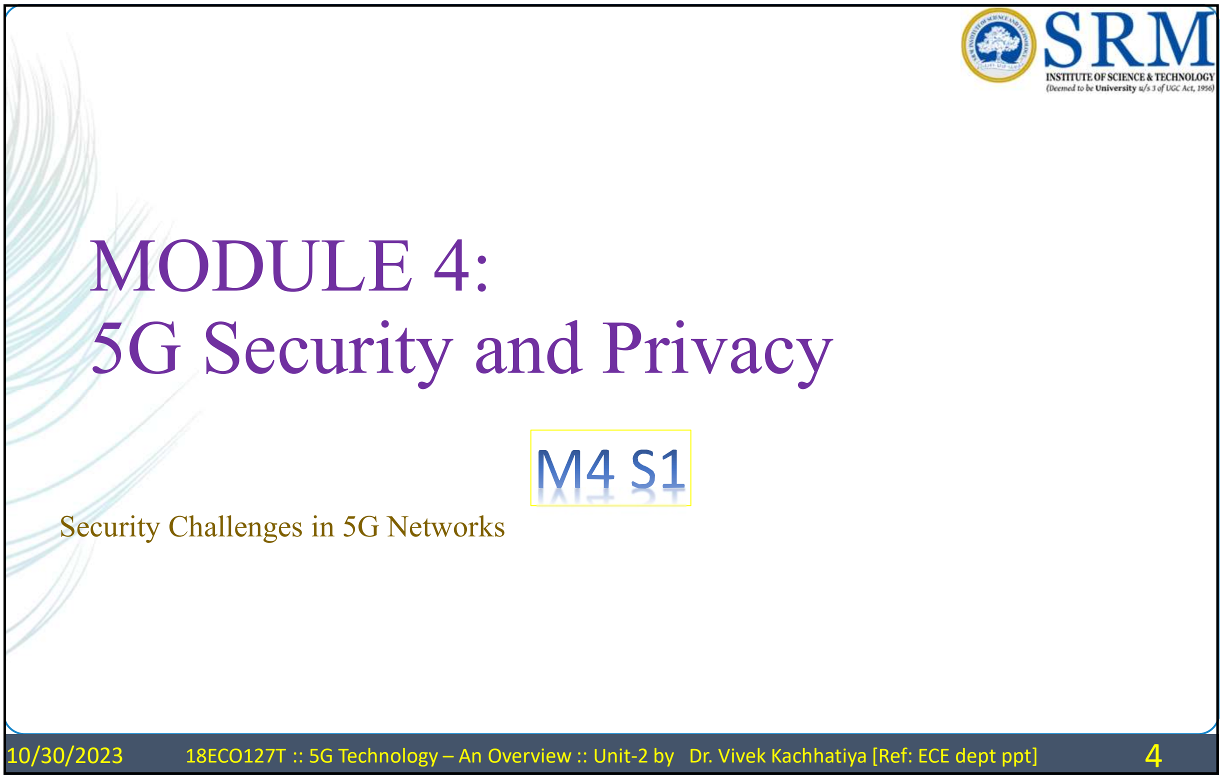
18ECO127T
5G Technology – An Overview

OPEN ELECTIVE (by ECE)
SEM:7

B.TECH

MODULE 4:
5G Security and Privacy

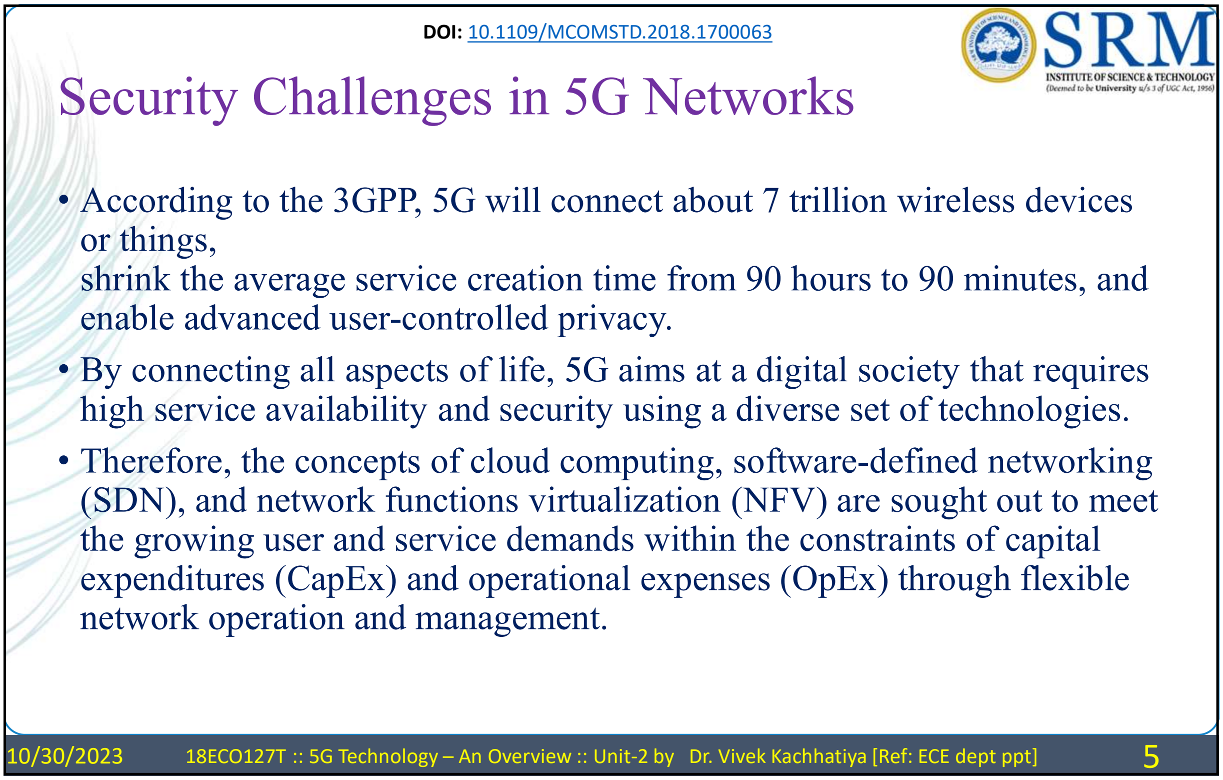
- Security Challenges in 5G Networks
- Authentication and Access Control in 5G
- Encryption in 5G
- Privacy-Preserving Techniques in 5G
- Threats Detection and Mitigation in 5G Networks
- Network Slice Isolation
- Virtualized Infrastructure Security
- Network Function Verification
- Secure Over-the-Air (OTA) Updates



MODULE 4: 5G Security and Privacy

M4 S1

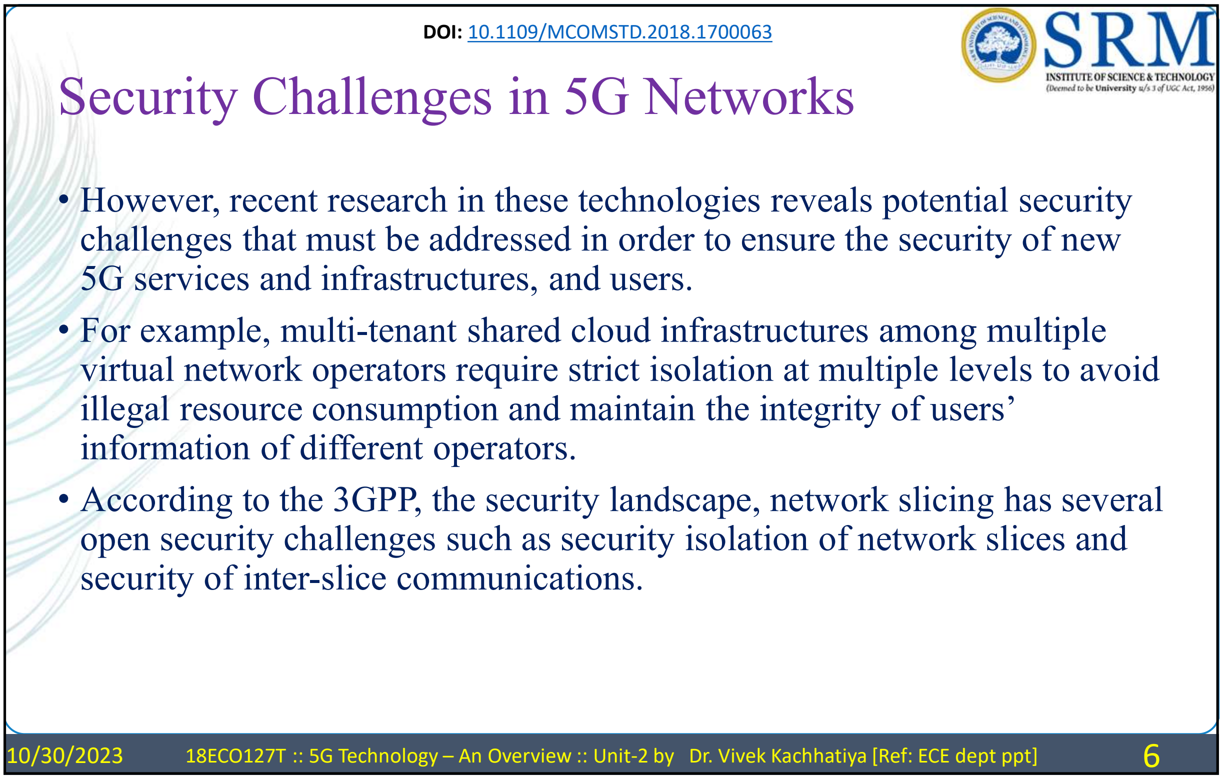
Security Challenges in 5G Networks



DOI: 10.1109/MCOMSTD.2018.1700063

Security Challenges in 5G Networks

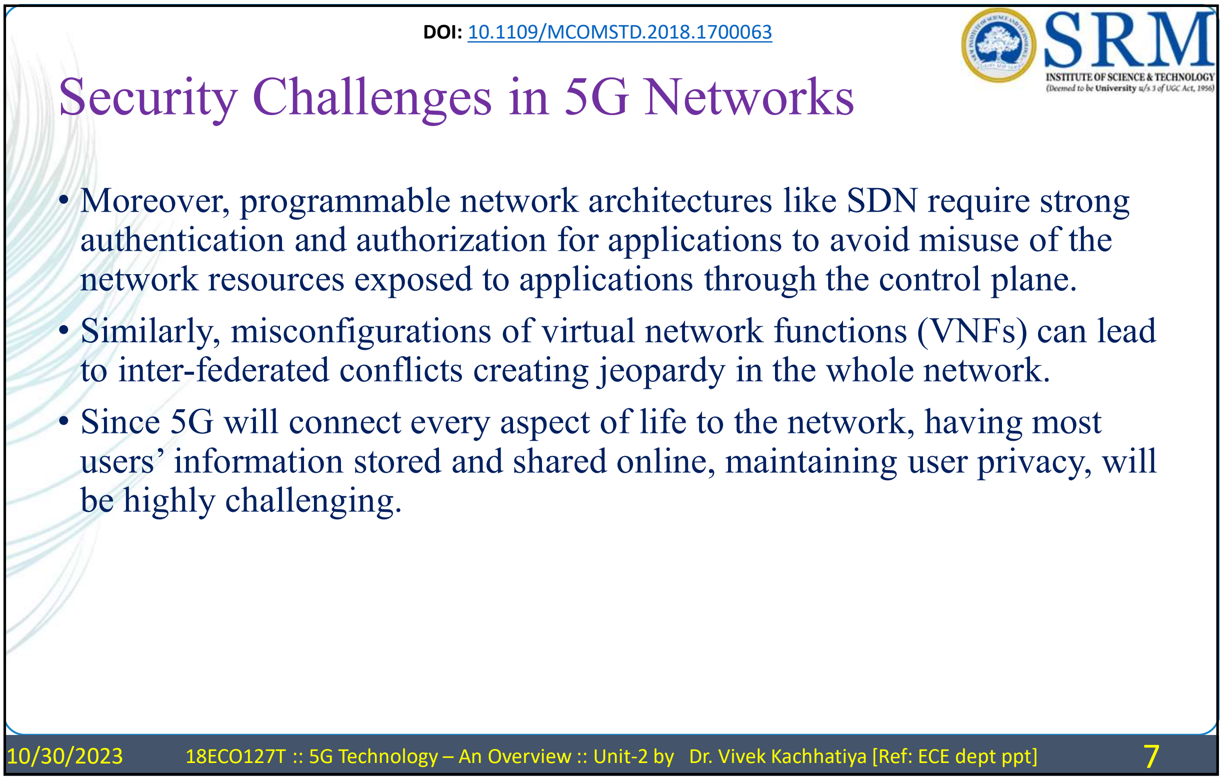
- According to the 3GPP, 5G will connect about 7 trillion wireless devices or things,
  shrink the average service creation time from 90 hours to 90 minutes, and enable advanced user-controlled privacy.
- By connecting all aspects of life, 5G aims at a digital society that requires high service availability and security using a diverse set of technologies.
- Therefore, the concepts of cloud computing, software-defined networking (SDN), and network functions virtualization (NFV) are sought out to meet the growing user and service demands within the constraints of capital expenditures (CapEx) and operational expenses (OpEx) through flexible network operation and management.



DOI: 10.1109/MCOMSTD.2018.1700063

Security Challenges in 5G Networks

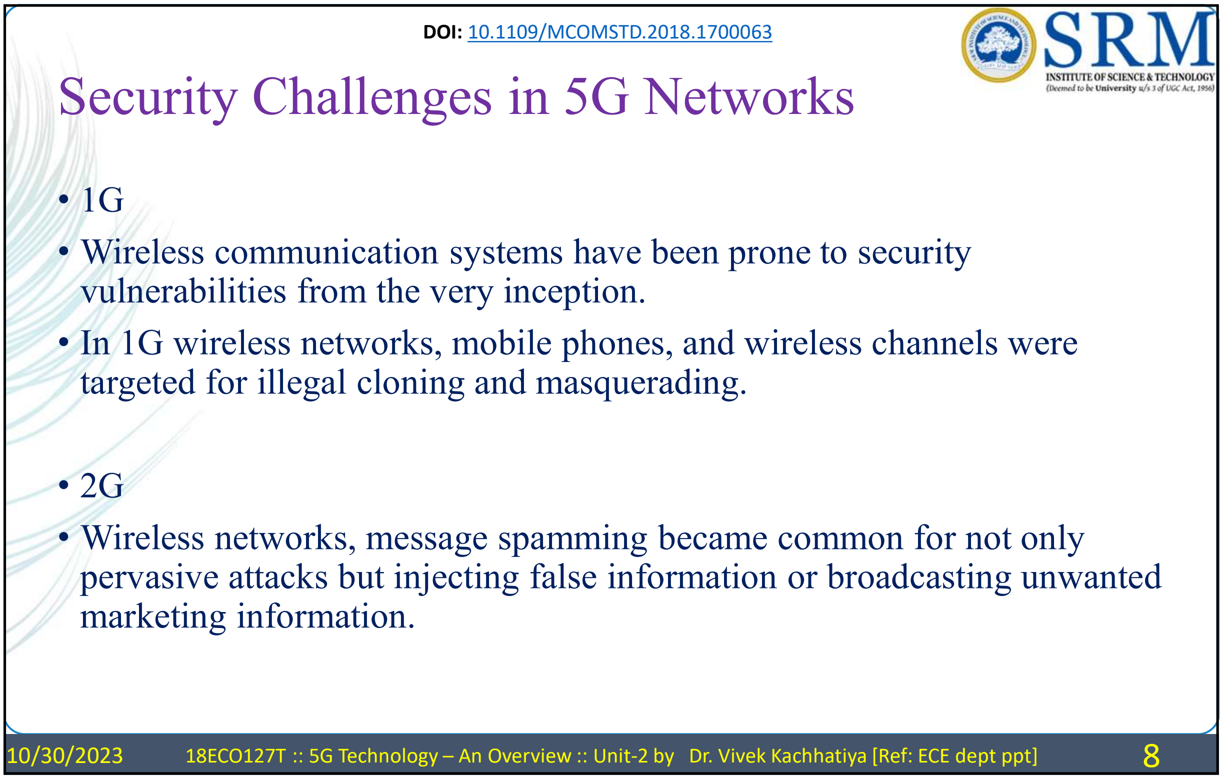
- However, recent research in these technologies reveals potential security challenges that must be addressed in order to ensure the security of new 5G services and infrastructures, and users.
- For example, multi-tenant shared cloud infrastructures among multiple virtual network operators require strict isolation at multiple levels to avoid illegal resource consumption and maintain the integrity of users' information of different operators.
- According to the 3GPP, the security landscape, network slicing has several open security challenges such as security isolation of network slices and security of inter-slice communications.



