ITUEvents

India Round– Part 2: AI Techniques for privacy-preserving remote medical diagnosis + spectrum and network resource sharing in 5G networks: ITU-ML5G-PS-21, 22

Prof. Brejesh Lall, IIT/D 27 July 2020

ITU

AI/ML in 5G Challenge

Applying machine learning in communication networks

ai5gchallenge@itu.int

Register here

Join us on Slack

Sponsors

CISCO ZTE

Organizer

ITU

ITU AI/ML in 5G Challenge

Dr. Brejesh Lall
Prof., EED, IITD

brejesh@ee.iitd.ac.in
Indian Institute of Technology, Delhi, India

Website:
https://sites.google.com/view/iitd5g/

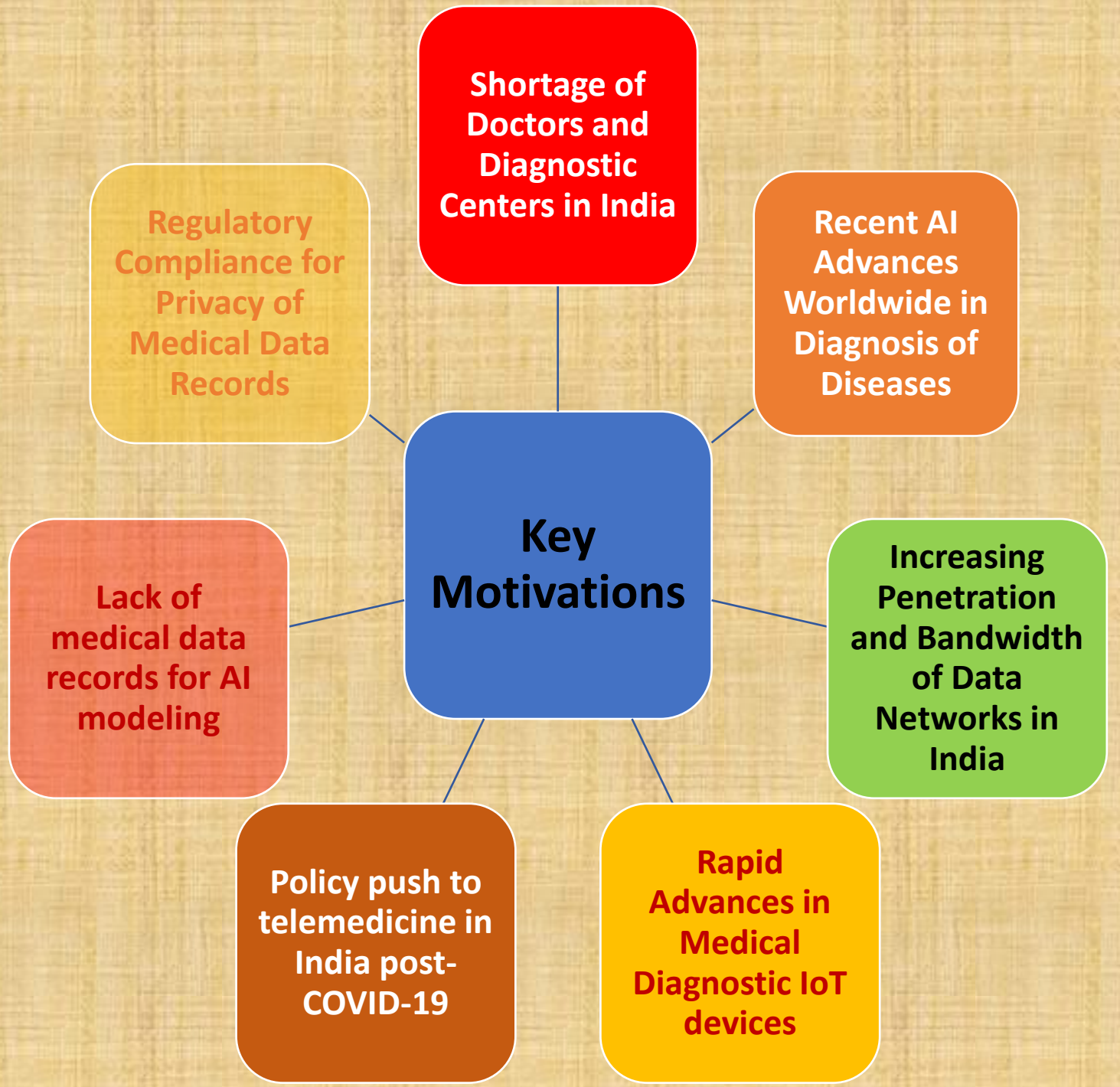
IEEE ComSoc
IEEE Communications Society
Delhi Chapter

Challenge ITU-ML5G-PS-022: Privacy Preserving AI/ML in 5G networks for healthcare applications

prashant@cdot.in

URL: https://sites.google.com/view/iitd5g/

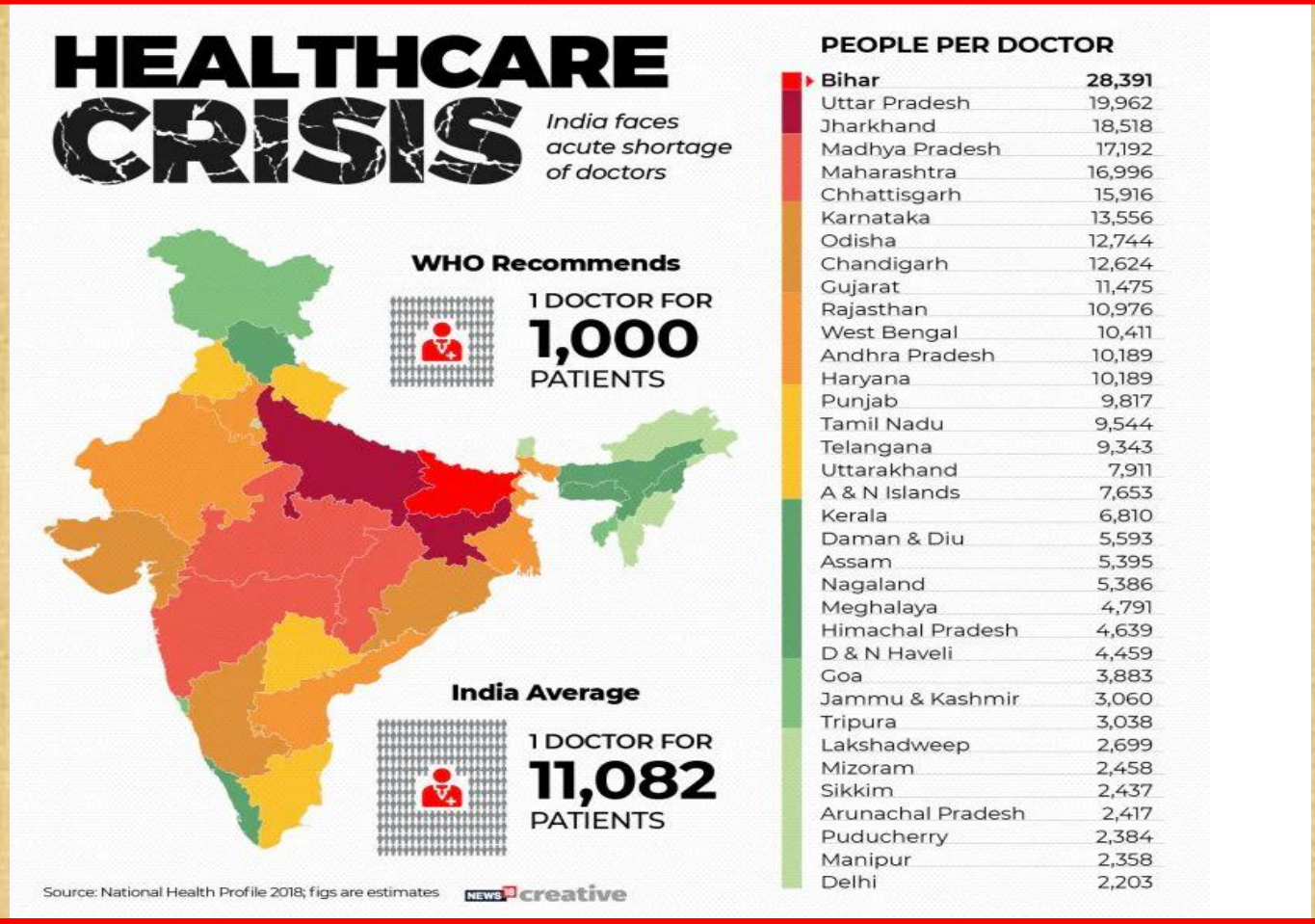
IEEE ComSoc
IEEE Communications Society
Delhi Chapter



URL: https://sites.google.com/view/iitd5g/

IEEE ComSoc
IEEE Communications Society
Delhi Chapter

Shortage of Doctors & Diagnostic Centers especially in Rural and Remote Areas in India



