligence is seen as a great transformative tech and the possibilities seem almost limitless to what it can eventually do. With these disruptive developments, questions arises about the functional capabilities to the ethics behind creating such powerful and potentially life-consequential technologies. As such, it makes sense to spend time considering what we want these systems to do and make sure we address ethical questions now so that we build these systems with the common good of humanity in mind. Following 9 ethical issues have been identified at World Economic Forum–ASEAN Summit 2018 titled "Top 9 ethical issues in artificial intelligence: -

(i) **Unemployment**- what happens after the end of jobs
(ii) **Inequality** -how do we distribute the wealth created by machines
(iii) **Humanity** –how do machines affect our behavior and interaction
(iv) **Artificial stupidity** – how can we guard against mistakes
(v) **Racist robots**-how do we eliminate AI bias

(vi) **Security** –how do we keep AI safe from adversaries

(vii) **Evil genies**-how do we protect against unintended consequences

(viii) **Singularity** –how do we stay in control of a complex intelligent system

(ix) **Robot rights** - how do we define the humane treatment of AI

## 7. Conclusion:

AI and Big Data are two of the emerging technologies that are used in Telecommunications sector extensively, helping CSPs manage, optimize and maintain not only their infrastructure, but their customer support operations as well. This paper has highlighted an AI-based network framework to introducing AI in communication networks and services, with SDN/ NFV collaboratively deployment. Technology is already a core part of the telecommunications industry, and as Big Data tools and applications become more available and sophisticated, AI can be expected to continue to grow in this space.

**Abbreviations:**

| | |
|---|---|
| AI: | Artificial Intelligence |
| SDN: | Software Defined Networks |
| NFV: | Network Function Virtualization |
| QoS: | Quality of Service |
| QoE: | Quality of Experience |
| IMS: | IP Multimedia Subsystems |
| ICT: | Information & Communication Technologies |
| DPI: | Deep Packet Inspection |
| DDoS: | Distributed Denial of Service (DDoS) |
| CDN: | Content Delivery Networks |
| NGN: | Next Generation Network (NGN) |
| EPC: | Evolved Packet Core |
| OS: | Operating system |
| FG-ML5G: | Focus Group- Machine Learning 5G |

**References:**


[1] http://www.oecd.org

[2] https://www.itu.int/en/journal/001/Documents/ITU2017-4.pdf

[3] https://www.itu.int/en/journal/001/Documents/itu2017-7.pdf

[4] https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/

[5] http://www.forbesindia.com/blog/business-strategy/artificial-intelligence-key-challenges-and-opportunities/

[6] https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/ai-security-white-paper-en.pdf?la=en&source=corp_comm

[7] https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx


*********