DOI: 10.1109/MCOMSTD.2018.1700063

Security Challenges in 5G Networks

- Moreover, programmable network architectures like SDN require strong authentication and authorization for applications to avoid misuse of the network resources exposed to applications through the control plane.
- Similarly, misconfigurations of virtual network functions (VNFs) can lead to inter-federated conflicts creating jeopardy in the whole network.
- Since 5G will connect every aspect of life to the network, having most users' information stored and shared online, maintaining user privacy, will be highly challenging.

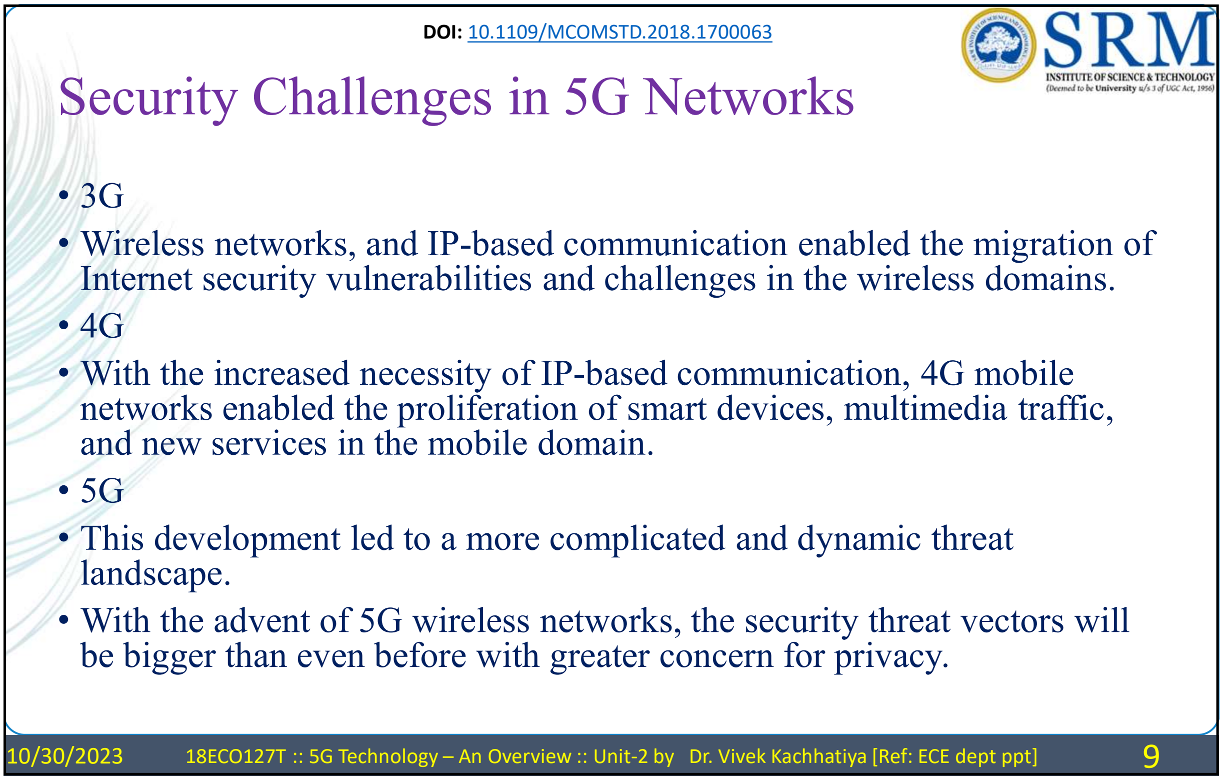


DOI: 10.1109/MCOMSTD.2018.1700063

Security Challenges in 5G Networks

- 1G
- Wireless communication systems have been prone to security vulnerabilities from the very inception.
- In 1G wireless networks, mobile phones, and wireless channels were targeted for illegal cloning and masquerading.

- 2G
- Wireless networks, message spamming became common for not only pervasive attacks but injecting false information or broadcasting unwanted marketing information.



DOI: 10.1109/MCOMSTD.2018.1700063

Security Challenges in 5G Networks

- 3G
- Wireless networks, and IP-based communication enabled the migration of Internet security vulnerabilities and challenges in the wireless domains.
- 4G
- With the increased necessity of IP-based communication, 4G mobile networks enabled the proliferation of smart devices, multimedia traffic, and new services in the mobile domain.
- 5G
- This development led to a more complicated and dynamic threat landscape.
- With the advent of 5G wireless networks, the security threat vectors will be bigger than even before with greater concern for privacy.

DOI: 10.1109/MCOMSTD.2018.1700063

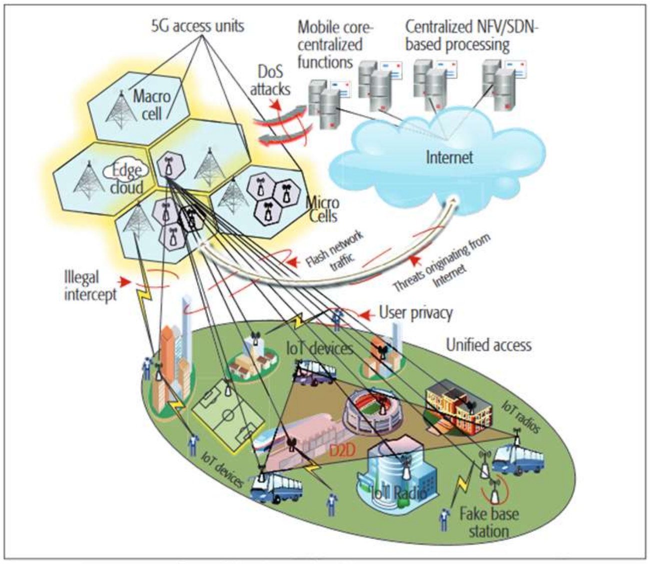
Security Challenges in 5G Networks

- 5G
- Therefore, it is crucial to highlight the security challenges that not only are threatening due to the wireless nature of mobile networks, but also exist in the potential technologies that are highly important for 5G.

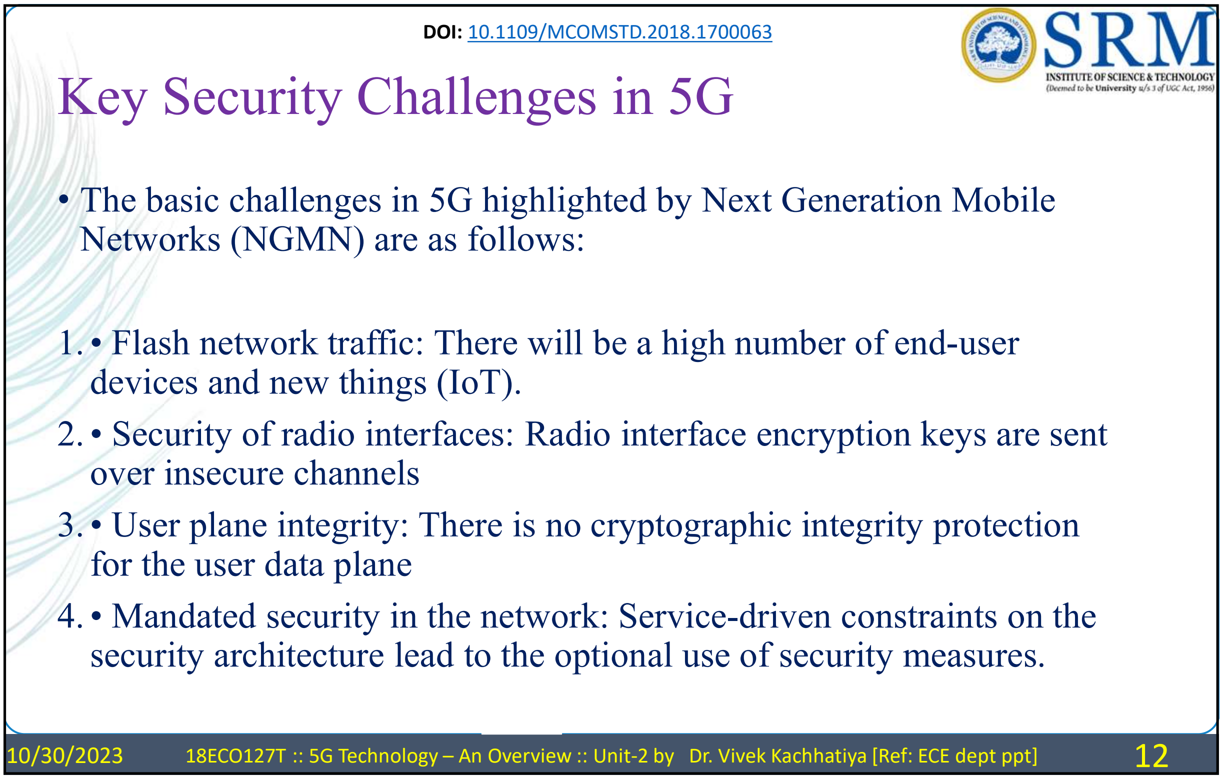
DOI: 10.1109/MCOMSTD.2018.1700063

Key Security Challenges in 5G

- 5G needs robust security architectures and solutions since it will connect every aspect of life to communication networks.
- Therefore, we investigate and highlight the important security and privacy challenges in 5G networks (depicted in Fig) and overview the potential solutions that could lead to secure 5G systems



. 5G network and the threat landscape.



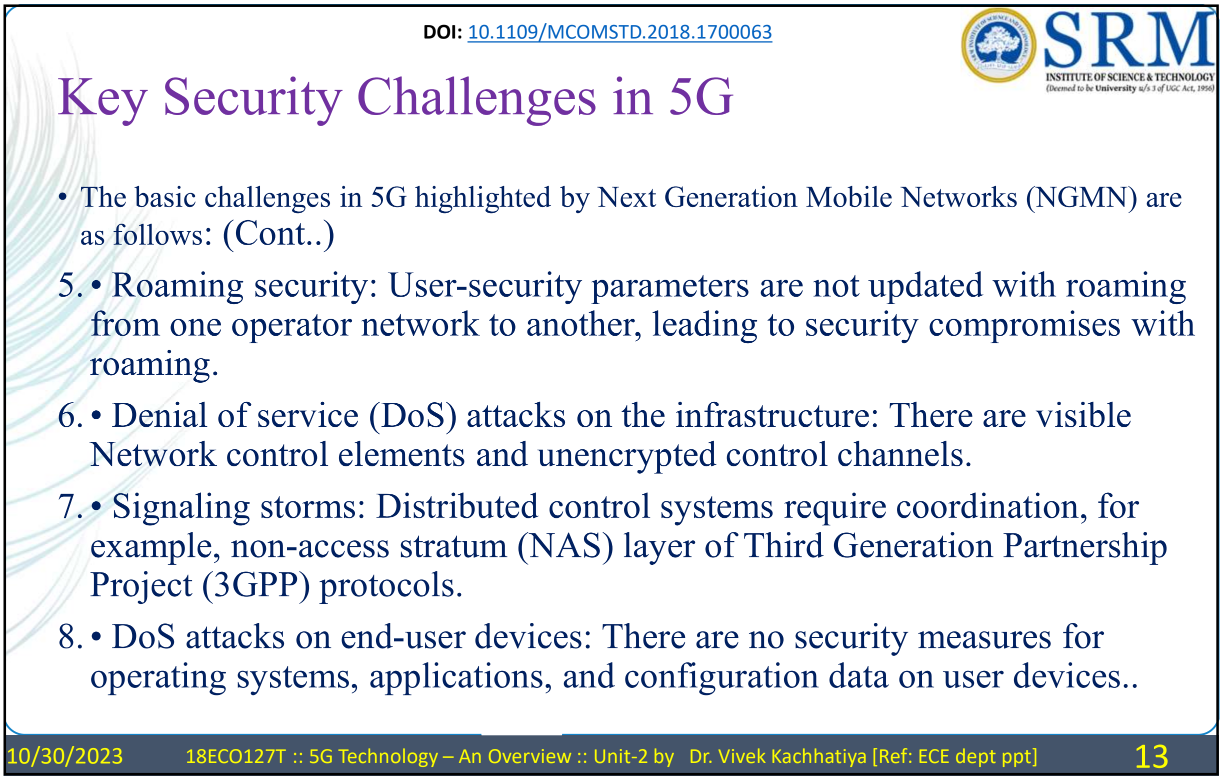
DOI: 10.1109/MCOMSTD.2018.1700063

SRM INSTITUTE OF SCIENCE & TECHNOLOGY (Deemed to be University u/s 3 of UGC Act, 1956)

Key Security Challenges in 5G

- The basic challenges in 5G highlighted by Next Generation Mobile Networks (NGMN) are as follows:

1. • Flash network traffic: There will be a high number of end-user devices and new things (IoT).
2. • Security of radio interfaces: Radio interface encryption keys are sent over insecure channels
3. • User plane integrity: There is no cryptographic integrity protection for the user data plane
4. • Mandated security in the network: Service-driven constraints on the security architecture lead to the optional use of security measures.



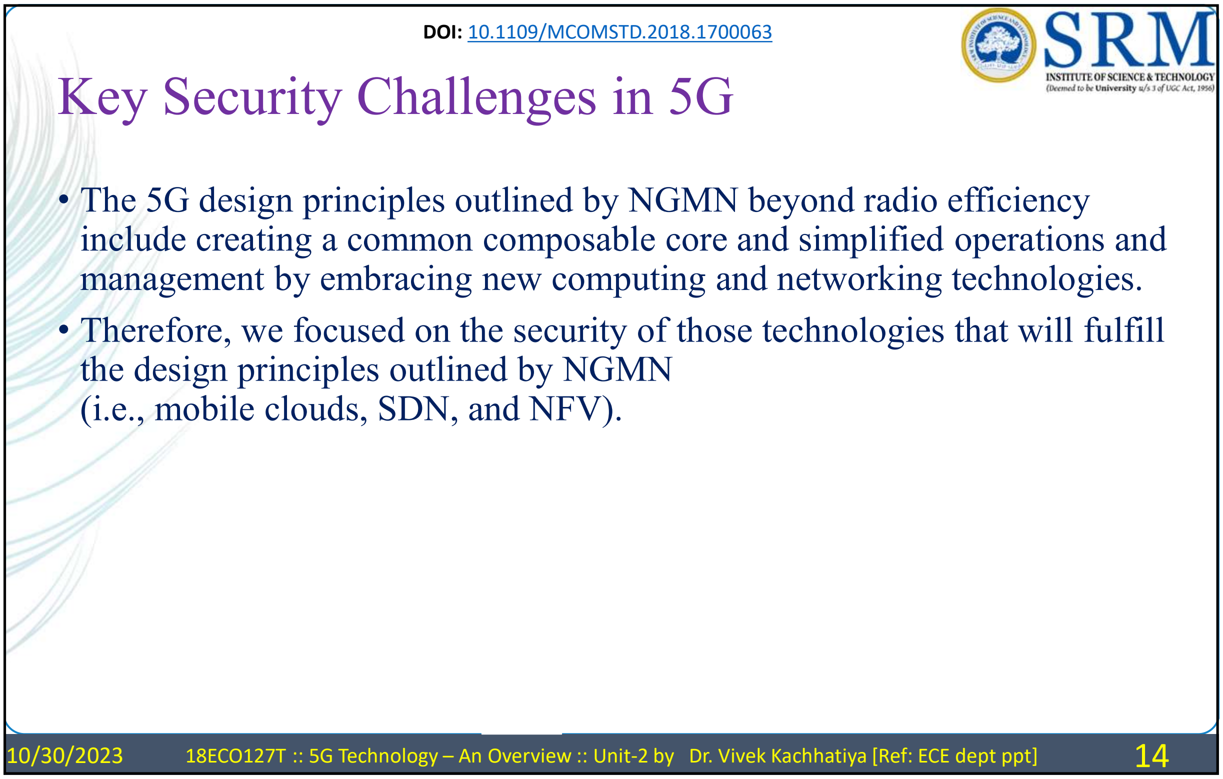
DOI: 10.1109/MCOMSTD.2018.1700063

SRM INSTITUTE OF SCIENCE & TECHNOLOGY (Deemed to be University u/s 3 of UGC Act, 1956)

Key Security Challenges in 5G

- The basic challenges in 5G highlighted by Next Generation Mobile Networks (NGMN) are as follows: (Cont..)