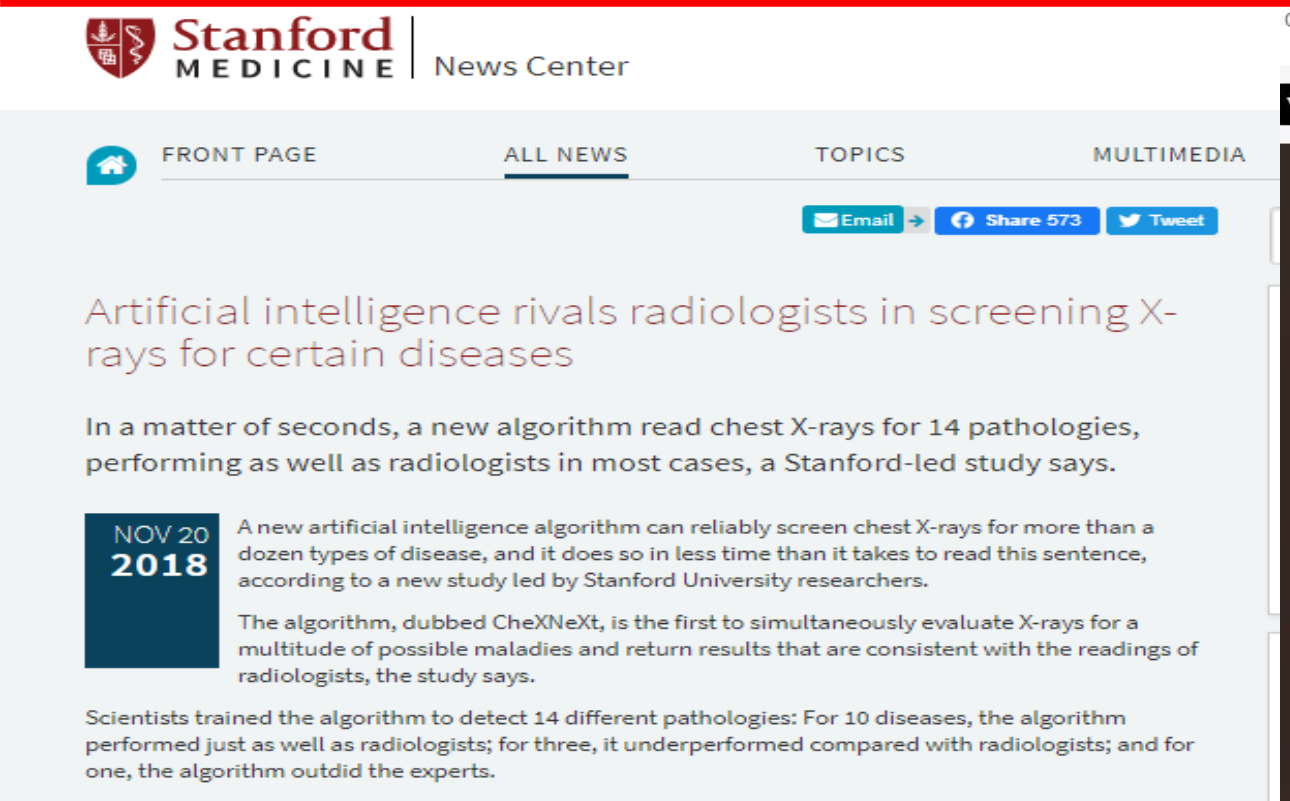
URL: https://sites.google.com/view/iitd5g/

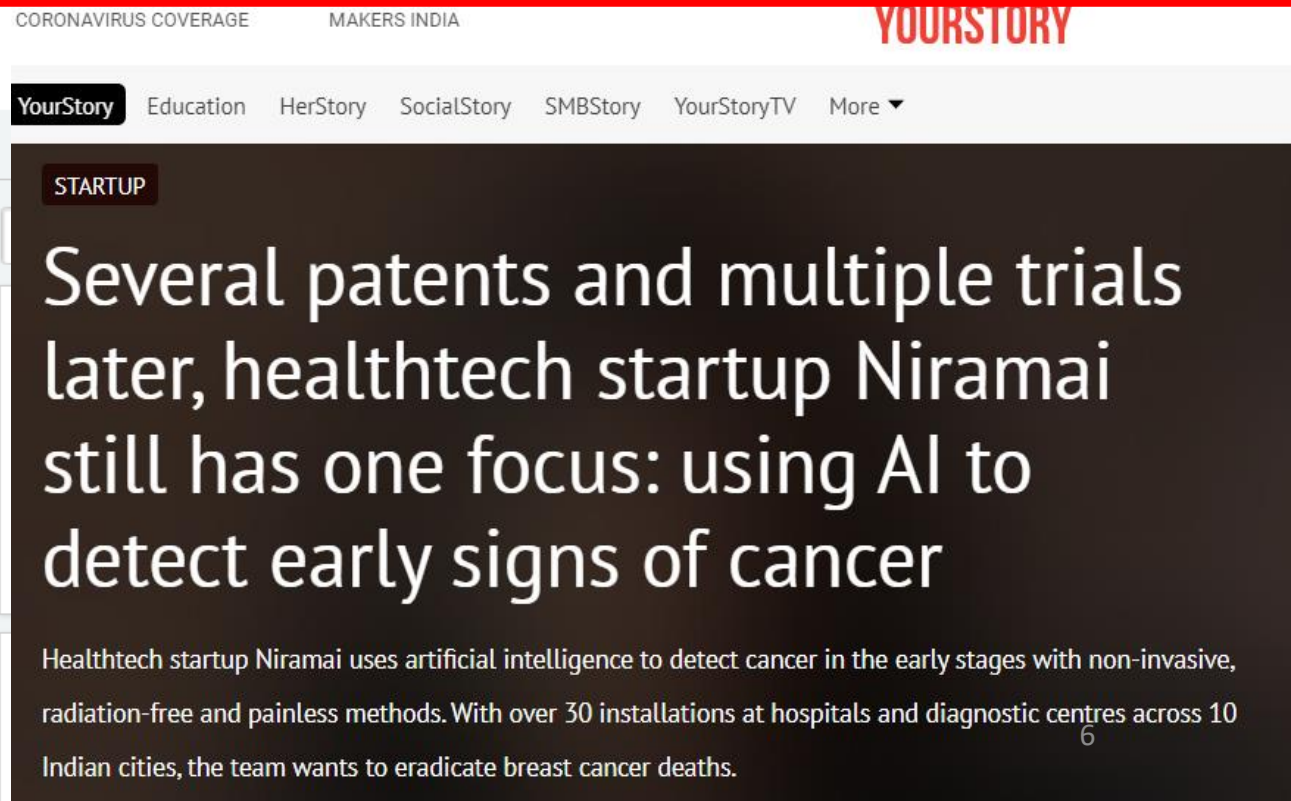
IEEE ComSoc
IEEE Communications Society
Delhi Chapter

Recent AI Advances Worldwide in Diagnosis of Diseases

AI algorithms have seen recent advancements in Diagnostic of Diseases such as:

- Diabetic Retinopathy
- Tuberculosis
- Breast cancer
- Brain Tumors





Lack of medical data records for AI modeling

- AI in medicine is hindered by limited dataset availability for algorithm training and validation
- Further, the available datasets do not have diversity. They are usually from a few institutions, geographic regions or patient demographics, and might therefore contain unquantifiable bias
- Individual healthcare institutes may have archives containing hundreds of thousands of records and images, but these data sources are typically kept siloed
- There are frequent security breaches of medical data records which leads to penalty as well as loss of reputation
- Security breaches discourage others to keep medical data records over the network

Healthcare providers that underwent cyberattacks in 2020 so far

Katie Adams - Monday, July 6th, 2020 Print | Email

Share Tweet Share 47

Here are the healthcare providers that experienced malware, ransomware and phishing incidents *Becker's Hospital Review* reported during the first half of 2020.

1. University of Florida, UF Health Shands in Gainesville and UF Health Jacksonville all reported email hacking incidents associated with an attack on a business associate that affected thousands of individuals.
2. Florida Orthopaedic Institute found that some personal information had been exposed during a ransomware attack on encrypted data stored on its servers.
3. University of California San Francisco paid $1.14 million to hackers after a ransomware attack on its medical school's computer servers.
4. Miami-based Cano Health reported a data breach that affected 28,268 individuals.
5. A data security incident involving Care New England's computer system caused the Providence, R.I.-

The Daily Swig

Cybersecurity news and views

Data Breaches Cyber-attacks Vulnerabilities Bug Bounties

LibreHealth medical records app exposes sensitive patient data

Jessica Haworth 17 July 2020 at 14:30 UTC

July 08, 2020 - The healthcare sector saw a whopping 41.4 million patient records breached in 2019, fueled by a 49 percent increase in hacking, according to the **Protenus** Breach Barometer. And despite the COVID-19 crisis, the pace of healthcare data breaches in 2020 continue to highlight some of the sector's biggest vulnerabilities.

The end of **2019** saw a host of ransomware attacks and vendor-related breaches that outpaced previous years in the healthcare sector. For comparison, the industry saw just 15 million records breached **in 2018**.

But while phishing campaigns tied to the Coronavirus peaked in **mid-April**, the rate of ransomware attacks and reported data breaches slowed amid the crisis. However, security **researchers** noted that though ransomware attacks remained flat from the rate seen at the end

Regulatory Compliance for Privacy of Medical Data Records

- HIPAA regulations in USA and GDPR compliance in Europe, make it mandatory to protect privacy of medical data.
- In India, Supreme Court declared right to privacy as a fundamental right in 2017
- Personal Data Protection (PDP) Bill introduced in Indian parliament in Sec 2019 sets rules for how personal data should be processed and stored, and lists people's rights with respect to their personal information
- Health Data is listed under Sensitive Personal Data under this PDP Bill which is expected to become a law in 2020

India: Supreme Court Declares Right To Privacy A Fundamental Right

31 August 2017

by Trilegal .

Trilegal

5 Liked this Article

On 24 August 2017, the Supreme Court of India in a historic judgement declared the right to privacy as a fundamental right protected under the Indian Constitution. In declaring that this right stems from the fundamental right to life and liberty, the Court's decision has far-reaching consequences.

A nine-judge bench of the Supreme Court in the case of *Puttuswamy v. Union of India* has declared that the right to privacy is a fundamental right protected under Part III of the Constitution of India. While primarily focused on the individual's right against the State for violations of their privacy, this landmark judgement will have repercussions across both State and non-State actors and will likely result in the enactment of a comprehensive law on privacy.

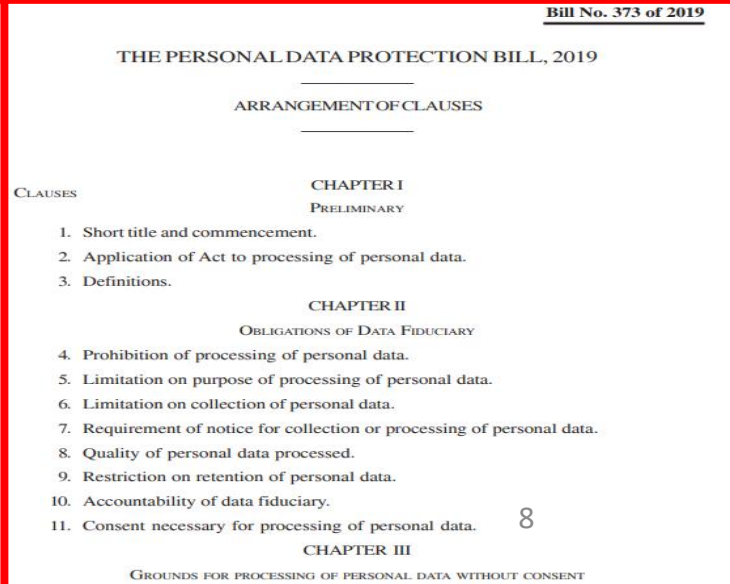
News Features ETT SPECIAL Slideshows Tele-Bytes Live Sessions

Telecom News / Latest Telecom News / Policy

Data nation's asset; must be secured: Ravi Shankar Prasad

Data is a nation's asset and it should be utilised properly for achieving prosperity, especially in sectors like healthcare, agriculture and education, Union Minister Ravi Shankar Prasad said on Saturday.