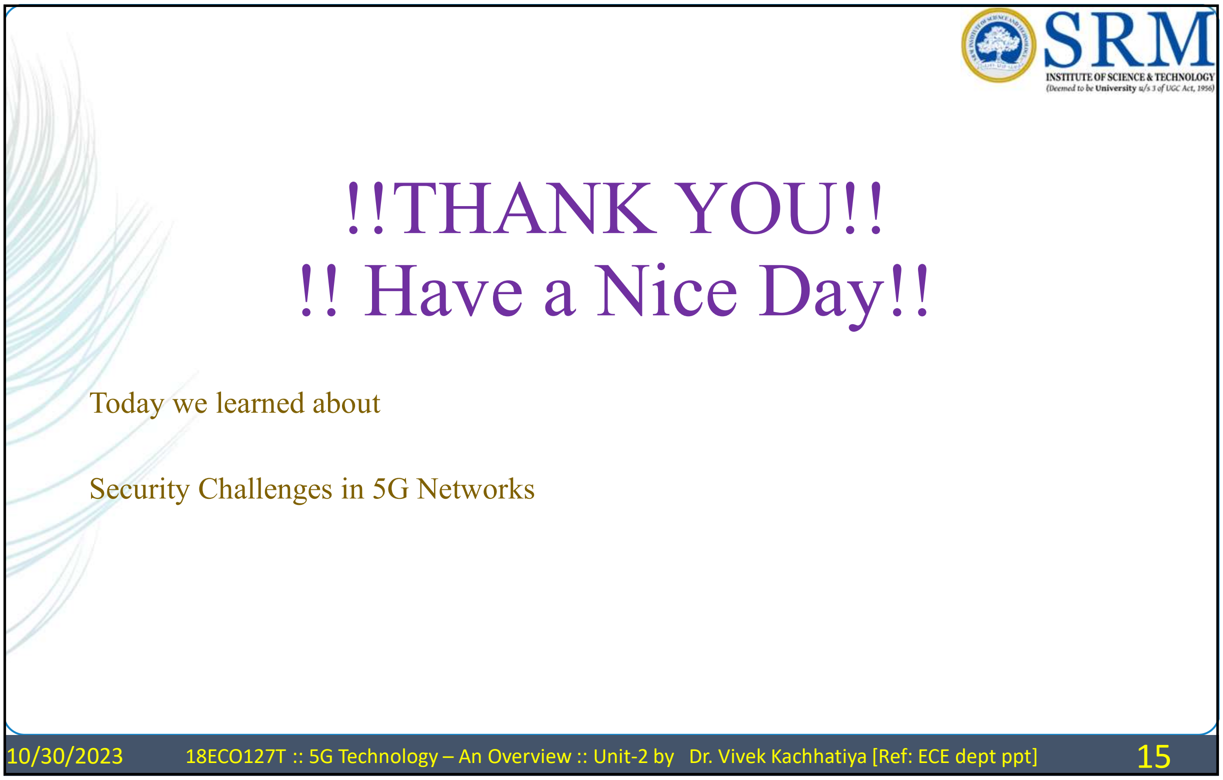
5. • Roaming security: User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming.
6. • Denial of service (DoS) attacks on the infrastructure: There are visible Network control elements and unencrypted control channels.
7. • Signaling storms: Distributed control systems require coordination, for example, non-access stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.
8. • DoS attacks on end-user devices: There are no security measures for operating systems, applications, and configuration data on user devices..



DOI: 10.1109/MCOMSTD.2018.1700063

Key Security Challenges in 5G

- The 5G design principles outlined by NGMN beyond radio efficiency include creating a common composable core and simplified operations and management by embracing new computing and networking technologies.
- Therefore, we focused on the security of those technologies that will fulfill the design principles outlined by NGMN
(i.e., mobile clouds, SDN, and NFV).



!!THANK YOU!!
!! Have a Nice Day!!

Today we learned about

Security Challenges in 5G Networks

MODULE 4:
5G Security and Privacy

M4 S2

Authentication and Access Control in 5G

Encryption in 5G

https://doi.org/10.1016/j.future.2020.02.014.

Authentication and Access Control in 5G

- The fifth generation of mobile networks, 5G, is expected to support a set of many requirements and use cases such as handling connectivity for a massive number of IoT (Internet of Things) devices.
- Authenticating IoT devices and controlling their access to the network plays a vital role in the security of these devices and of the whole cellular system.
- In current cellular networks, as well as in 3GPP specifications release 16 on 5G, the AAC (Authentication and Access Control) of IoT devices is done in the same manner as the AAC of MBB (Mobile Broadband) UE (User Equipment).
- Considering the expected growth of IoT devices, this will likely induce a very high load on the connectivity provider’s CN (Core Network) and cause network failures.

https://doi.org/10.1016/j.future.2020.02.014.

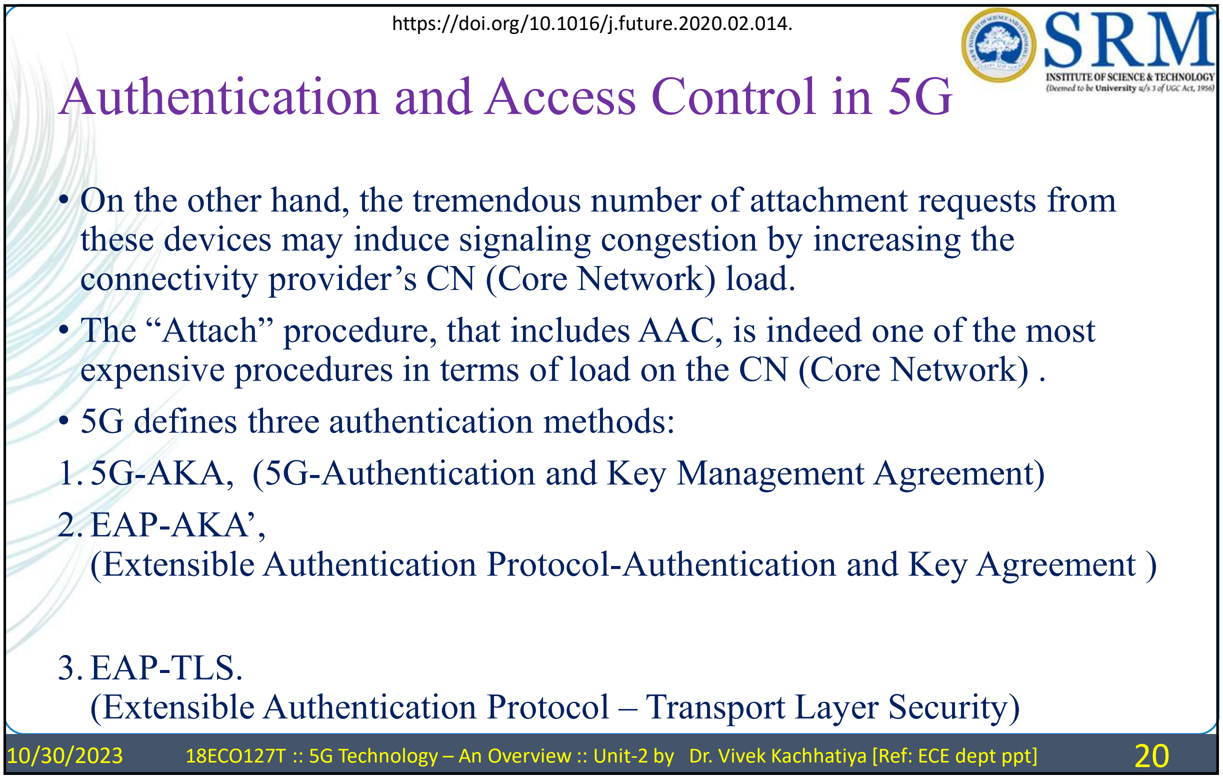
Authentication and Access Control in 5G

- Along with mobility, security is one of the most important aspects of cellular systems.
- AAC (Authentication and access control) plays a vital role in ensuring the expected security level.
- In 3G and 4G, authentication and access control of subscribers are done through AKA (authentication and key agreement) protocols.
- These protocols (UMTS-AKA protocol in 3G and EPS-AKA in 4G) are based on the unique identities of subscribers and symmetric cryptographic algorithms

https://doi.org/10.1016/j.future.2020.02.014.

Authentication and Access Control in 5G

- The system subscribers’ identities and the secret keys (that are used in symmetric cryptographic algorithms) are provisioned in secured elements (e.g., SIM cards or embedded SIM) and stored in cellular system’s database as well.
- Executing these AKA protocols to establish a secure connection with the cellular system is mandatory for each UE (composed of a mobile device and a secured element) to obtain its cellular connectivity.
- However, these well-established principles may prevent cellular systems from supporting the connectivity of a massive number of devices, in particular when considering the context of the IoT — where a high growth rate of connected devices is anticipated.
- On one hand, most devices are constrained in terms of energy supply and computational capacities preventing them from running complex security protocols like EPS-AKA.

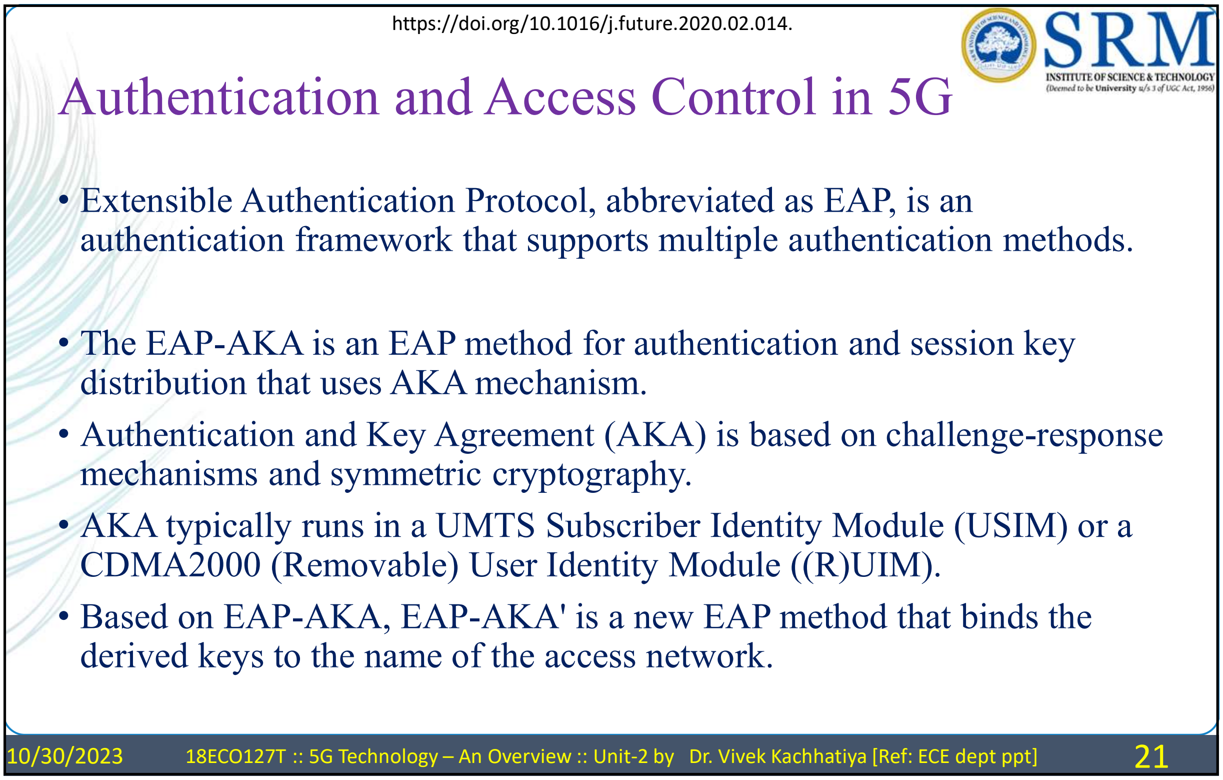


https://doi.org/10.1016/j.future.2020.02.014.

Authentication and Access Control in 5G

- On the other hand, the tremendous number of attachment requests from these devices may induce signaling congestion by increasing the connectivity provider’s CN (Core Network) load.
- The “Attach” procedure, that includes AAC, is indeed one of the most expensive procedures in terms of load on the CN (Core Network) .
- 5G defines three authentication methods:

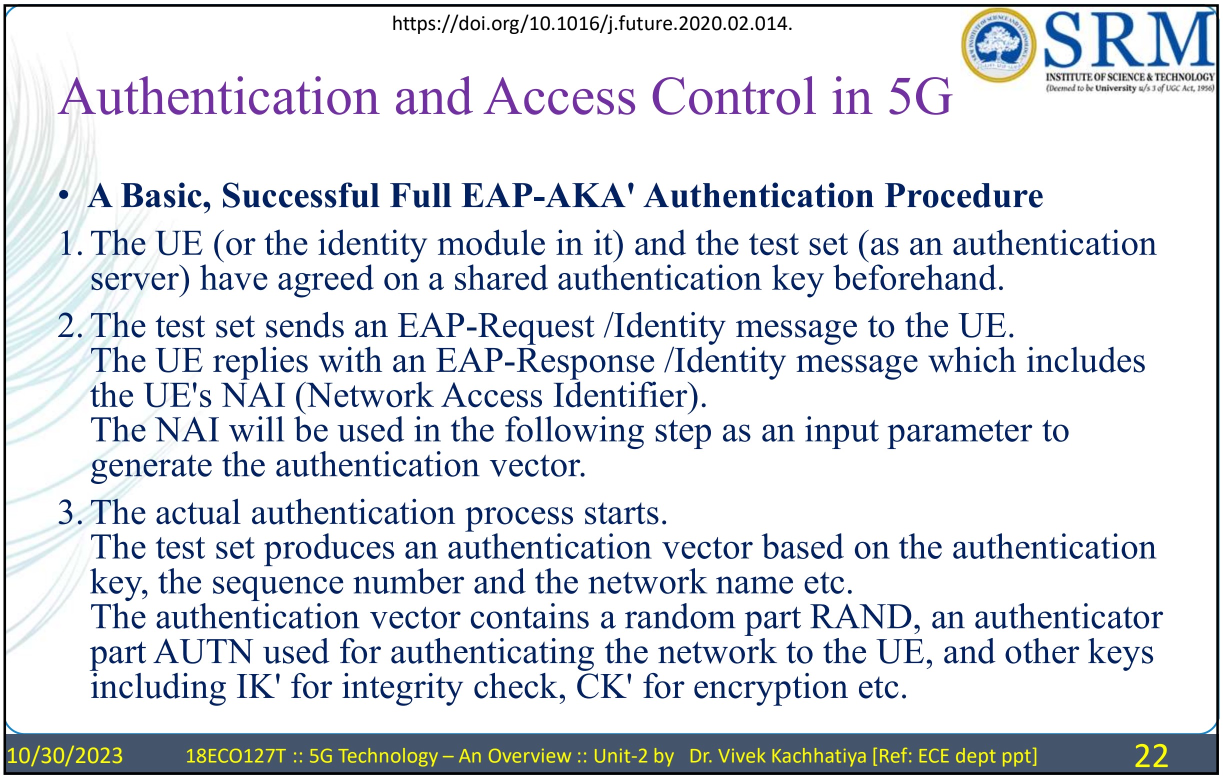
1. 5G-AKA, (5G-Authentication and Key Management Agreement)
2. EAP-AKA’,
   (Extensible Authentication Protocol-Authentication and Key Agreement)
3. EAP-TLS.
   (Extensible Authentication Protocol – Transport Layer Security)



https://doi.org/10.1016/j.future.2020.02.014.

Authentication and Access Control in 5G

- Extensible Authentication Protocol, abbreviated as EAP, is an authentication framework that supports multiple authentication methods.
- The EAP-AKA is an EAP method for authentication and session key distribution that uses AKA mechanism.
- Authentication and Key Agreement (AKA) is based on challenge-response mechanisms and symmetric cryptography.
- AKA typically runs in a UMTS Subscriber Identity Module (USIM) or a CDMA2000 (Removable) User Identity Module ((R)UIM).
- Based on EAP-AKA, EAP-AKA' is a new EAP method that binds the derived keys to the name of the access network.