PTI • July 19, 2020, 10:29 IST



Bill No. 373 of 2019

THE PERSONAL DATA PROTECTION BILL, 2019

ARRANGEMENT OF CLAUSES

CLAUSES

CHAPTER I

PRELIMINARY

1. Short title and commencement.
2. Application of Act to processing of personal data.
3. Definitions.

CHAPTER II

OBLIGATIONS OF DATA FIDUCIARY

4. Prohibition of processing of personal data.
5. Limitation on purpose of processing of personal data.
6. Limitation on collection of personal data.
7. Requirement of notice for collection or processing of personal data.
8. Quality of personal data processed.
9. Restriction on retention of personal data.
10. Accountability of data fiduciary.
11. Consent necessary for processing of personal data.

CHAPTER III

GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT

Increasing Penetration and Bandwidth of Data Networks in India

- Over past few years, India has seen increased penetration and bandwidth of data networks primarily due to proliferation of Mobile 4G Networks
- This trend is expected to further increase in future due to deployment of 4G networks in rural and remote areas as well as due to upcoming 5G Networks
- Since urban areas are already saturated, Rural and remote areas (which are grossly underserviced) are expected to see high growth

India's digital revolution continues to be propelled by the rural masses

Rural India registered a 45% growth in the monthly active internet users in 2019. It is now estimated that there are 264 million internet users in rural India, and this is expected to reach 304 million in 2020.

THE ECONOMIC TIMES | Industry

English Edition | E-Paper

Home Industry Auto Banking/Finance Cons. Products Energy Ind'l Goods/Svs Healthcare/Biotech

Telecom News | Telecom Policy

Business News › Industry › Telecom › Telecom News › 4G dominates overall data traffic in India, 3G falls sharply: Study

4G dominates overall data traffic in India sharply: Study

ET Bureau • Last Updated: Feb 27, 2020, 01:14 PM IST

SHARE

Synopsis

"Data consumption in India has grown by 47% in 2019 with 4G constituting 96% of the total data traffic consumed across the country. 3G data traffic registered its highest ever decline of 30% in 2019," a study showed. However, broadband penetration in India is still 47% which is significantly lower than China (95%) and other European nations at around 95-115%.

Advances in Medical Diagnostic IoT devices (Internet of Medical Things or IoMT)

BUSINESS OPPORTUNITY INDUSTRY ANALYTICS

IoT Medical Devices Market to Witness Robust Expansion throughout the COVID-19

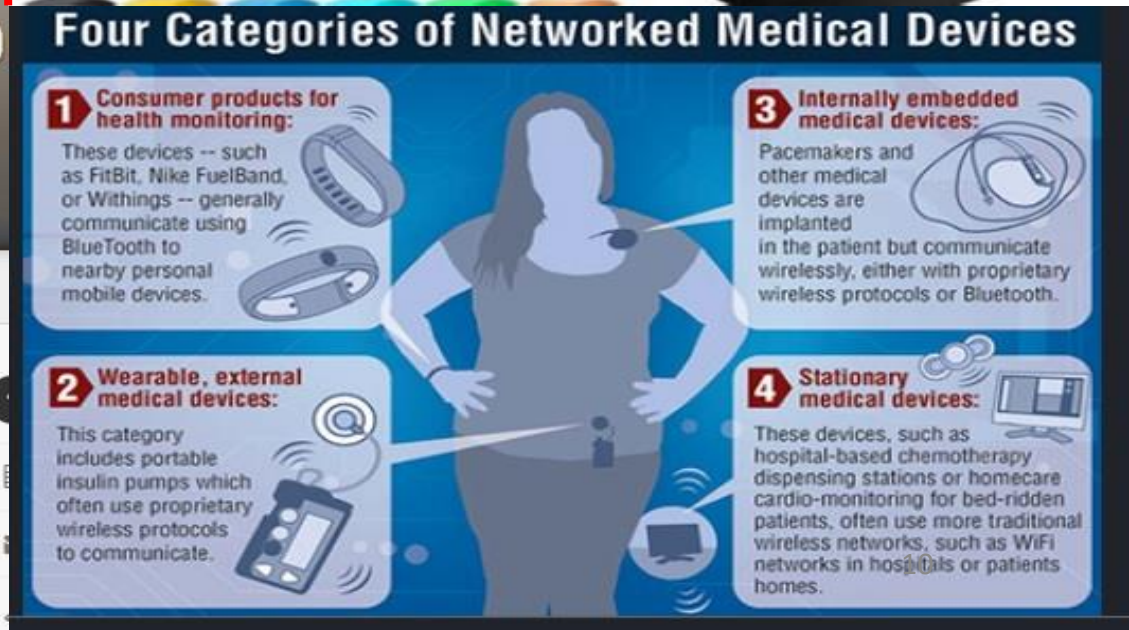
By johnsimth1212@gmail.com July 15, 2020

DIGITAL INFORMATION WORLD ABOUT US

IoT in Healthcare Expectations for 2020

Web Desk Thursday, February 13, 2020

The Internet of things (IoT) is poised to transform the healthcare industry to the same degree it has changed the way businesses operate and impacted the lives of countless individuals around the world. Data collected from Internet of medical things (IoMT) devices makes it possible to deliver healthcare in more effective and creative ways. Additional information obtained through IoT monitoring devices analyzed with the help of AI applications in healthcare will allow medical professionals to develop more focused and personalized treatment programs for their patients and increase the well-being of the global population.



Policy push to telemedicine in India post-COVID-19

- Ministry of Health in India in partnership with NITI Aayog (the premier policy 'Think Tank' of the Government of India) has released Telemedicine Guidelines in March 2020
- Guidelines mention that technologies such as Artificial Intelligence, Internet of Things, advanced data science-based decision support systems etc. can be used to assist and support a RMP (Registered Medical Practitioner) for patient evaluation, diagnosis or management

BOARD OF GOVERNORS

In supersession of the Medical Council of India

Telemedicine Practice Guidelines

Enabling Registered Medical Practitioners to Provide Healthcare Using Telemedicine

[This constitutes Appendix 5 of the Indian Medical Council (Professional Conduct, Etiquette and Ethics Regulation, 2002]

25 March 2020

NITI Aayog

English | Hindi

deralism · Competitive Federalism · Think Tank · SDGs · Monitoring & Evaluation · Atal Innovation Mission · Verticals · Publications · Work With NITI · RTI

Telemedicine: A Blessing In Disguise In Time Of COVID-19

6 May 2020 - 0 Submitted by

Sh. R Ramanan(Additional Secretary and Mission Director, Himanshu Agrawal(Young Professional, AIM, NITI Aayog)AIM, NITI Aayog), Naman Agrawal(Innovation Lead, AIM, NITI Aayog)

At this hour of Coronavirus Disease 2019 (COVID-19) chaos and unease, social distancing is one of the primary measures taken by nations to combat the COVID-19 pandemic.

World Health Organization (WHO) has also recognised telemedicine[1] as an essential step in strengthening Health System Response to COVID-19. WHO also recommended, telemedicine as one of the alternative models to boost clinical performance and support decisions in the context of optimising service delivery.

In India, there are a lot of imbalances and bottlenecks in terms of healthcare infrastructure, which include uneven quality and access to health services.

Privacy Preservation Techniques (PPT) for AI

- Privacy Preserving Techniques (PPT) refers to the set of techniques that are used to ensure that the data records can be used for AI algorithmic training without disclosing the personal identifiable information (PII) of data records.
- The objective of PPT is to respect the privacy and the security of the underlying data while still being able to train and use AI systems.

Need for Privacy Preservation Techniques for AI in Healthcare

- PPT assures the medical data providers (individuals or diagnostic centers or hospitals) to provide medical data records for training of AI-based algorithms for medical diagnosis.
- There are multiple hospitals that have patient data. If all that data could be used for AI training using PPT, then much better diagnosis algorithms can be developed.

URL: https://sites.google.com/view/iitd5g/

IEEE ComSoc IEEE Communications Society Delhi Chapter

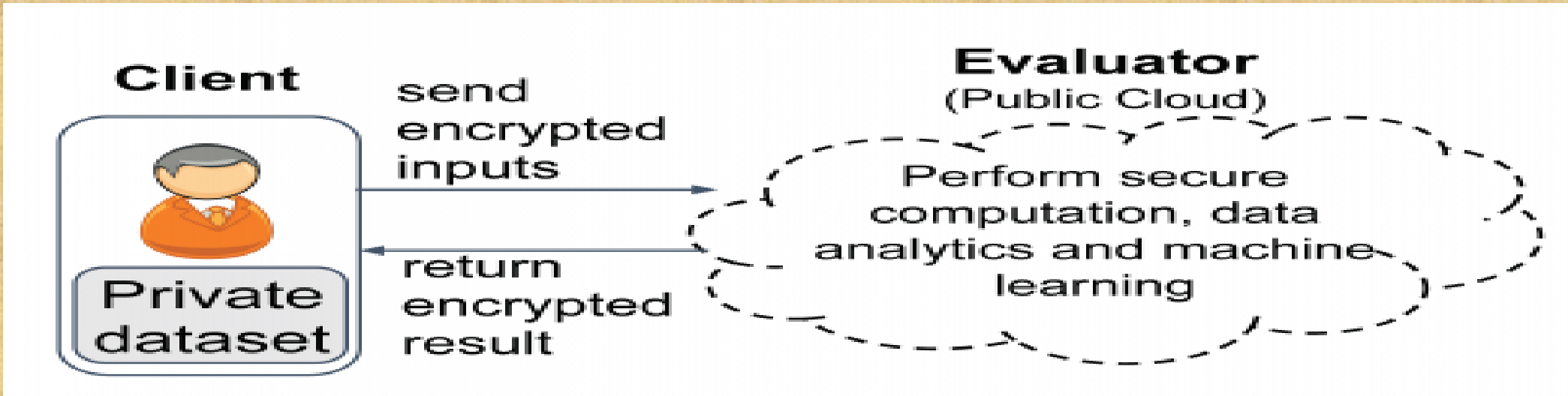
Current Common Privacy Preservation Techniques

- Homomorphic Encryption
- Federated Learning
- Differential Privacy
- Secure Multi Party Computation

URL: https://sites.google.com/view/iitd5g/

Homomorphic Encryption

- It is a type of encryption technique which allows functions to be computed on encrypted data.
- Data owner can encrypt the data with a unique private key. Thus, personal data remains secure and private even when it is being used to train the AI algorithms for medical diagnosis.