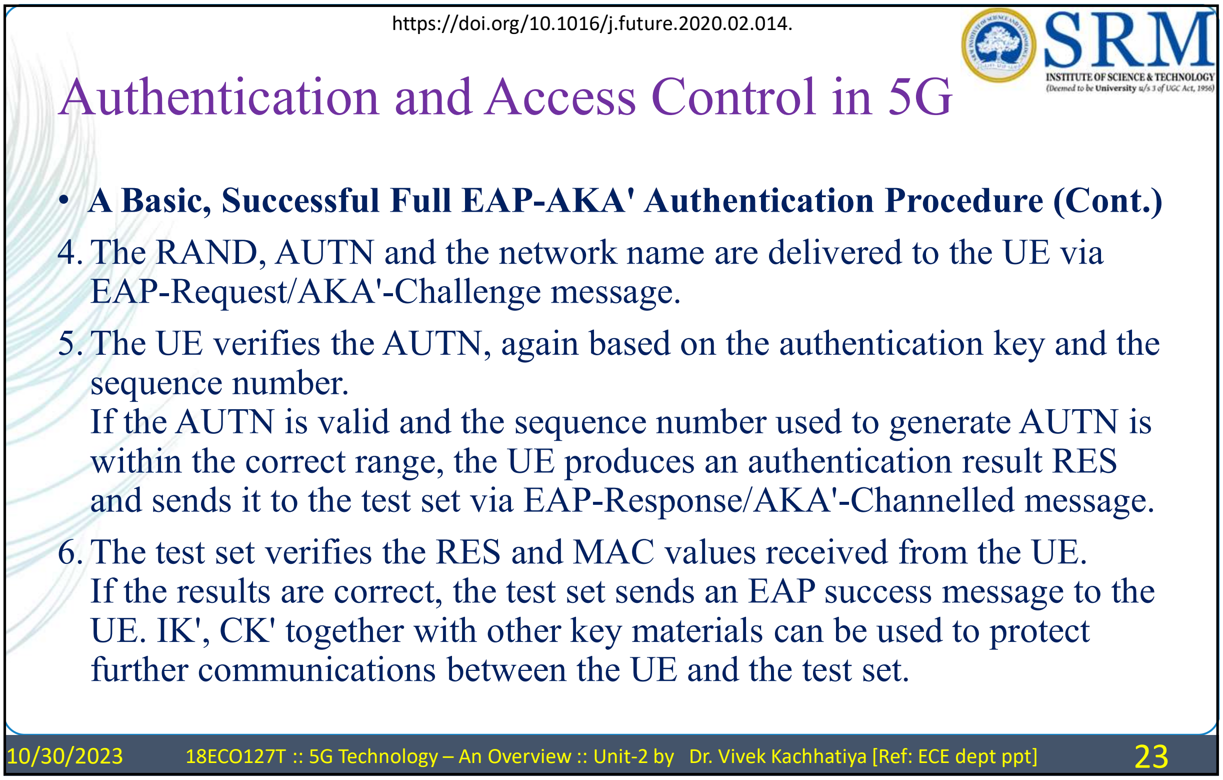


https://doi.org/10.1016/j.future.2020.02.014.

Authentication and Access Control in 5G

- **A Basic, Successful Full EAP-AKA' Authentication Procedure**

1. The UE (or the identity module in it) and the test set (as an authentication server) have agreed on a shared authentication key beforehand.
2. The test set sends an EAP-Request /Identity message to the UE.
   The UE replies with an EAP-Response /Identity message which includes the UE's NAI (Network Access Identifier).
   The NAI will be used in the following step as an input parameter to generate the authentication vector.
3. The actual authentication process starts.
   The test set produces an authentication vector based on the authentication key, the sequence number and the network name etc.
   The authentication vector contains a random part RAND, an authenticator part AUTN used for authenticating the network to the UE, and other keys including IK' for integrity check, CK' for encryption etc.



https://doi.org/10.1016/j.future.2020.02.014.

Authentication and Access Control in 5G

- **A Basic, Successful Full EAP-AKA' Authentication Procedure (Cont.)**

4. The RAND, AUTN and the network name are delivered to the UE via EAP-Request/AKA'-Challenge message.
5. The UE verifies the AUTN, again based on the authentication key and the sequence number.
   If the AUTN is valid and the sequence number used to generate AUTN is within the correct range, the UE produces an authentication result RES and sends it to the test set via EAP-Response/AKA'-Channelled message.
6. The test set verifies the RES and MAC values received from the UE.
   If the results are correct, the test set sends an EAP success message to the UE. IK', CK' together with other key materials can be used to protect further communications between the UE and the test set.

Encryption in 5G

- The security of the radio interface keys is still a challenge, as it needs secure exchange of keys encrypted like the Host Identity Protocol (HIP)-based schemes.
- The same **end-to-end encryption protocol** can be used for user plane integrity.
- Roaming security and network-wide mandated security policies can be achieved using centralized systems that have a global visibility of the users' activities and network traffic behavior (e.g., SDN).
- Signaling storms will be more challenging due to the excessive connectivity of UEs, small base stations, and high user mobility.
- The cloud radio access network (C-RAN) and edge computing are the potential problem solvers for these challenges, but the design of these technologies must consider the increase in signaling traffic as an important aspect of the future networks as described by NGMN.

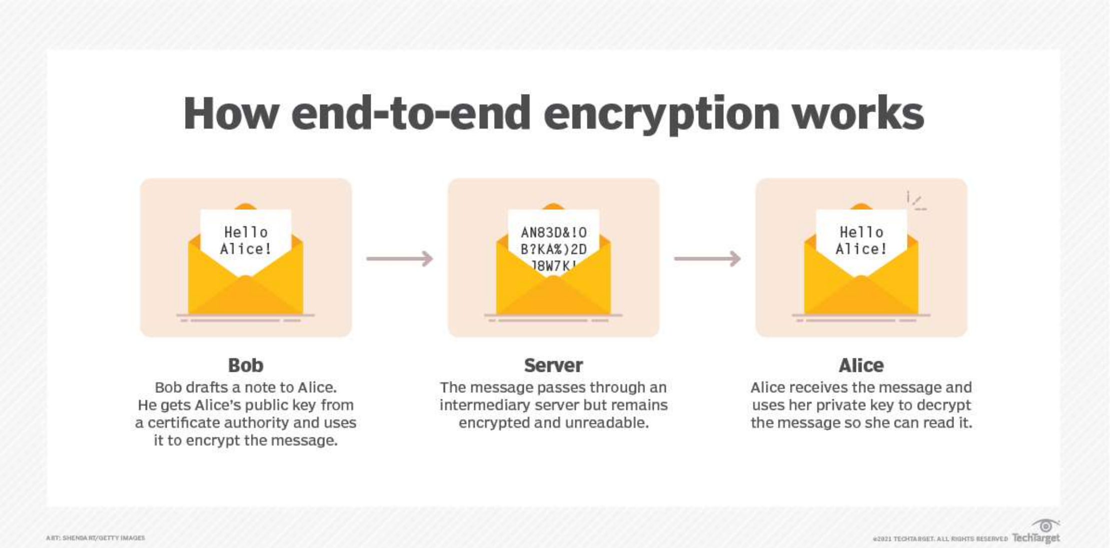
Encryption in 5G

- **What is end-to-end encryption?**
- End-to-end encryption (E2EE) is a method of secure communication that prevents third parties from accessing data while it's transferred from one end system or device to another.
- In E2EE, the data is encrypted on the sender's system or device, and only the intended recipient can decrypt it.
  As it travels to its destination, the message cannot be read or tampered with by an internet service provider (ISP), application service provider, hacker or any other entity or service.

Encryption in 5G

- **How does end-to-end encryption work?**
- The cryptographic keys used to encrypt and decrypt the messages are stored on the endpoints. This approach uses public key encryption.
- Public key, or asymmetric, encryption uses a public key that can be shared with others and a private key.
- Once shared, others can use the public key to encrypt a message and send it to the owner of the public key.
- The message can only be decrypted using the corresponding private key, also called the decryption key.

Encryption in 5G



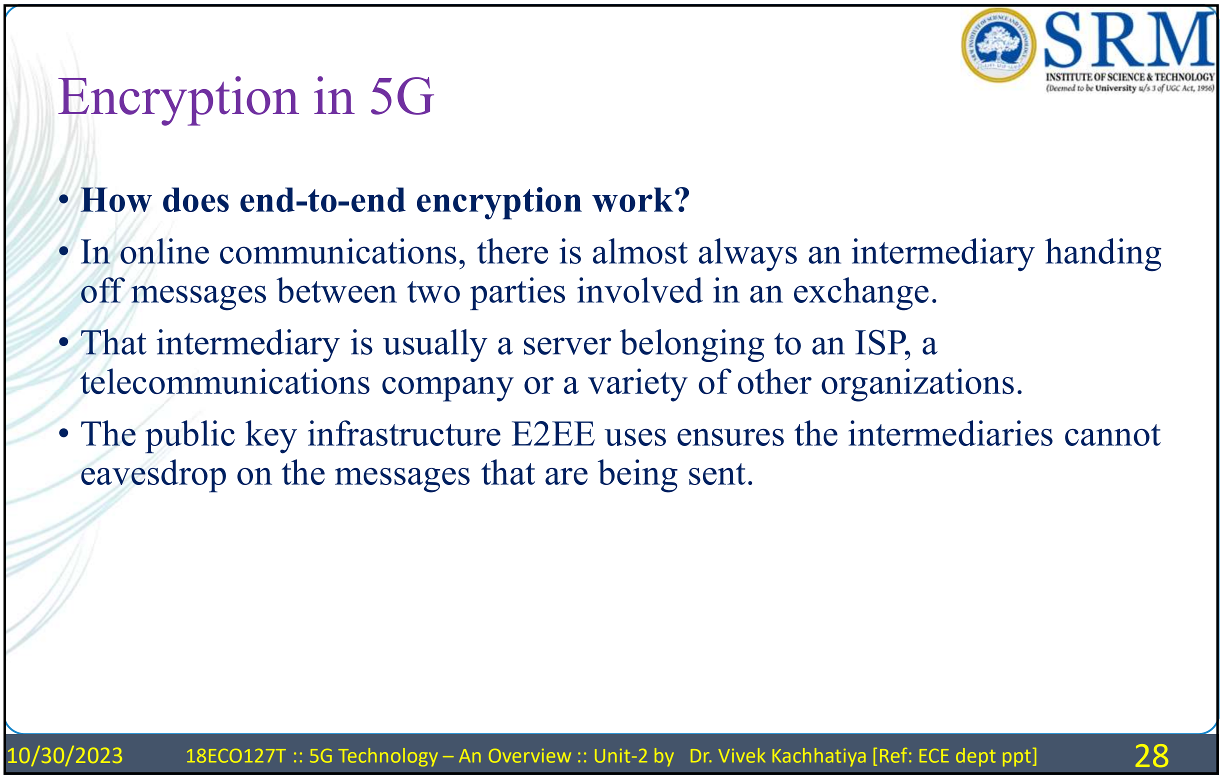
How end-to-end encryption works

Bob
Bob drafts a note to Alice. He gets Alice's public key from a certificate authority and uses it to encrypt the message.

Server
The message passes through an intermediary server but remains encrypted and unreadable.

Alice
Alice receives the message and uses her private key to decrypt the message so she can read it.

ART: SHENDART/GETTY IMAGES



Encryption in 5G

- **How does end-to-end encryption work?**
- In online communications, there is almost always an intermediary handing off messages between two parties involved in an exchange.
- That intermediary is usually a server belonging to an ISP, a telecommunications company or a variety of other organizations.
- The public key infrastructure E2EE uses ensures the intermediaries cannot eavesdrop on the messages that are being sent.

!!THANK YOU!!
!! Have a Nice Day!!

Today we learned about

Authentication and Access Control in 5G

Encryption in 5G

MODULE 4:
5G Security and Privacy

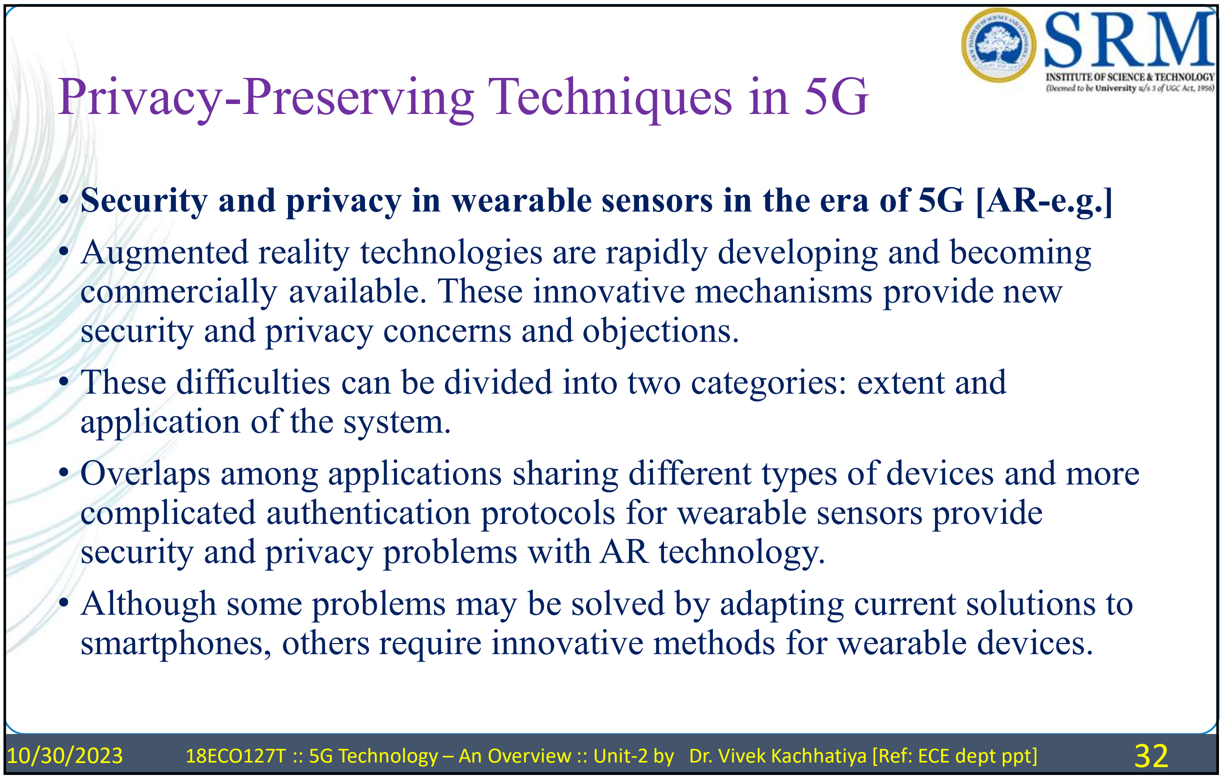
M4 S3

Privacy-Preserving Techniques in 5G

Threat Detection and Mitigation in 5G Networks

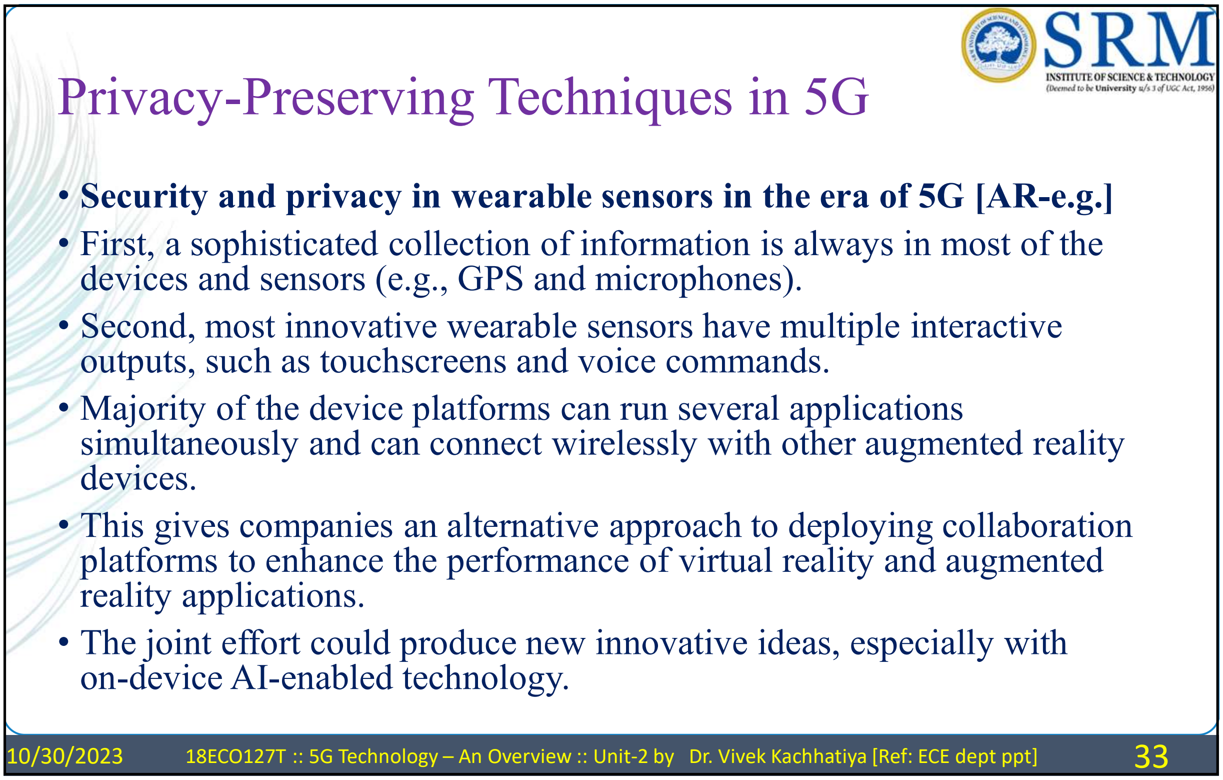
Privacy-Preserving Techniques in 5G

- A critical challenge for the government and enterprises is ensuring data security and privacy when processing huge datasets.
- Most IT companies collect, transport, store, and analyze large datasets and face significant privacy issues every day.
- These issues make the realization of the “Society 5.0” project a challenging issue.
- The issues of data protection during transmission and at rest have attracted scholarly attention recently.
- Cryptographic-based security mechanisms propose different solutions to safeguard the security of datasets as they transit across networks or are stored in data warehouses, for example, encryption and blockchain technologies.
- However, the unresolved issue is how to preserve the privacy of the collected data effectively and securely while it is being processed.



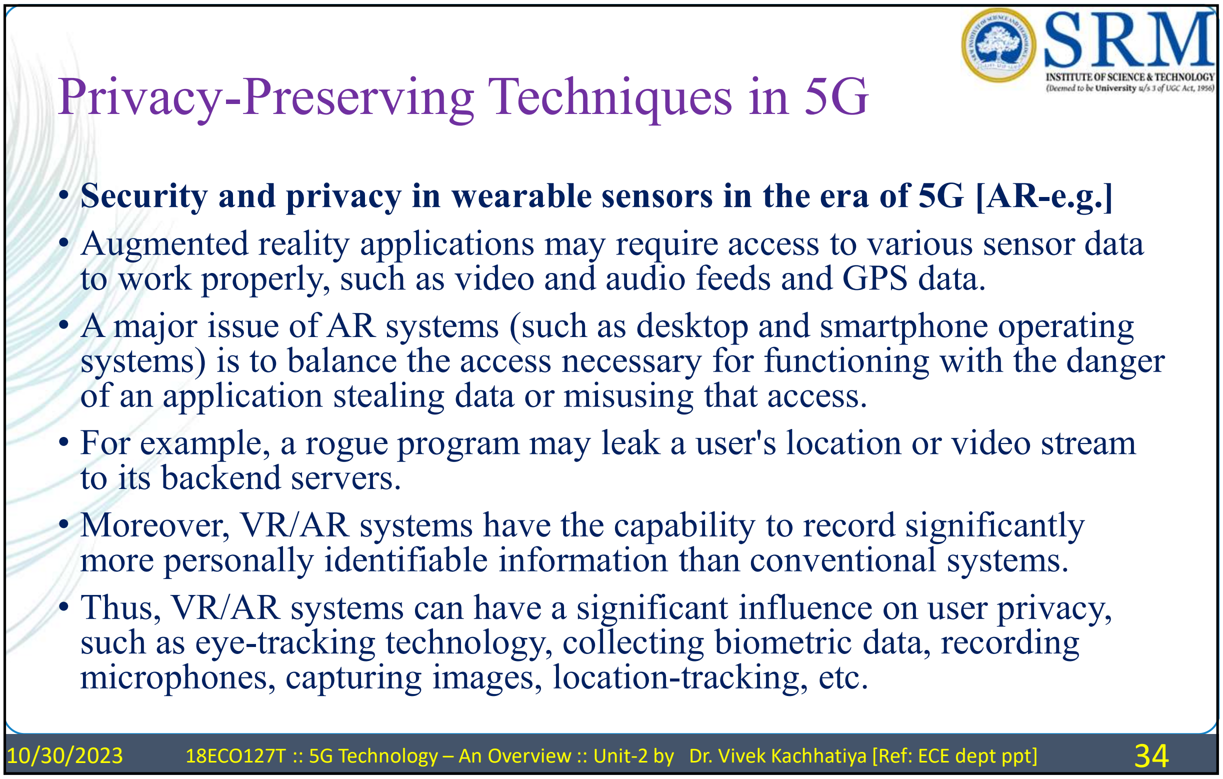
Privacy-Preserving Techniques in 5G

- **Security and privacy in wearable sensors in the era of 5G [AR-e.g.]**
- Augmented reality technologies are rapidly developing and becoming commercially available. These innovative mechanisms provide new security and privacy concerns and objections.
- These difficulties can be divided into two categories: extent and application of the system.
- Overlaps among applications sharing different types of devices and more complicated authentication protocols for wearable sensors provide security and privacy problems with AR technology.
- Although some problems may be solved by adapting current solutions to smartphones, others require innovative methods for wearable devices.



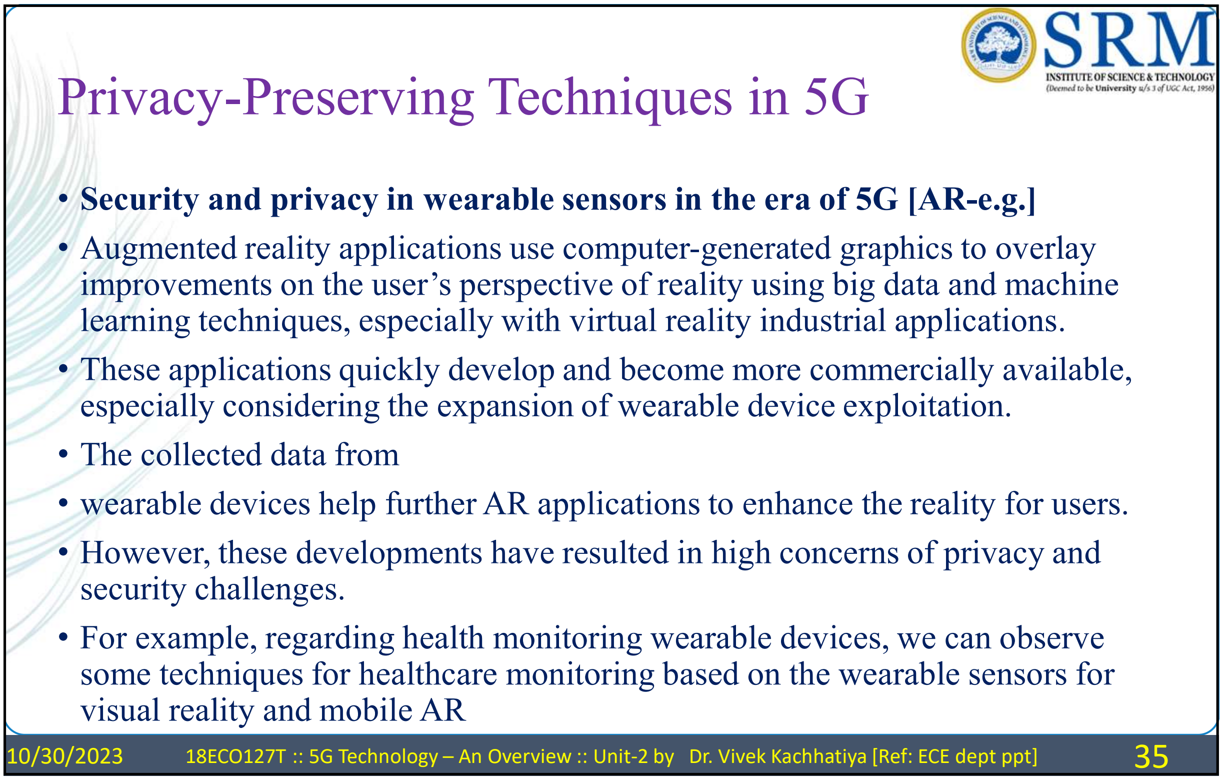
Privacy-Preserving Techniques in 5G

- **Security and privacy in wearable sensors in the era of 5G [AR-e.g.]**
- First, a sophisticated collection of information is always in most of the devices and sensors (e.g., GPS and microphones).
- Second, most innovative wearable sensors have multiple interactive outputs, such as touchscreens and voice commands.
- Majority of the device platforms can run several applications simultaneously and can connect wirelessly with other augmented reality devices.
- This gives companies an alternative approach to deploying collaboration platforms to enhance the performance of virtual reality and augmented reality applications.
- The joint effort could produce new innovative ideas, especially with on-device AI-enabled technology.



Privacy-Preserving Techniques in 5G

- **Security and privacy in wearable sensors in the era of 5G [AR-e.g.]**
- Augmented reality applications may require access to various sensor data to work properly, such as video and audio feeds and GPS data.
- A major issue of AR systems (such as desktop and smartphone operating systems) is to balance the access necessary for functioning with the danger of an application stealing data or misusing that access.
- For example, a rogue program may leak a user's location or video stream to its backend servers.
- Moreover, VR/AR systems have the capability to record significantly more personally identifiable information than conventional systems.
- Thus, VR/AR systems can have a significant influence on user privacy, such as eye-tracking technology, collecting biometric data, recording microphones, capturing images, location-tracking, etc.

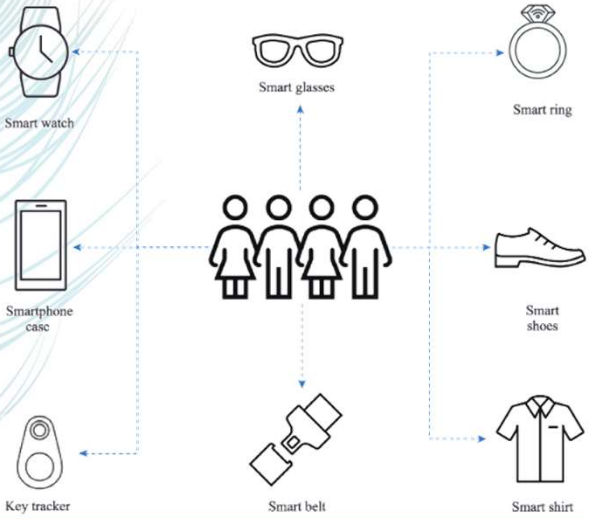


Privacy-Preserving Techniques in 5G

- **Security and privacy in wearable sensors in the era of 5G [AR-e.g.]**
- Augmented reality applications use computer-generated graphics to overlay improvements on the user's perspective of reality using big data and machine learning techniques, especially with virtual reality industrial applications.
- These applications quickly develop and become more commercially available, especially considering the expansion of wearable device exploitation.
- The collected data from
- wearable devices help further AR applications to enhance the reality for users.
- However, these developments have resulted in high concerns of privacy and security challenges.
- For example, regarding health monitoring wearable devices, we can observe some techniques for healthcare monitoring based on the wearable sensors for visual reality and mobile AR

Privacy-Preserving Techniques in 5G

- **Security and privacy in wearable sensors in the era of 5G [AR-e.g.]**



- Figure shows some examples of wearable devices that can be used for AR and VR applications.
- There are other security aspects for wearable healthcare sensors.
- This may cause some problems by manipulating the physical hardware or some problems when the device is measuring data from several sensors and preserving the privacy for predictive analysis.

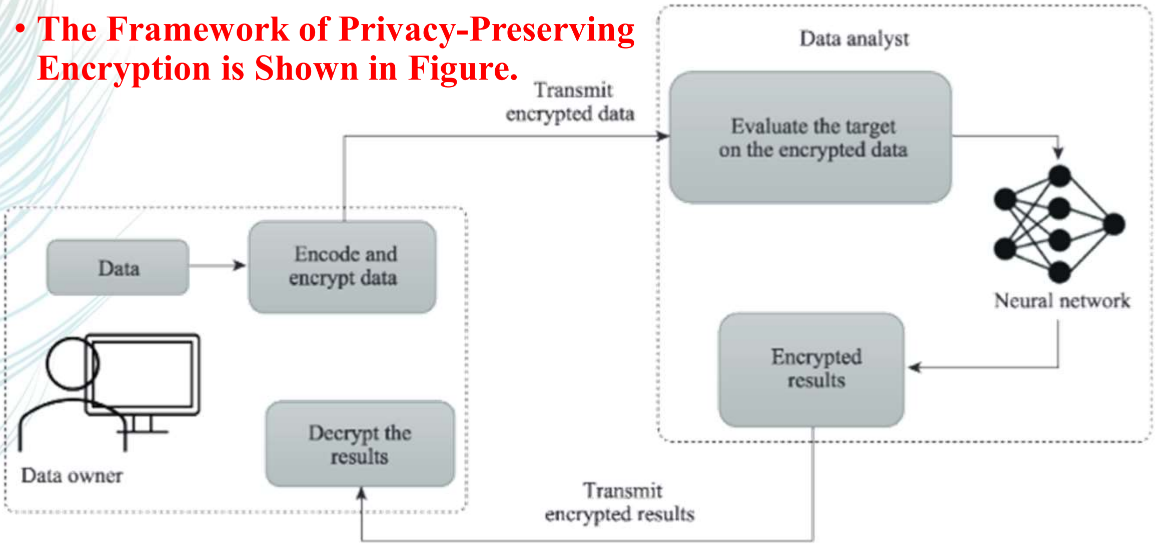
Privacy-Preserving Techniques in 5G

- **Framework Of The Privacy-preserving Technique**
- Our main goal is to assess state-of-the-art solutions for the statistical analysis of confidential data and minimize concerns of the user's privacy.
- These techniques should enable the use of advanced analytic techniques over encrypted private information sets with very large and diverse big datasets.
- They can also have the capacity to delegate computations to a third party, such as cloud providers, considering the resources.
- In addition, the competency of data analysts has spurred advancements toward efficient privacy-preserving deep learning for big data analysis.
- Therefore, several techniques have been developed to assess the usability, level of security, and performance of homomorphic encryption when used in big data applications.