URL: https://sites.google.com/view/iitd5g/

IEEE ComSoc
IEEE Communications Society
Delhi Chapter

Federated Learning

- Federated learning is a technique of training machine learning algorithms on private, fragmented data, stored on distributed servers and devices.

Key Feature:

- This technique decentralizes deep learning by removing the need to pool data into a centralized location. Instead, the model is trained in multiple iterations at different distributed sites
- Data at each distributed site/client remains private

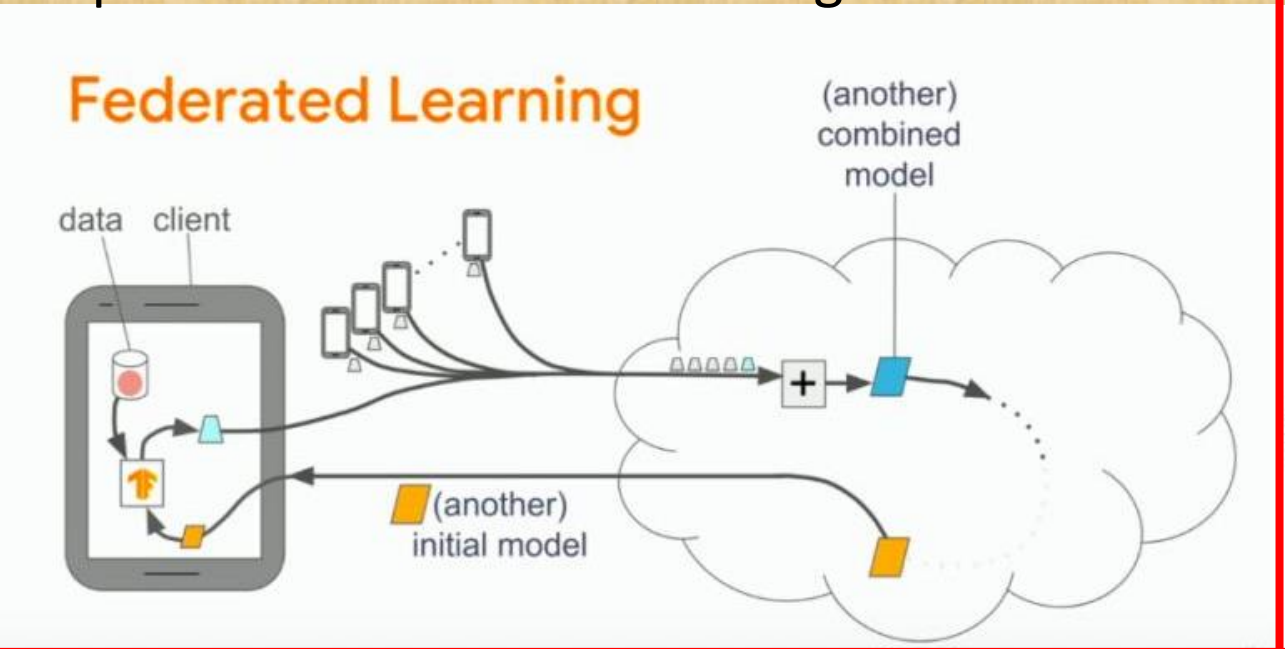
Steps:

- Training on the same algorithm is done at multiple distributed locations using the minimal data available at each distributed location.
- The trained algorithm parameters (and not the data) is pooled on a central server, which aggregates all their contributions into a new, composite algorithm.
- These steps are repeated leading to models across distributed locations to converge.

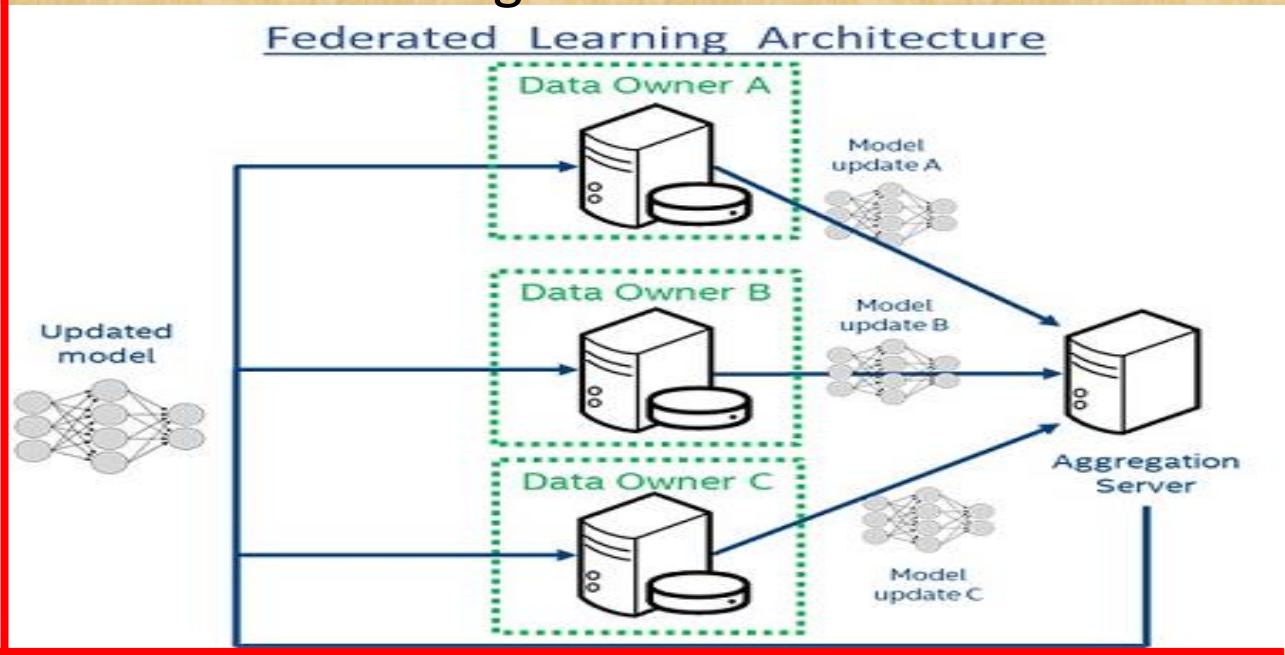
URL: https://sites.google.com/view/iitd5g/

Federated Learning Illustrated

Scenario 1: A very large number of distributed devices (such as mobile phones or IoT Sensors) each having some quantity of private data required for distributed training



Scenario 2: A few number of distributed devices (such as data servers) each having a large quantity of private date required for distributed training



URL: https://sites.google.com/view/iitd5g/

IEEE ComSoc
IEEE Communications Society
Delhi Chapter

Differential Privacy

- This technique involves injecting a small amount of noise into the raw data before feeding it into a local machine learning model, thus making it difficult for malicious actors to extract the original files from the trained model.
- An algorithm can be considered differentially private if an observer seeing its output cannot tell if it used a particular individual's information in the computation.
- Differential Privacy provides a mathematically provable guarantee of privacy protection against a wide range of privacy attacks including differencing attack, linkage attacks, and reconstruction attacks

URL: https://sites.google.com/view/iitd5g/

Types of Differential Privacy

- **Centralized Differential Privacy**

In this approach, the noise that protects the data set is added after the fact by the party that collected the information

- **Local Differential Privacy**

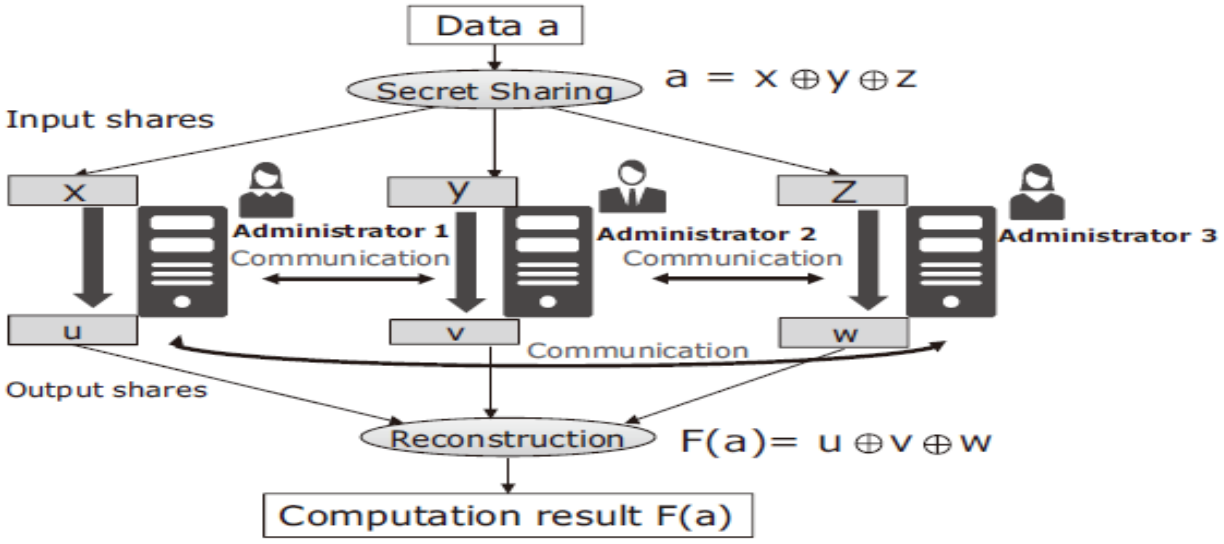
In this approach, the noise is directly built into the act of collecting data. In this way, there's not even an original "true" database to safekeep — the holder of the information never got it in the first place.