•Privacy-Preserving Techniques in 5G

Framework Of The Privacy-preserving Technique

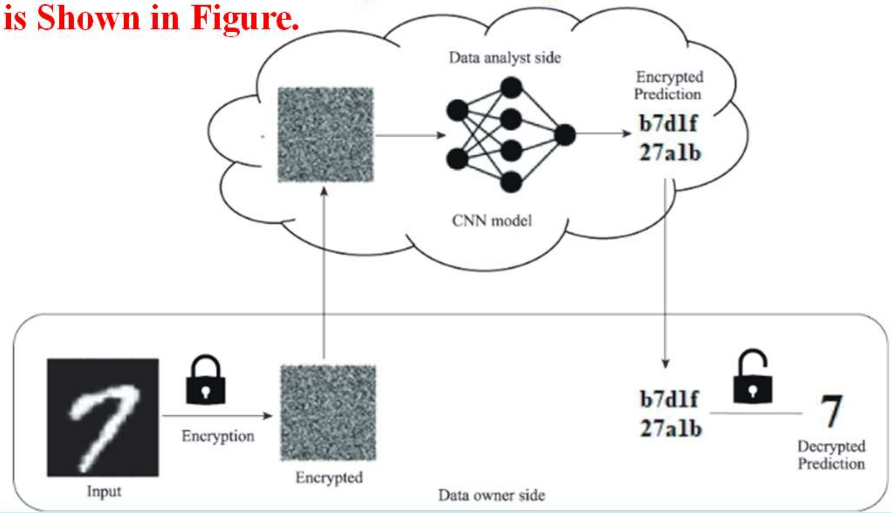
- **The Framework of Privacy-Preserving Encryption is Shown in Figure.**



•Privacy-Preserving Techniques in 5G

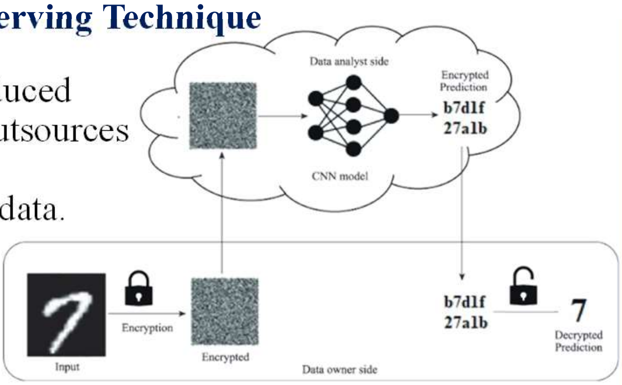
Framework Of The Privacy-preserving Technique

- **The Framework of Advance Privacy-Preserving Encryption is Shown in Figure.**



•Privacy-Preserving Techniques in 5G

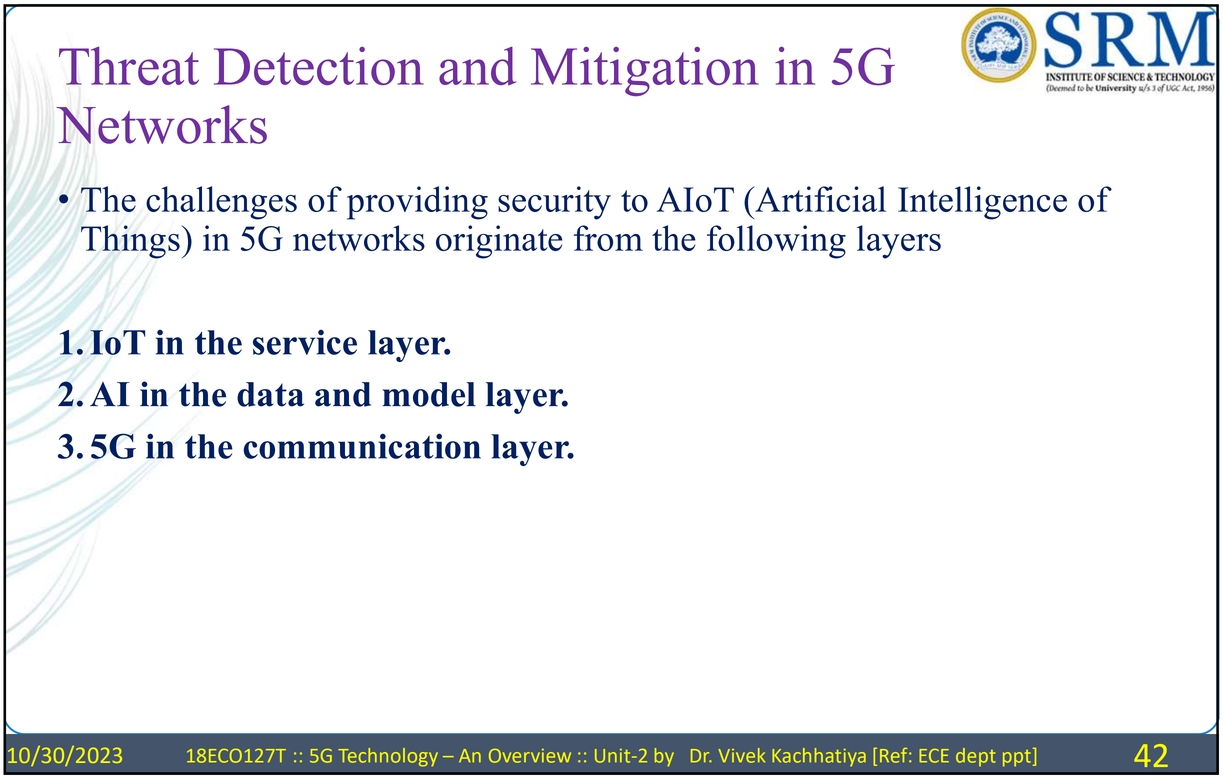
Framework Of The Privacy-preserving Technique



- Initially, private prediction is introduced as a service when the data owner outsources a third party for analytics or the prediction of private encrypted data.
- For example-1, consider an untrustworthy data analyst with a trained model and perhaps the computational capabilities to perform the analytic tasks.
- For example-2, consider an untrustworthy data analyst with a trained model and perhaps the computational capabilities to perform the prediction challenge.

Threat Detection and Mitigation in 5G Networks

- With communications, computation, and storage capabilities, IoT devices in cyberspace could deeply interact with humans in the physical world.
- The features of high transmission rate, low latency, and ubiquitous connectivity make 5G a promising communication bearer to support applications of AIoT (Artificial Intelligence of Things).
- For example, an intelligent factory scenario in Non-Public Network (NPN) where AIoT devices with 5G connectivity are deployed in a factory to facilitate the high-precision operations of manufacturing.
- Moreover, AIoT integrated into a vehicle enables autonomous driving with the assistance of low latency and reliable 5G communications.
- The combination of core technologies of 5G, AI, and IoT, on the one hand, opens the door to innovation but, on the other hand, amplifies the security threats originating from individual components.



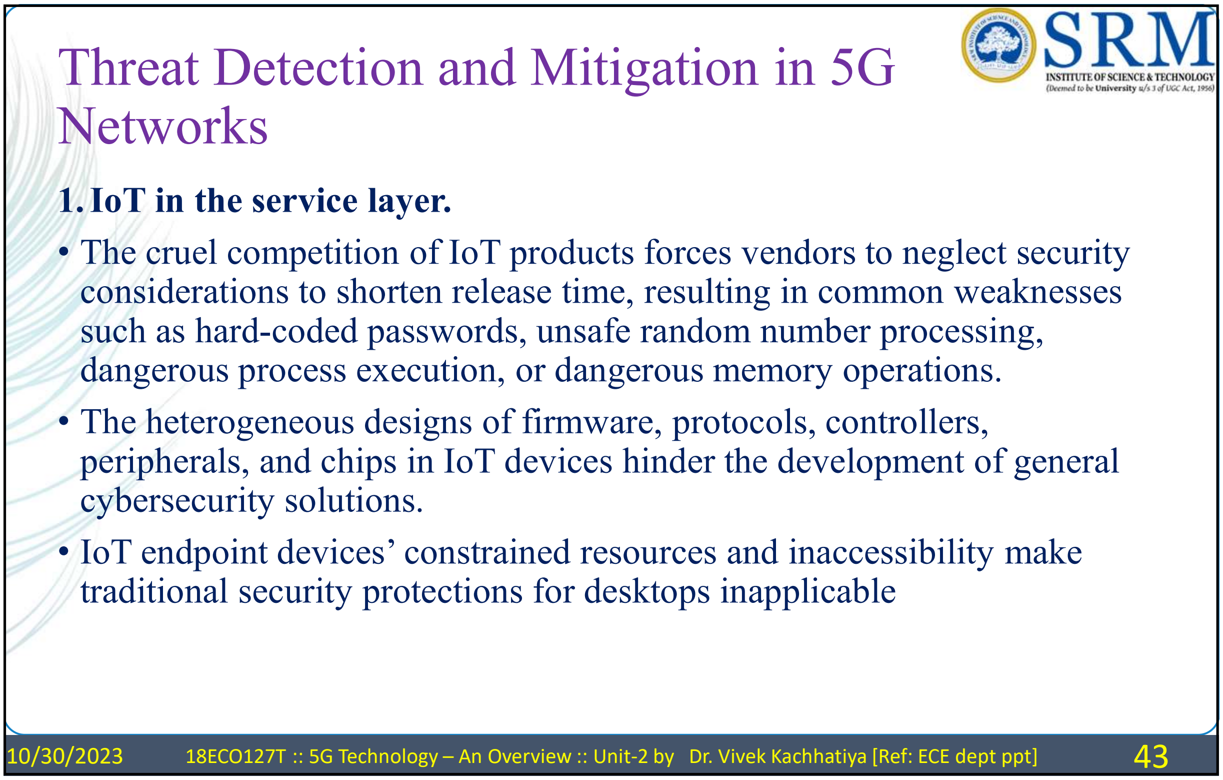
Threat Detection and Mitigation in 5G Networks

- The challenges of providing security to AIoT (Artificial Intelligence of Things) in 5G networks originate from the following layers

1. IoT in the service layer.

2. AI in the data and model layer.

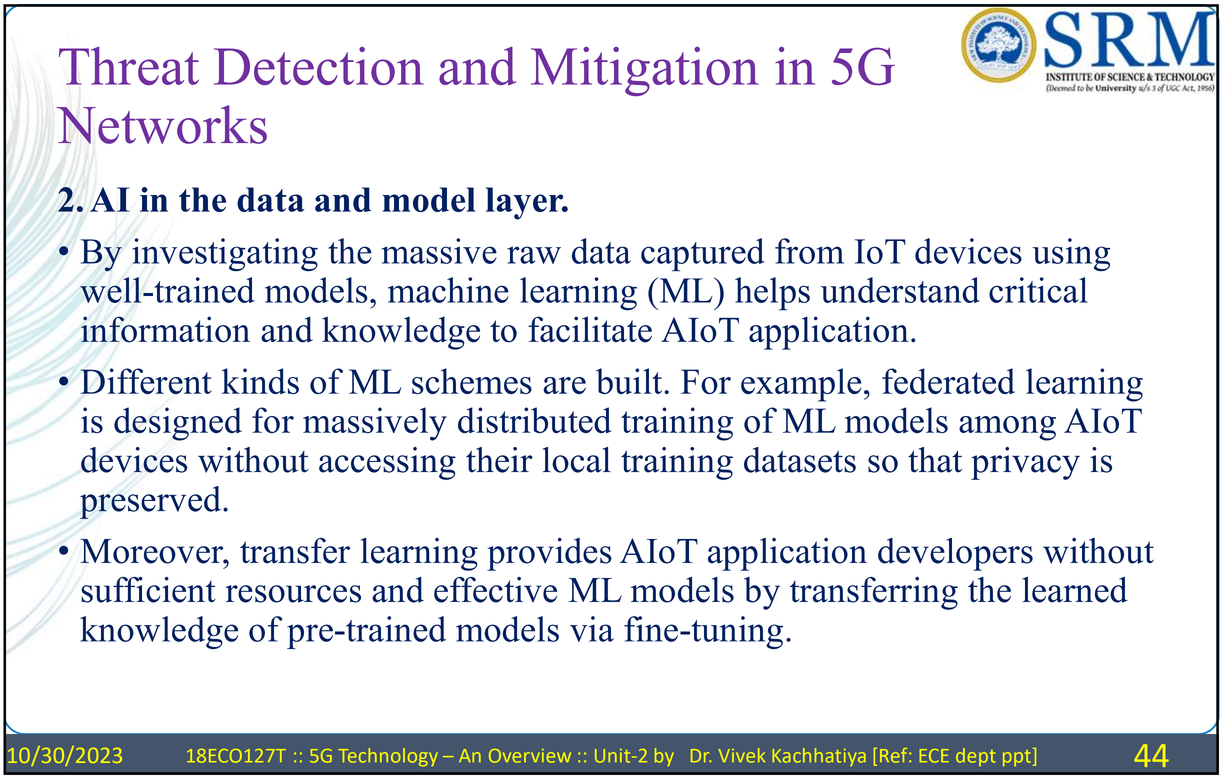
3. 5G in the communication layer.



Threat Detection and Mitigation in 5G Networks

1. IoT in the service layer.

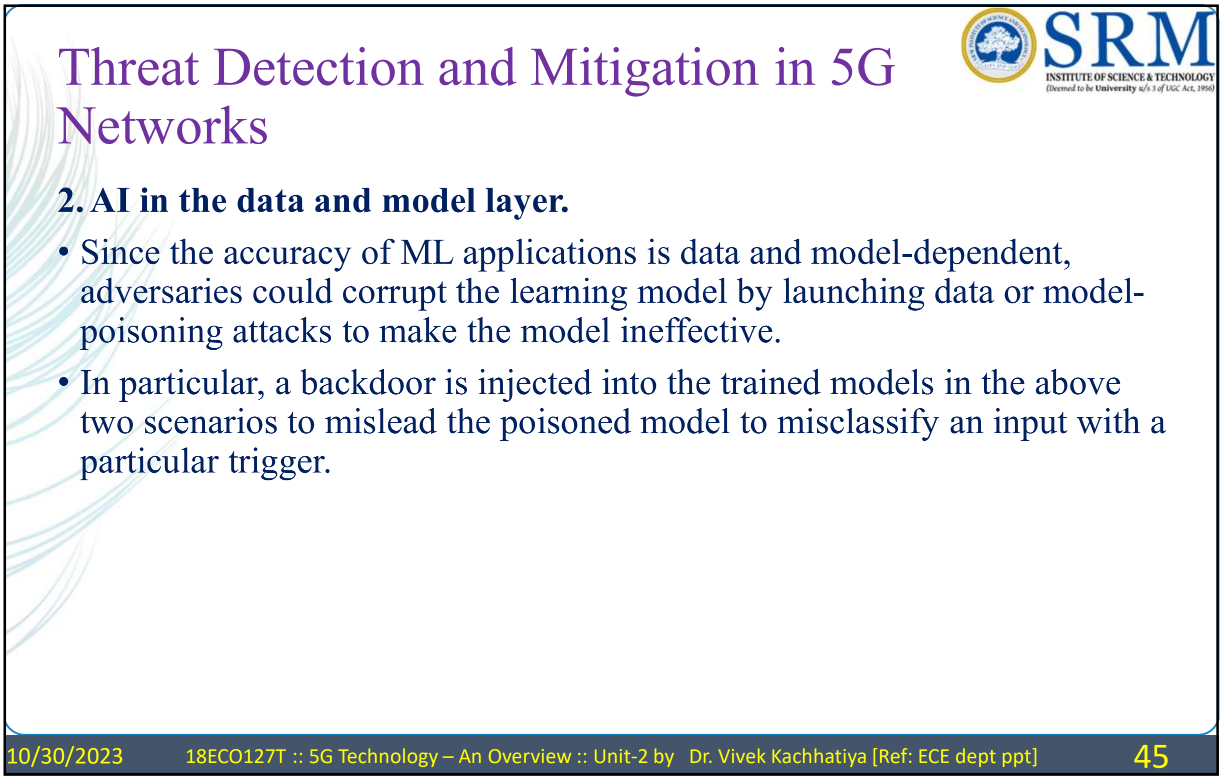
- The cruel competition of IoT products forces vendors to neglect security considerations to shorten release time, resulting in common weaknesses such as hard-coded passwords, unsafe random number processing, dangerous process execution, or dangerous memory operations.
- The heterogeneous designs of firmware, protocols, controllers, peripherals, and chips in IoT devices hinder the development of general cybersecurity solutions.
- IoT endpoint devices' constrained resources and inaccessibility make traditional security protections for desktops inapplicable



Threat Detection and Mitigation in 5G Networks

2. AI in the data and model layer.

- By investigating the massive raw data captured from IoT devices using well-trained models, machine learning (ML) helps understand critical information and knowledge to facilitate AIoT application.
- Different kinds of ML schemes are built. For example, federated learning is designed for massively distributed training of ML models among AIoT devices without accessing their local training datasets so that privacy is preserved.
- Moreover, transfer learning provides AIoT application developers without sufficient resources and effective ML models by transferring the learned knowledge of pre-trained models via fine-tuning.



Threat Detection and Mitigation in 5G Networks

2. AI in the data and model layer.

- Since the accuracy of ML applications is data and model-dependent, adversaries could corrupt the learning model by launching data or model-poisoning attacks to make the model ineffective.
- In particular, a backdoor is injected into the trained models in the above two scenarios to mislead the poisoned model to misclassify an input with a particular trigger.

Threat Detection and Mitigation in 5G Networks

3. 5G in the communication layer.

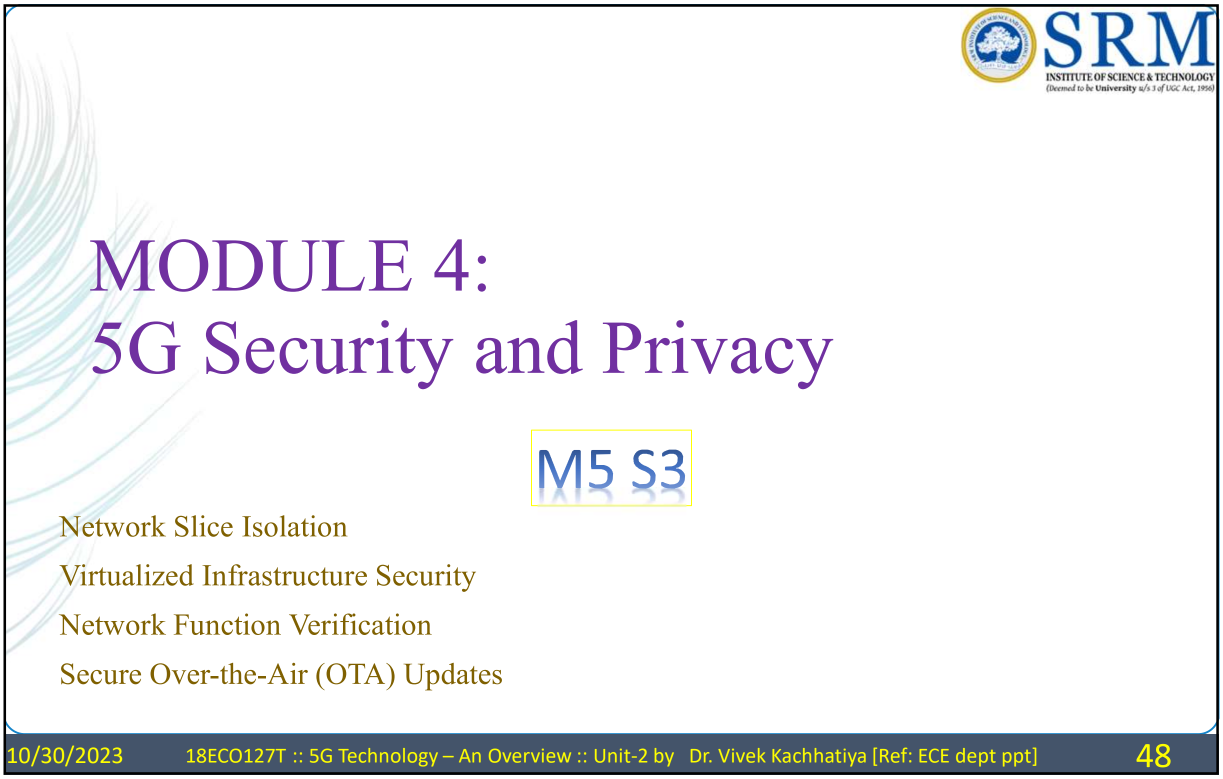
- The sophisticated Authentication and Key Agreement (AKA) procedures evolved from each generation of the cellular network provide mutual authentication as well as confidentiality and integrity protection between User Equipment (UE) and Core Network (CN).
- The public key protection for signaling messages exchanged before AKA make spoofing or relaying of message much more difficult.
- The appearance of cheap Software-Defined Radio (SDR) and 5G open source enables the attack from rogue/fake Base Station (BS), where experimental 5G BS behaving the same as the operational one misleads victim UE to achieve sensitive information stealing or service disabling.

!!THANK YOU!!
!! Have a Nice Day!!

Today we learned about

Privacy-Preserving Techniques in 5G

Threat Detection and Mitigation in 5G Networks



MODULE 4:
5G Security and Privacy

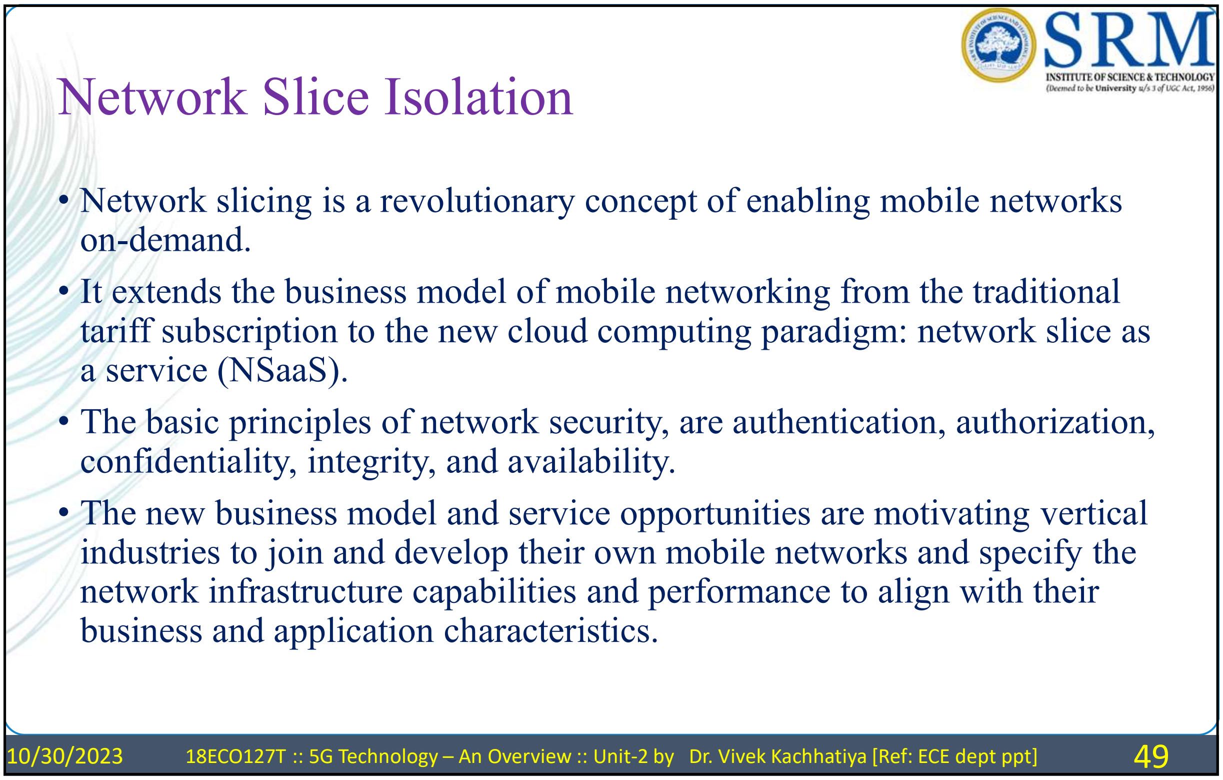
M5 S3

Network Slice Isolation

Virtualized Infrastructure Security

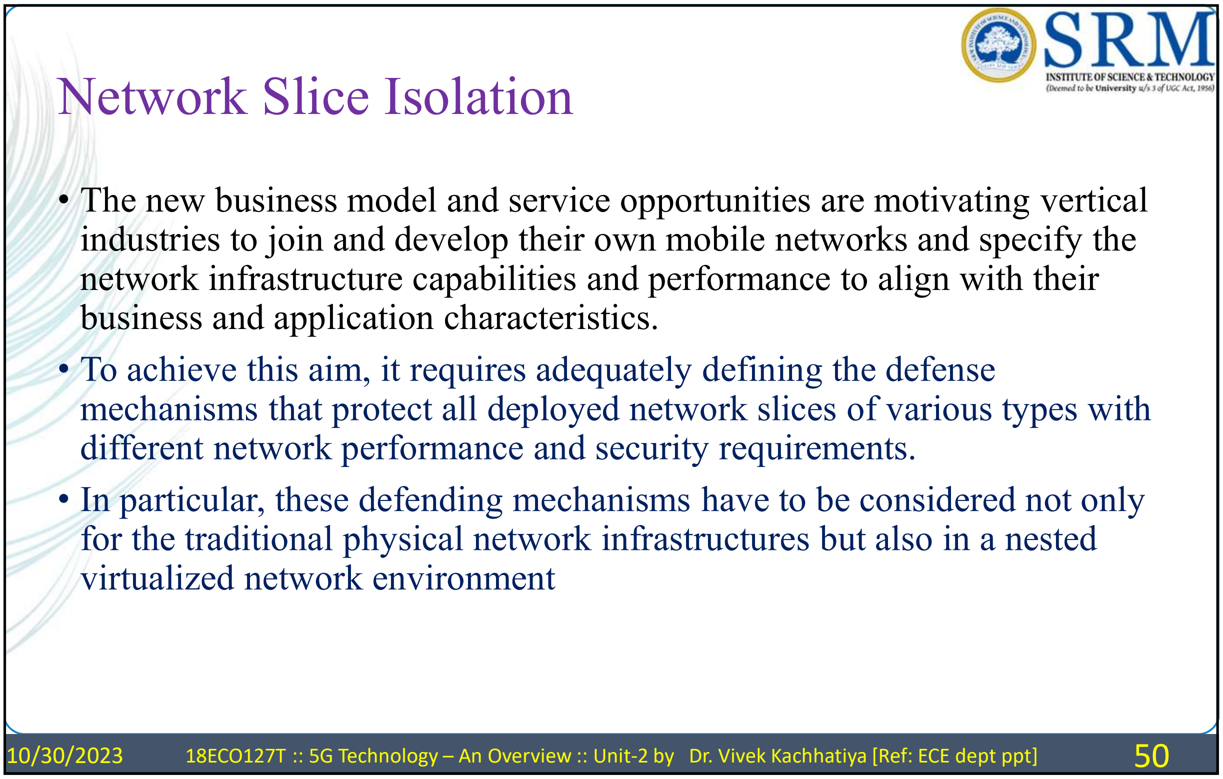
Network Function Verification

Secure Over-the-Air (OTA) Updates



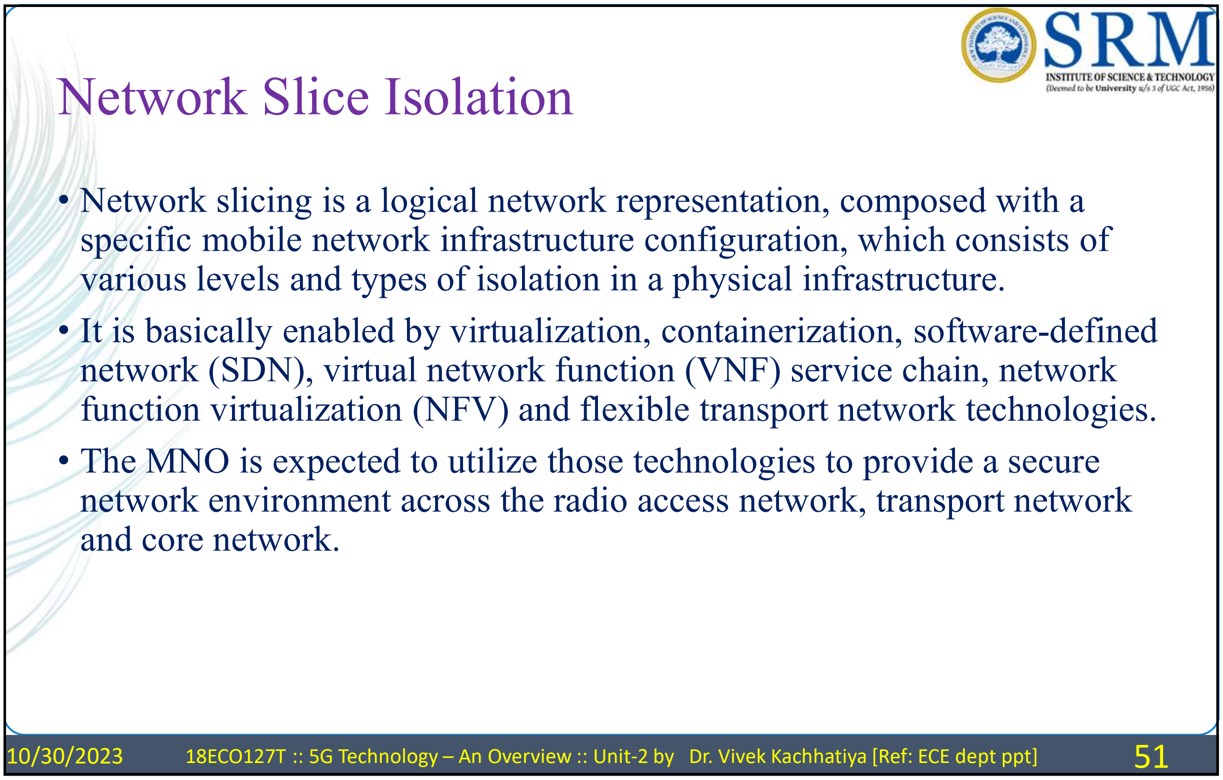
Network Slice Isolation

- Network slicing is a revolutionary concept of enabling mobile networks on-demand.
- It extends the business model of mobile networking from the traditional tariff subscription to the new cloud computing paradigm: network slice as a service (NSaaS).
- The basic principles of network security, are authentication, authorization, confidentiality, integrity, and availability.
- The new business model and service opportunities are motivating vertical industries to join and develop their own mobile networks and specify the network infrastructure capabilities and performance to align with their business and application characteristics.



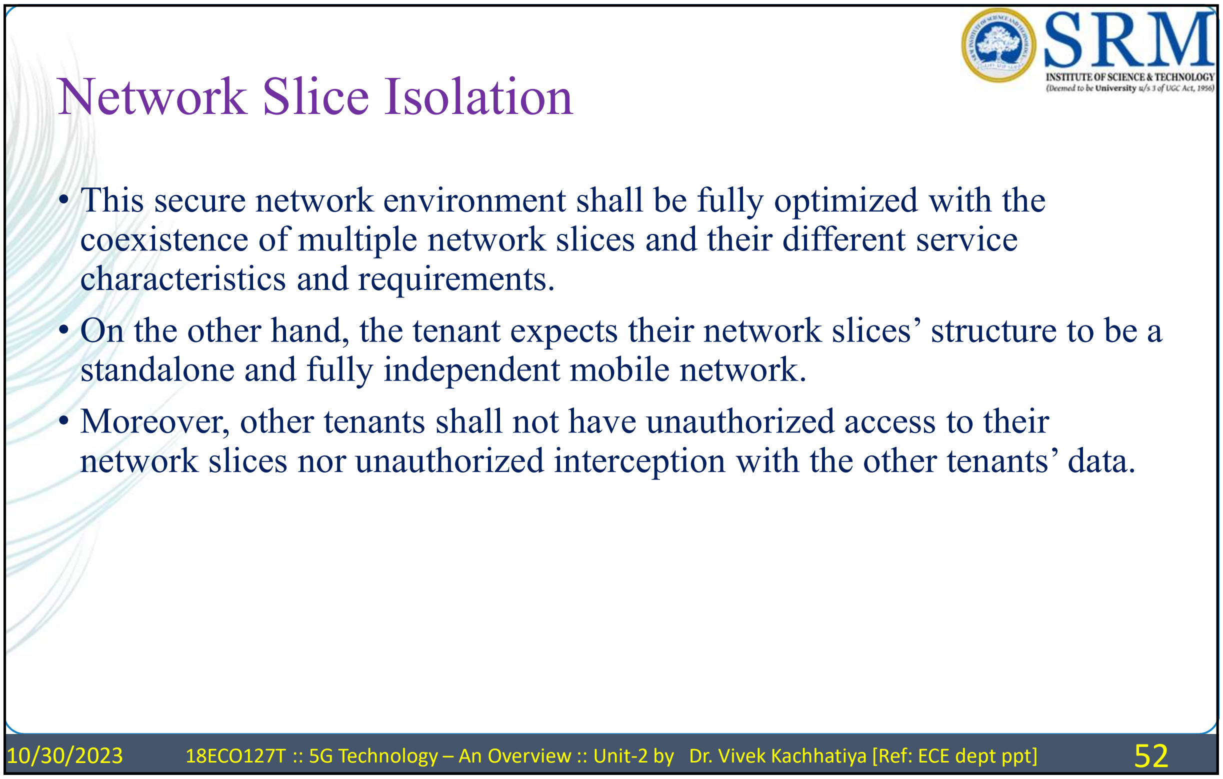
Network Slice Isolation

- The new business model and service opportunities are motivating vertical industries to join and develop their own mobile networks and specify the network infrastructure capabilities and performance to align with their business and application characteristics.
- To achieve this aim, it requires adequately defining the defense mechanisms that protect all deployed network slices of various types with different network performance and security requirements.
- In particular, these defending mechanisms have to be considered not only for the traditional physical network infrastructures but also in a nested virtualized network environment