URL: https://sites.google.com/view/iitd5g/

Secure Multi-Party Computation (MPC)

- Secure Multi-Party Computation (SMPC) is a generic cryptographic primitive that enables distributed parties to jointly compute an arbitrary functionality without revealing their own private inputs and outputs.
- MPC is based on Shamir's Secret Sharing Scheme

- Private data is split into several, smaller parts. Each part of this data is sent to a separate independent server, so that each server processes only a small part of the private data.
- Result is constructed by combining processed outputs of all the distributed servers



URL: https://sites.google.com/view/iitd5g/

IEEE ComSoc
IEEE Communications Society
Delhi Chapter

Note to Participants

- Each of the Privacy Preservation Techniques when applied to training AI algorithms has some advantages. Participants need to study both advantages and limitations of all PPTs and then decide which PPT technique is more suitable.
- It may also be more suitable, to combine some or all of the Privacy Preservation Techniques to evolve a new combo PPT scheme that maximizes advantages and minimizes limitations of individual PPT schemes, to arrive at the best solution
- Problem Statement, Evaluation Criteria, Data Sources, Resources, References etc. are already mentioned under problem# ITU-ML5G-PS-022 at ITU web-site against URL: https://www.itu.int/en/ITU-T/AI/challenge/2020/Documents/ML5G-I-237-R5_v8.docx as well as on regional host website at https://sites.google.com/view/iitd5g/challenge-problems/privacy-preserving-aiml-in-5g-networks-for-healthcare-applications
- Some additional references for further study and libraries/ tools for implementation are also being provided on the next two slides

Challenge Statement

- Design & Implement a suitable Privacy-Preserving AI Technique to share Patient Data Records available in multiple Distributed Patient Data Repositories and use the shared data to train a data model for medical diagnosis.
  - This must be done without compromising the privacy of patient data records.
- Host the trained data model on a web-server ensuring patient privacy is not compromised and implement REST APIs on the server for the purpose of inference from the trained data model.
- Implement an easy-to-use UI-based tool on a smartphone to do medical diagnostic inference for a patient by calling the REST APIs on the web-server.

References for Further Study (1 of 2) (Most of these are in addition to references provided with problem statement at the challenge web-sites)

Papers, Articles and Blogs:

1. "How To Backdoor Federated Learning" https://arxiv.org/pdf/1807.00459.pdf
2. Intel, Penn Medicine Launch Federated Learning Model For Brain Tumors - AI Trends https://www.aitrends.com/ai-in-medicine/intel-penn-medicine-launch-federated-learning-model-for-brain-tumors/
3. "Differential Privacy" MIT Technology Review https://www.technologyreview.com/technology/differential-privacy/
4. "CRYPTFLOW: Secure TensorFlow Inference" https://www.microsoft.com/en-us/research/uploads/prod/2019/09/CrypTFlow.pdf
5. https://www.unite.ai/what-is-federated-learning/

Books:

1. "The Algorithmic Foundations of Differential Privacy" https://www.cis.upenn.edu/~aaroth/privacybook.html
2. "A Pragmatic Introduction to Secure Multi-Party Computation" http://securecomputation.org/docs/pragmaticmpc.pdf

Youtube Videos:

1. **Differential Privacy:** https://youtu.be/gI0wk1CXlsQ https://youtu.be/-JRURYTfBXQ
2. **Secure MPC:** https://www.youtube.com/watch?v=-1H1Sp-_5YU

URL: https://sites.google.com/view/iitd5g/

References for Further Study (2 of 2)(Most of these are in addition to references provided with problem statement at the challenge web-sites)

Code Libraries and Tools:

1. https://github.com/IBM/fhe-toolkit-android/blob/master/GettingStarted.md
2. https://github.com/Microsoft/SEAL
3. https://palisade-crypto.org/
4. https://github.com/tf-encrypted/tf-encrypted
5. https://www.tensorflow.org/federated/get_started
6. https://github.com/IBM/federated-learning-lib
7. https://github.com/google/differential-privacy/
8. https://github.com/IBM/differential-privacy-library
9. https://github.com/tensorflow/privacy
10. https://github.com/opendifferentialprivacy/
11. https://github.com/Google/private-join-and-compute

URL: https://sites.google.com/view/iitd5g/

IEEE ComSoc
IEEE Communications Society
Delhi Chapter

Challenge ITU-ML5G-PS-021: Dynamic Resource (Spectrum) Access

amit.oberoi@alumni.iitd.ac.in

Challenge on Website

https://sites.google.com/view/iitd5g/challenge-problems/5g-mlai-dynamic-spectrum-access

Background

Today, the motivation for dynamic spectrum access allocation is for spectrum sharing between LTE and 5G to make 5G roll out faster and less costly. Use of Generalised Frequency division Multiplexing (GFDM) for opportunistic cognitive waveform as brought out in [1] for such a scenario has been discussed often. It has been proposed in [2] that network slicing and QoS techniques can be used for mission critical radio access in 5G.

However, it is expected that 5G systems would be capable of employing explosively scalable bandwidths for varying applications. Even though spectrum efficient schemes have been proposed to be deployed for 5G, the only way forward is to share the spectrum dynamically amongst users using cognitive approach. It has been shown in [3] that various strategies for spectrum and network resource sharing can be employed to get significant reduction in per user requirement. In [4] has been proposed to incorporate some degree of intelligence into the spectrum management process using a 'Smart Spectrum Model'. The concept is to use historical as well as real time inputs to take decisions for utilizing spectrum spaces by utilizing a three layered viz "data", "information" and "knowledge" model. The paper has carried out limited demonstrations to show improved performance at the physical layer for sensing spectrum utilization and taking a decision to either utilize an available free slot or to back off. It has been discussed in [5] that Machine Learning can be theoretically applied to most functions for 5G or Beyond 5G communications, however real world implementation of this would be costly, time consuming and complex and therefore it

3 GPP Release 17

Release 17

- NR MIMO
- NR Sidelink enh.
- 52.6 - 71 GHz with existing waveform
- Dynamic Spectrum Sharing (DSS) enh.
- Industrial IoT / URLLC enh.
- Study - IoT over Non Terrestrial Networks (NTN)
- NR over Non Terrestrial Networks (NTN)
- NR Positioning enh.
- Low complexity NR devices
- Power saving
- NR Coverage enh.
- Study - NR eXtended Reality (XR)
- NB-IoT and LTE-MTC enh.
- 5G Multicast broadcast
- Multi-Radio DCCA enh.
- Multi SIM
- Integrated Access and Backhaul (IAB) enh.
- NR Sidelink relay
- RAN Slicing
- Enh. for small data
- SON / Minimization of drive tests (MDT) enh.
- NR Quality of Experience
- eNB architecture evolution, LTE C-plane / U-plane split
- Satellite components in the 5G architecture
- Non-Public Networks enh.
- Network Automation for 5G - phase 2
- Edge Computing in 5GC
- Proximity based Services in 5GS
- Network Slicing Phase 2
- Enh. V2x Services
- Advanced Interactive Services
- Access Traffic Steering, Switch and Splitting support in the 5G system architecture
- Unmanned Aerial Systems
- 5GC LoCation Services
- Multimedia Priority Service (MPS)
- 5G Wireless and Wireline Convergence
- 5G LAN-type services
- User Plane Function (UPF) enh. for control and 5G Service Based Architecture (SBA)

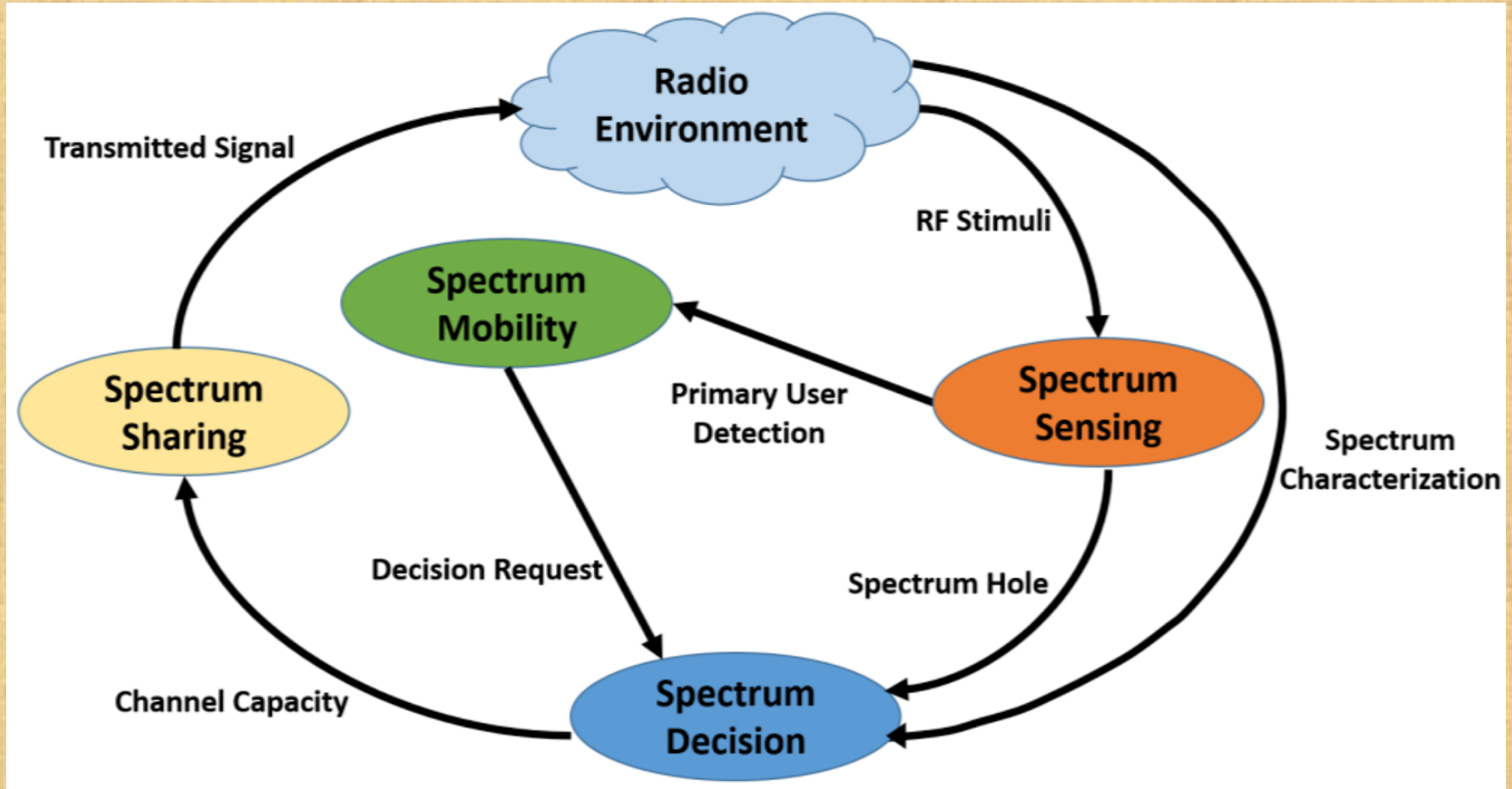
These are some of the Rel-17 headline features, prioritized during the December 2019 Plenaries (TSG#86)

Start of work: January 2020

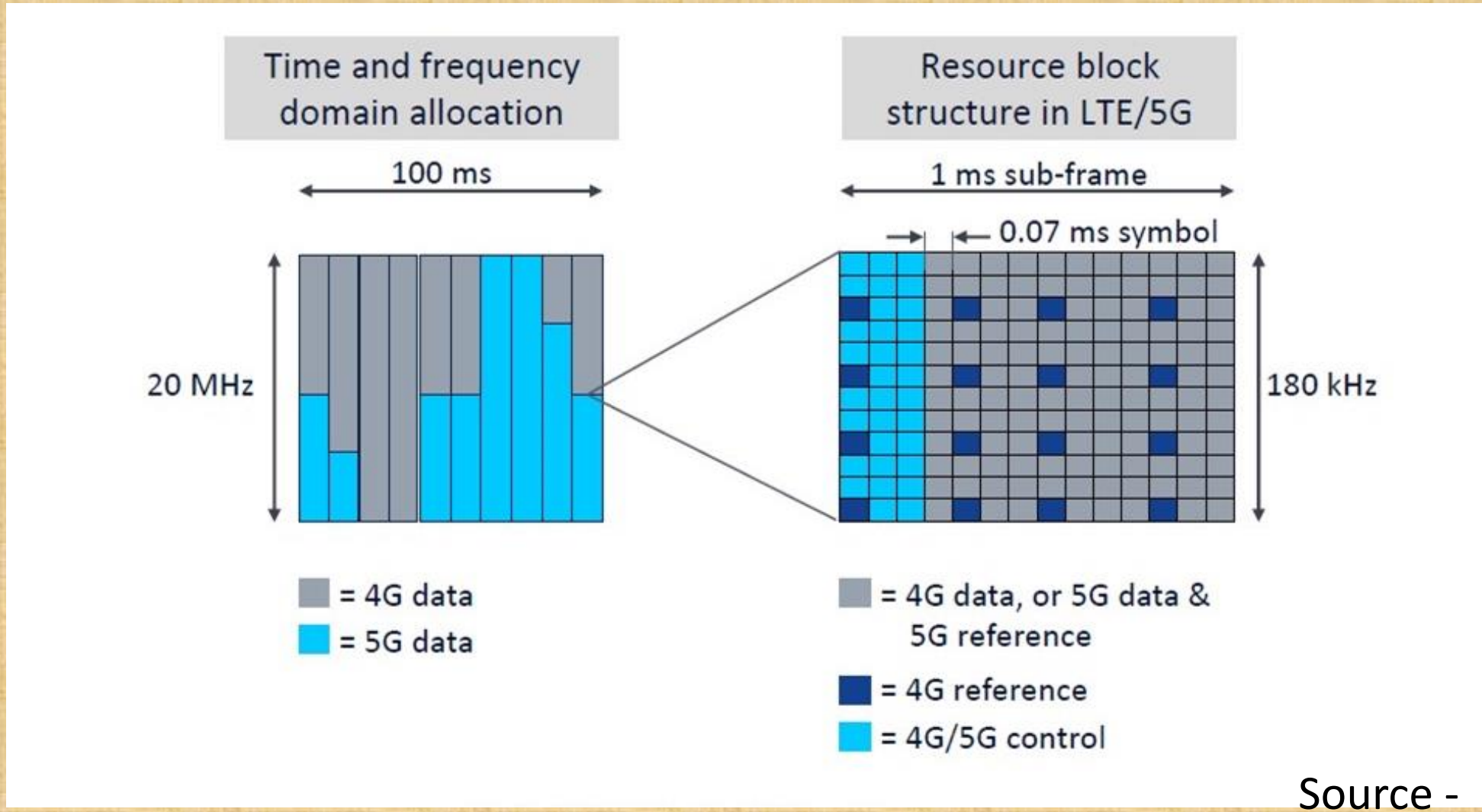
Full details of the content of Rel-17 are in the Work Plan: www.3gpp.org/specifications/work-plan

Cognitive Radio Concept

- **Primary users**
- **Secondary users**
- **Opportunistic Spectrum Access**

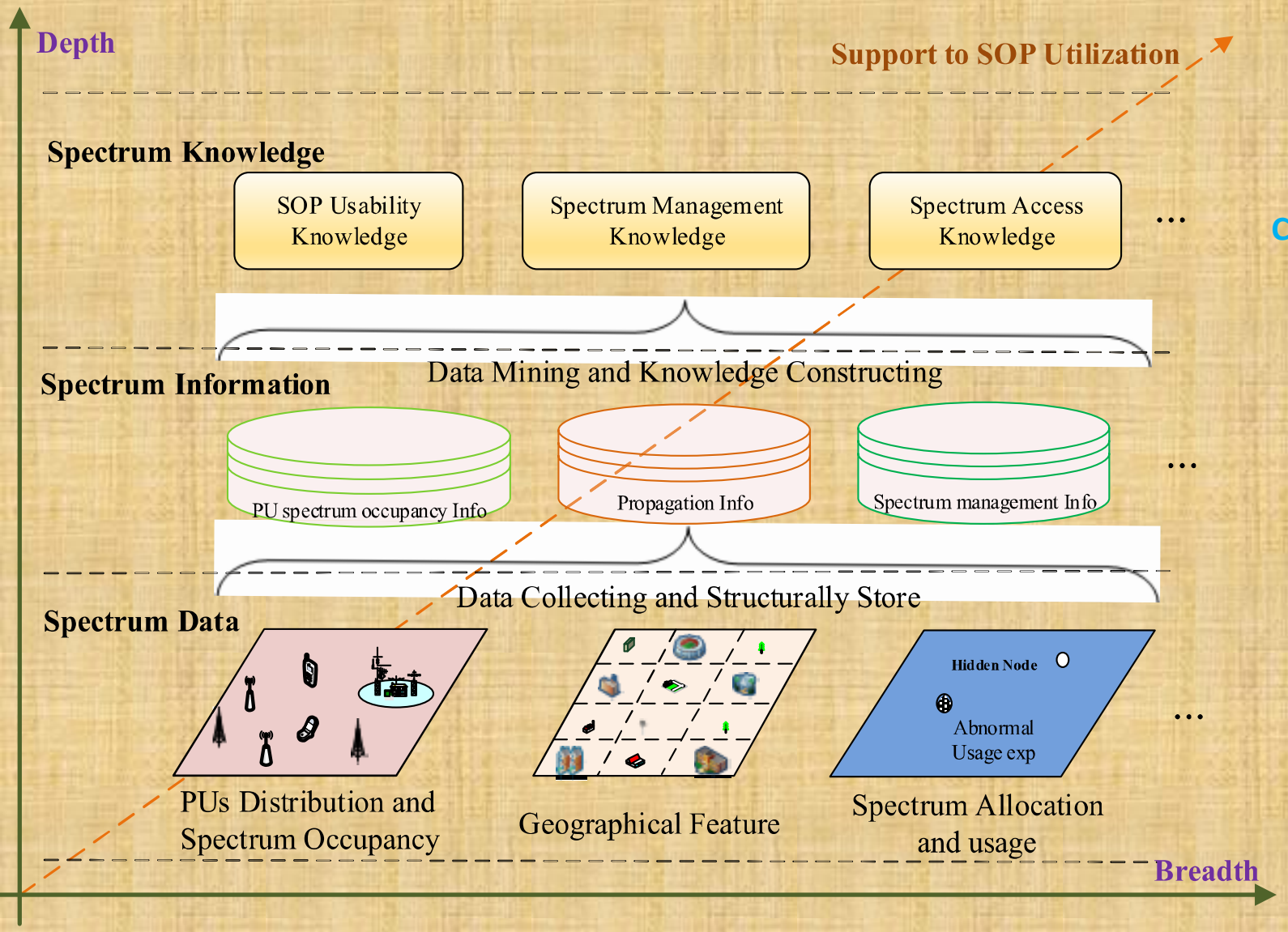


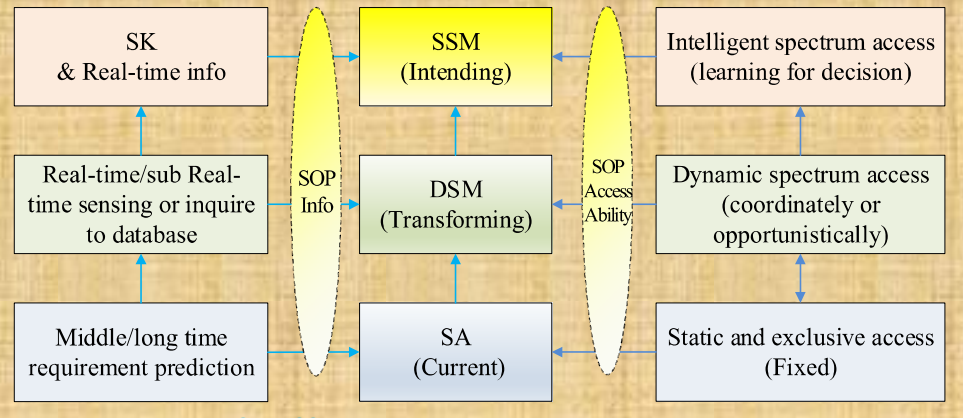
Resource Allocation



Source - blog.3g4g.co.uk

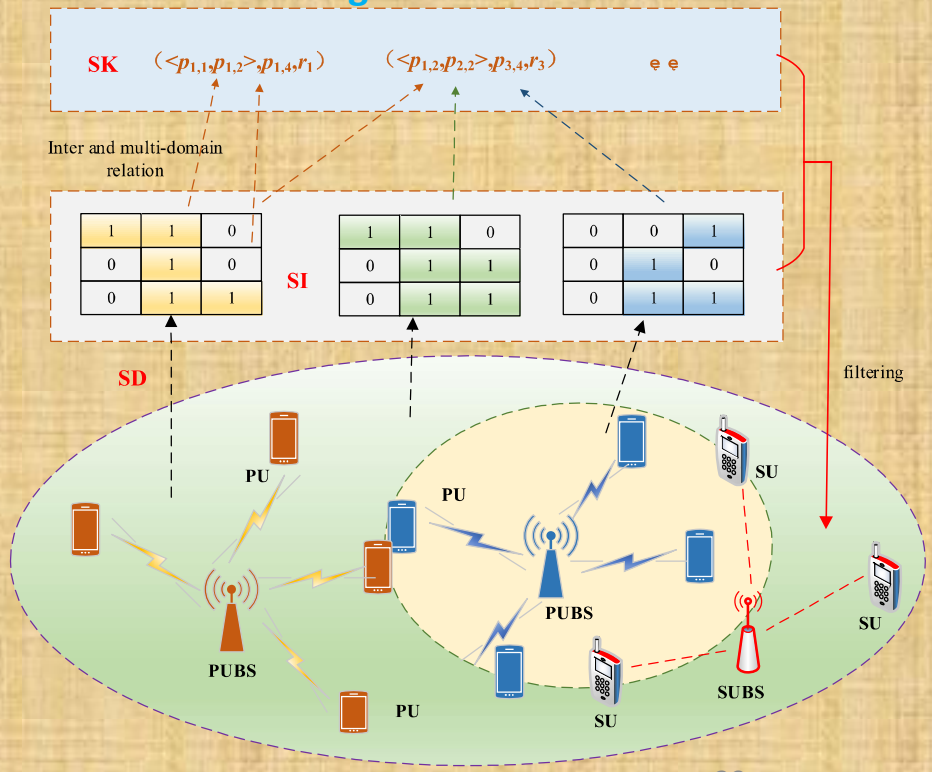
Three-layer SOP information model





Comparison of different spectrum management model

The working framework of SSM



Ref: Y. C. L. W. Jianzhao Zhang, "**Spectrum Knowledge and Real-Time Observing Enabled smart spectrum Management**," IEEE Access, vol. 8, 2020.

5G

- ★ Huge Data Rates
- ★ Multiple Bands
- ★ Multiple Uses

- ★ Mission Critical Applns
- ★ M2M
- ★ V2X
- ★ IoT
- ★ Immersive Technologies

Smart Spectrum Model

- ★ **Data**
- ★ **Information**
- ★ **Knowledge**

- ★ **User Patterns**
- ★ **Decisions for Opportunistic Access**
- ★ **Homogeneous Approach -> UE + Network**

Intelligent Inputs

- **Expected Resource demand**
  - **Location**
  - **Time**
  - **Type of User**
- **Available Slack for immediate Allocation**
- **Spaces for Free Access advertised to UEs**
- **Low latency Mission Critical Bands**
- **Previous Performance in Bands**
- **Quality of Spectrum spaces based upon climatic conditions / locations**
- **Special Conditions during disaster management for mission critical requirements**

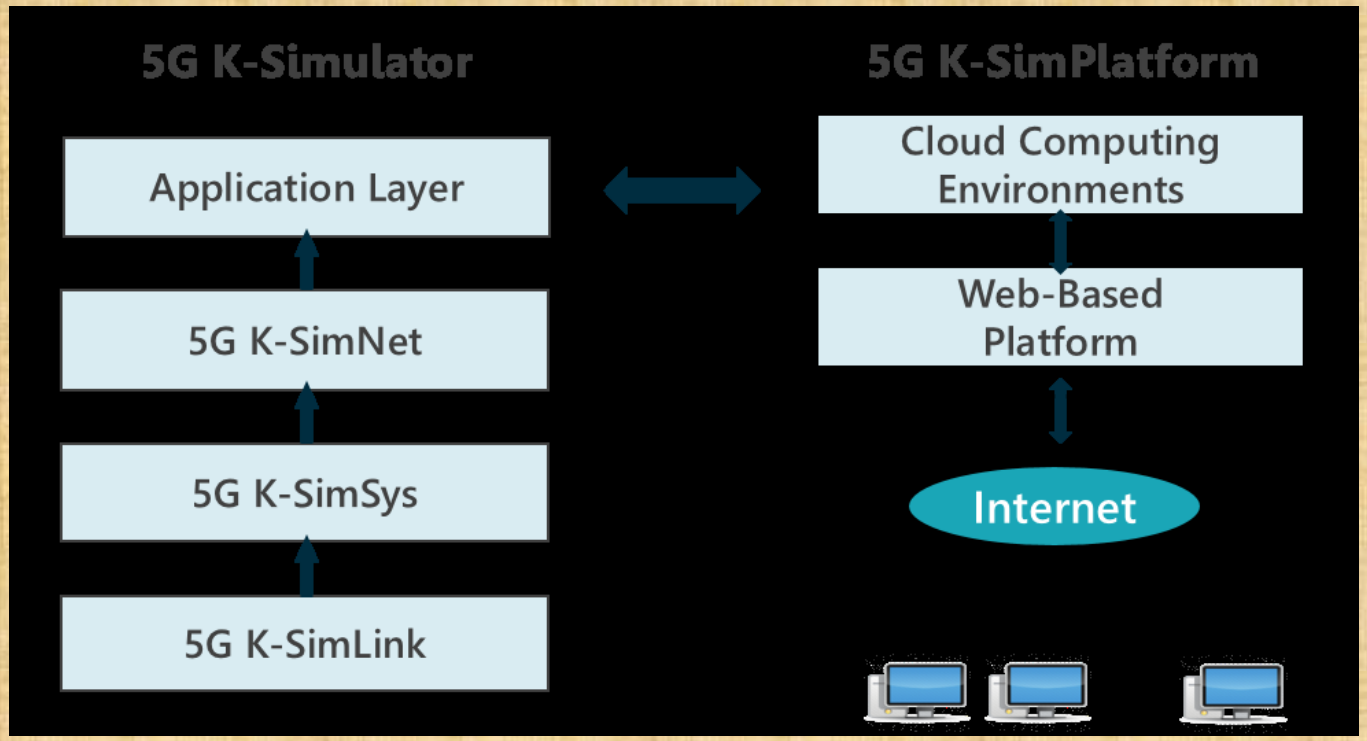
Challenge

- ❑ **Identification of Key Variables for DSA**
- ❑ **Propose a Framework using Key Variables**

- ❑ **Preferably comply with O-RAN**
- ❑ **In Line with ITU-T Y.3174**

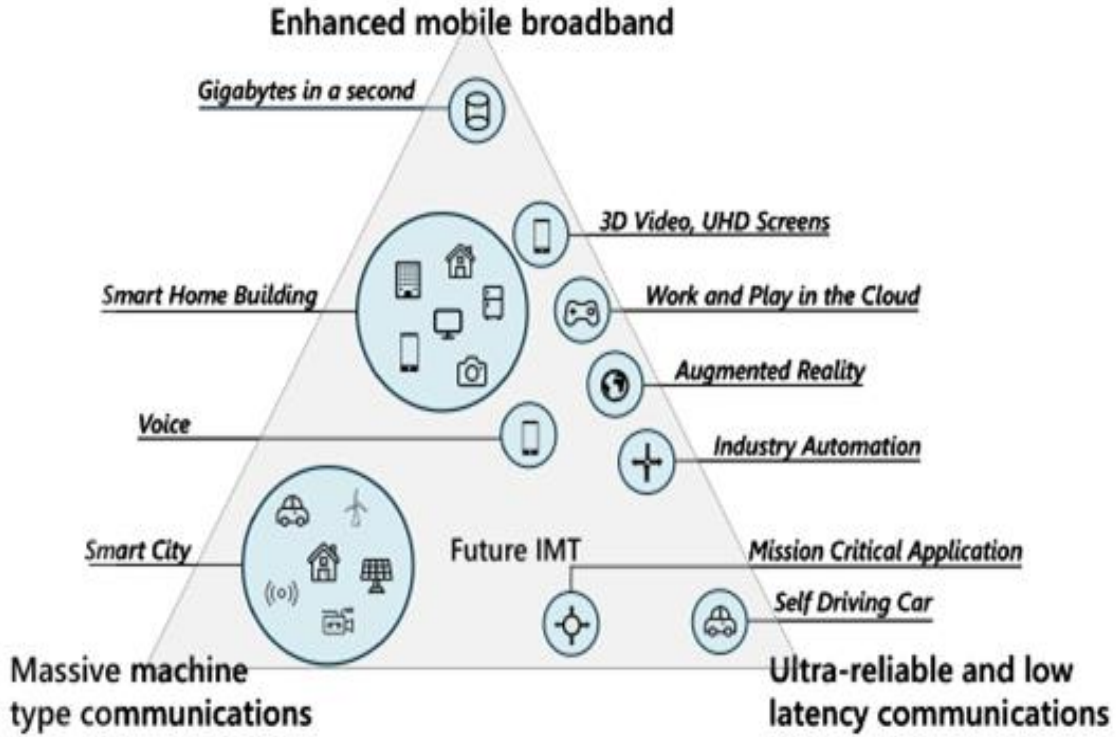
- ★ **SYNTHESISE DATA**
- ★ **LOGICAL APCH**

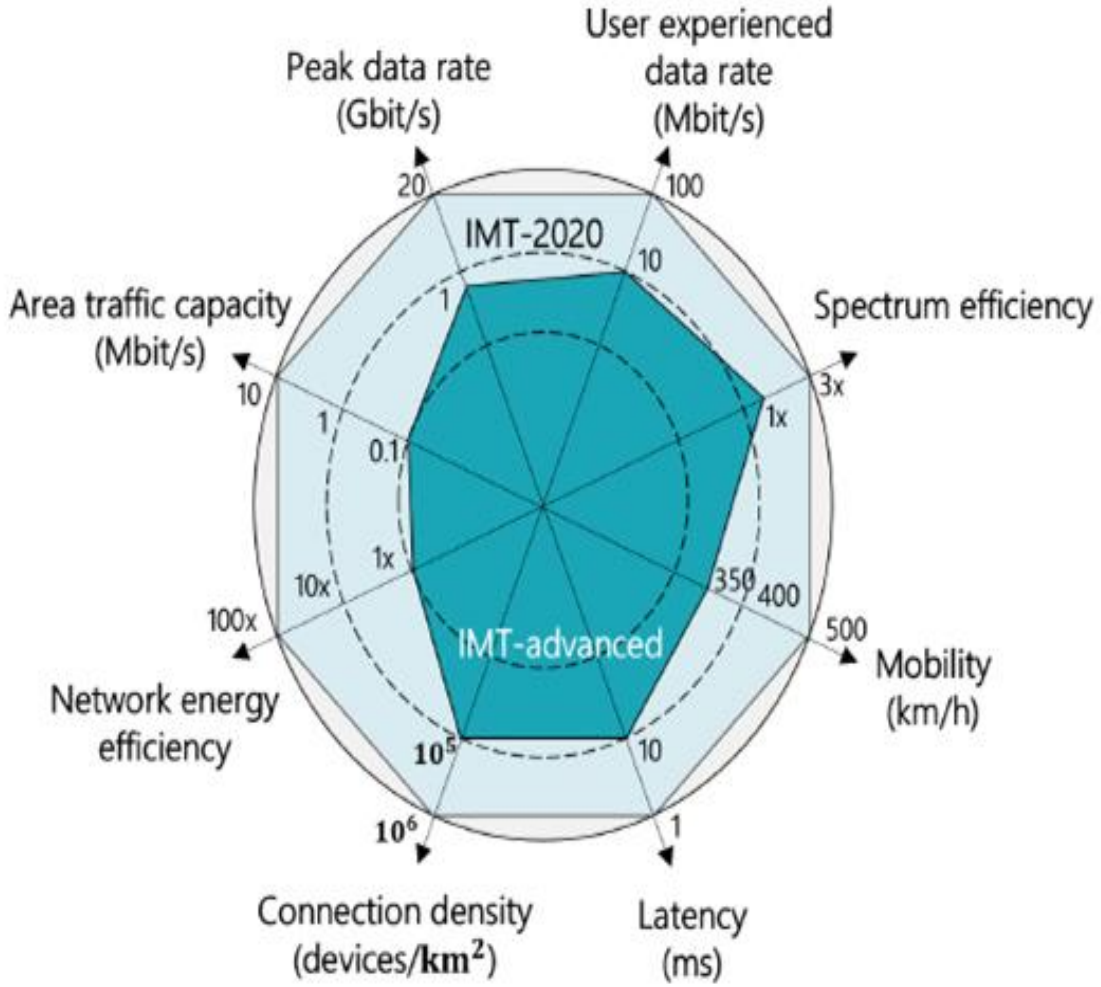
Synthetic Data : Open Source Nw Simulators



5G K-Simulator Platform

Optimise KPIs





Resources

- **Usage of Network Simulators in Machine-Learning-Assisted 5G/6G** Networks Francesc Wilhelmi, Marc Carrascosa, Cristina Cano, Anders Jonsson, Vishnu Ram, and Boris Bellalta , March 2020
- M. W. L.Shang, "**A survey of advanced techniques for spectrum sharing in 5G networks**," IEE wireless communications, vol. 24, pp. 44-51, Oct 2017.
- Y. C. L. W. Jianzhao Zhang, "**Spectrum Knowledge and Real-Time Observing Enabled smart spectrum Management**," IEEE Access, vol. 8, 2020.
- W. L. ME Morocho-Cayamcela, "**Machine Learning for 5G/B5G Mobile and wireless Communications : Potential , Limitations, and Future Directions**," IEEE Access, vol. 7, Sep 2019.

THANK YOU

Machine Learning for Wireless LANs + Japan Challenge Introduction
ITU-ML5G-PS-031, ITU-ML5G-PS-032
29 July 2020

ITUEvents

ITU
AI/ML in 5G
Challenge

Applying machine learning in communication networks

ai5gchallenge@itu.int

Register here
Join us on Slack

Sponsors

Organizer

Federated Learning vs Secure Multiparty computation

- MPC is a cryptographic definition which reveals no intermediate information during the whole computation, all it reveals is the final result.
- In contrast, FL is a machine learning definition that iteratively collects and updates the model, which is revealed in each iteration.
- MPC enjoys a much higher security level, at the price of
  - expensive cryptographic operations, which often results in higher computation and communication cost.
- FL loosen the security requirements, enabling
  - more clear and efficient implementation.

Resource Allocation

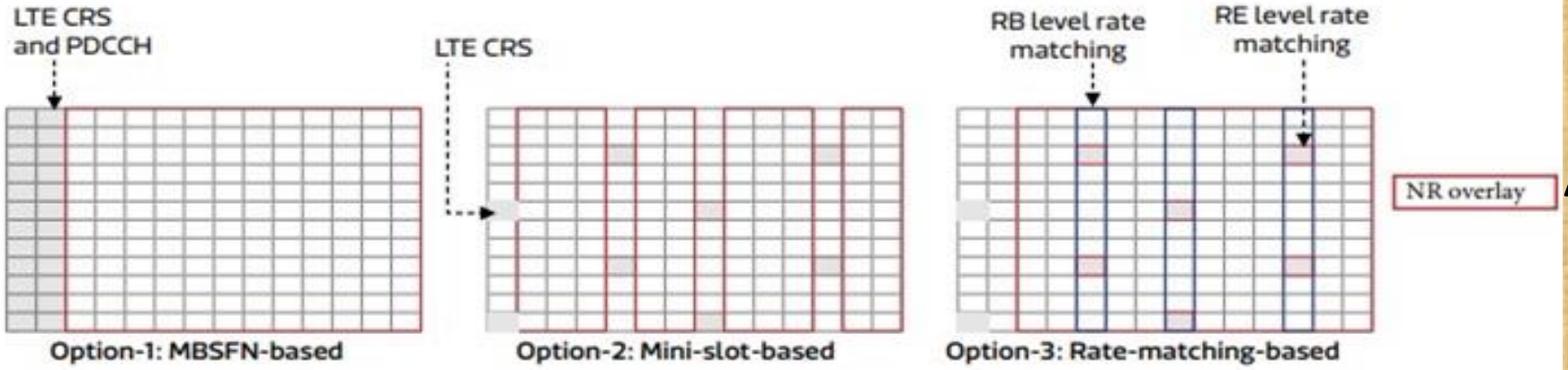
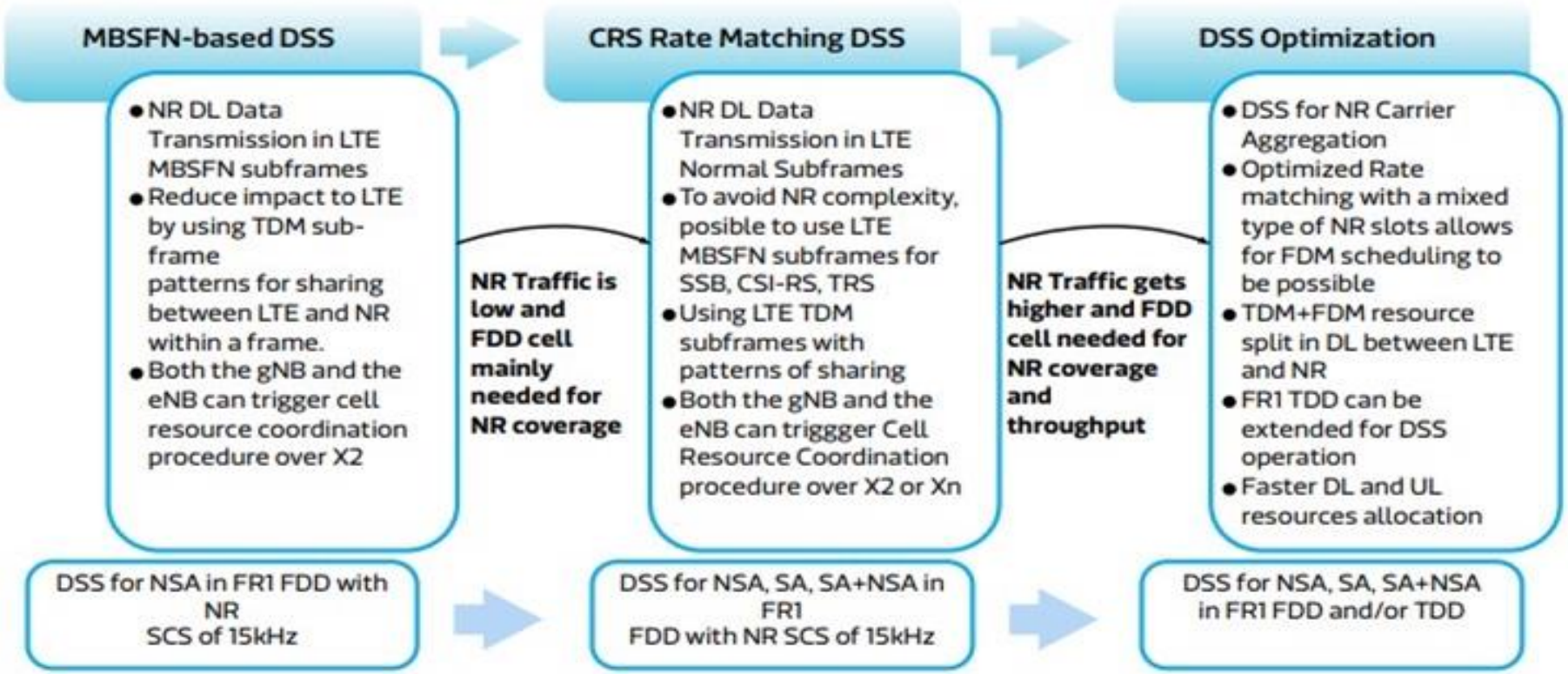


Figure 1. DSS Deployment Options



Source - blog.3g4g.co.uk

5G Core (Nw simulator)