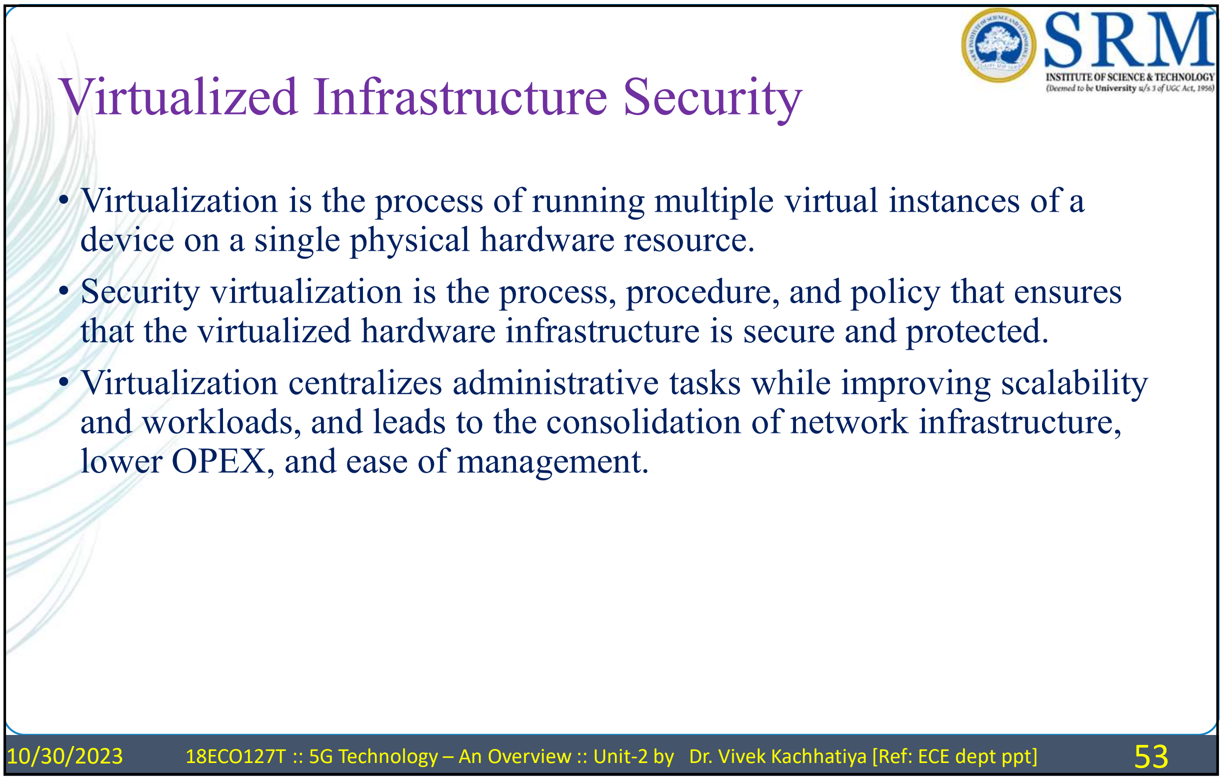
Network Slice Isolation

- Network slicing is a logical network representation, composed with a specific mobile network infrastructure configuration, which consists of various levels and types of isolation in a physical infrastructure.
- It is basically enabled by virtualization, containerization, software-defined network (SDN), virtual network function (VNF) service chain, network function virtualization (NFV) and flexible transport network technologies.
- The MNO is expected to utilize those technologies to provide a secure network environment across the radio access network, transport network and core network.



Network Slice Isolation

- This secure network environment shall be fully optimized with the coexistence of multiple network slices and their different service characteristics and requirements.
- On the other hand, the tenant expects their network slices' structure to be a standalone and fully independent mobile network.
- Moreover, other tenants shall not have unauthorized access to their network slices nor unauthorized interception with the other tenants' data.



Virtualized Infrastructure Security

- Virtualization is the process of running multiple virtual instances of a device on a single physical hardware resource.
- Security virtualization is the process, procedure, and policy that ensures that the virtualized hardware infrastructure is secure and protected.
- Virtualization centralizes administrative tasks while improving scalability and workloads, and leads to the consolidation of network infrastructure, lower OPEX, and ease of management.

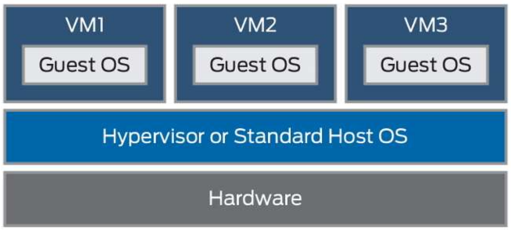
Virtualized Infrastructure Security

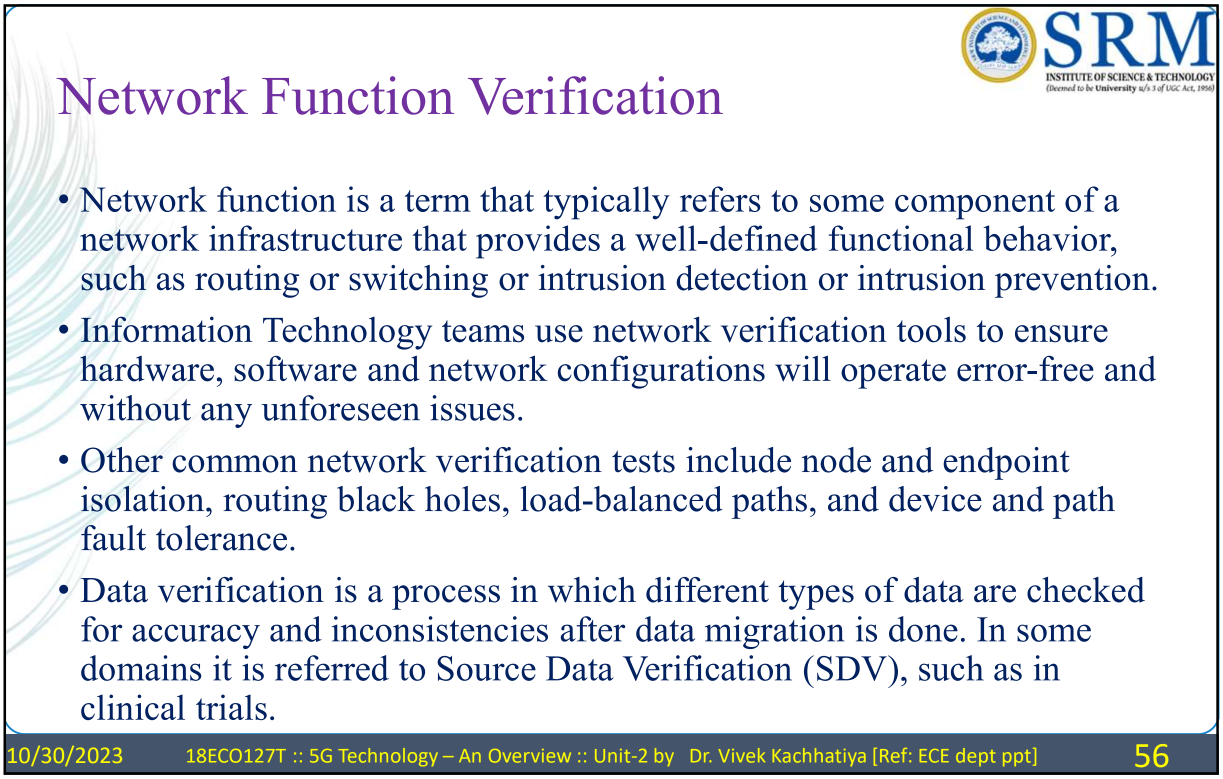
- **Problems with Security Virtualization Addresses**
- Virtualization introduces security challenges that physical security systems cannot adequately protect against:

1. File sharing between hosts and guests is not secure.
2. Isolation between components such as guest OSs and applications, hypervisors, hardware are weakened.
3. Multiple servers are consolidated which increases the risk that a compromise may spread from applications on the same host.
4. For intrusion prevention systems (IPS), malware targeted for physical and virtual machines causes infection via the virtual network. Other security threats include unauthorized access, denial of service, and exploits.

Virtualized Infrastructure Security

- Security virtualization acts as a barrier to secure perimeter access to a network.
- It provides dedicated security services and assured traffic isolation within the cloud, along with customizable firewall controls as an additional managed service.
- Enterprises and service providers can leverage their virtualization investment to create a granular security perimeter, giving dedicated security resources within a cloud construct to tenants and service subscribers.





SRM INSTITUTE OF SCIENCE & TECHNOLOGY (Deemed to be University u/s 3 of UGC Act, 1956)

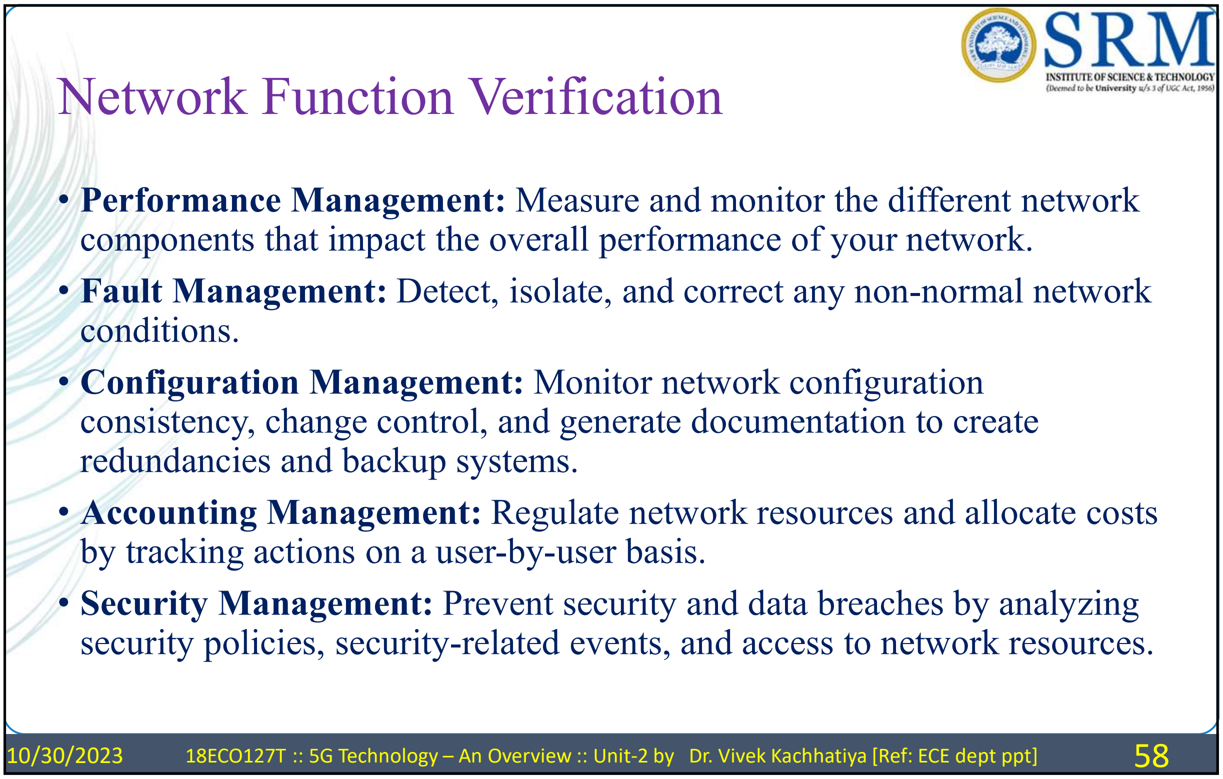
Network Function Verification

- Network function is a term that typically refers to some component of a network infrastructure that provides a well-defined functional behavior, such as routing or switching or intrusion detection or intrusion prevention.
- Information Technology teams use network verification tools to ensure hardware, software and network configurations will operate error-free and without any unforeseen issues.
- Other common network verification tests include node and endpoint isolation, routing black holes, load-balanced paths, and device and path fault tolerance.
- Data verification is a process in which different types of data are checked for accuracy and inconsistencies after data migration is done. In some domains it is referred to Source Data Verification (SDV), such as in clinical trials.

SRM INSTITUTE OF SCIENCE & TECHNOLOGY (Deemed to be University u/s 3 of UGC Act, 1956)

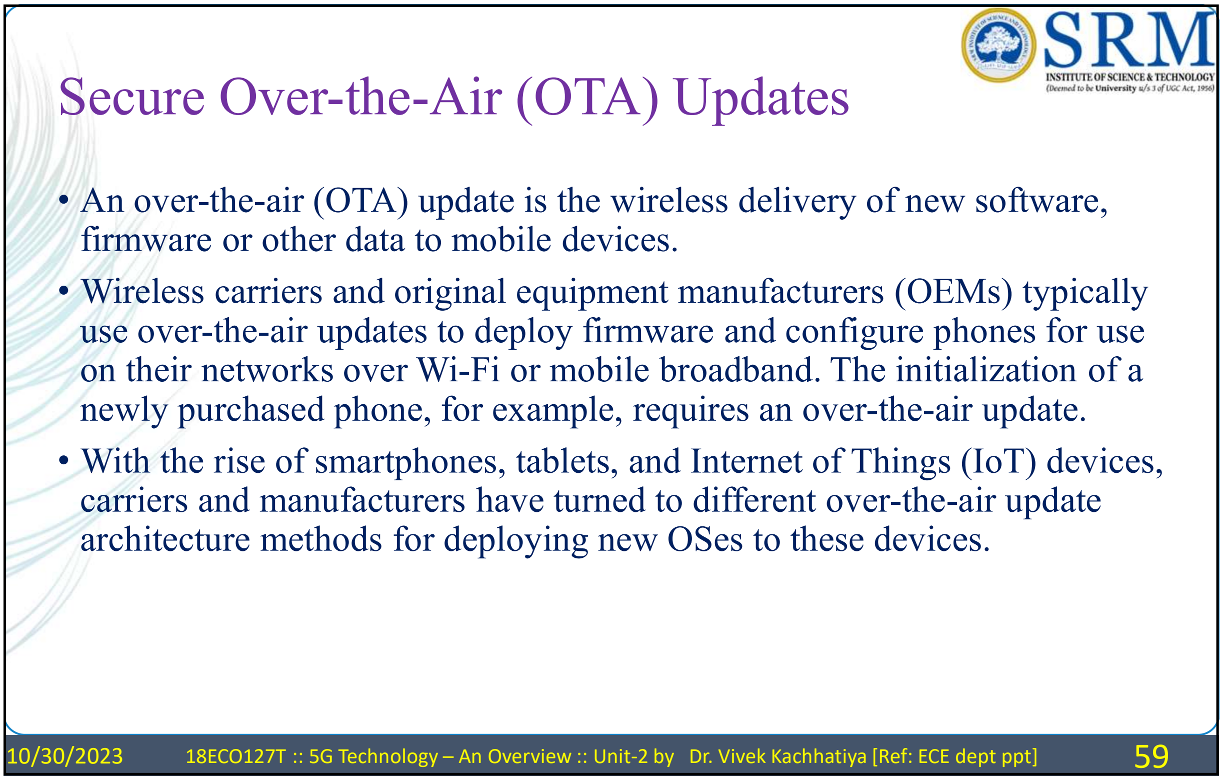
Network Function Verification

- The ISO is an international nongovernmental organization that develops proprietary, industrial, and commercial standards.
- Comprised of representatives from various countries and standards organizations, the ISO defines five main types of network management solutions as the following:
- Performance Management:
- Fault Management:
- Configuration Management:
- Accounting Management:
- Security Management:
- Each of these five functional areas plays a vital role in successfully implementing and maintaining an effective network management system.



Network Function Verification

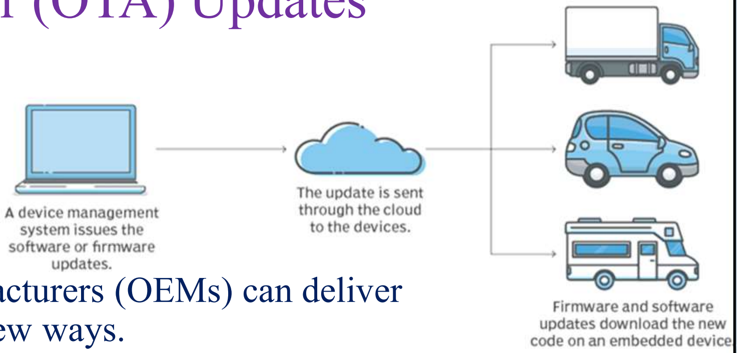
- **Performance Management:** Measure and monitor the different network components that impact the overall performance of your network.
- **Fault Management:** Detect, isolate, and correct any non-normal network conditions.
- **Configuration Management:** Monitor network configuration consistency, change control, and generate documentation to create redundancies and backup systems.
- **Accounting Management:** Regulate network resources and allocate costs by tracking actions on a user-by-user basis.
- **Security Management:** Prevent security and data breaches by analyzing security policies, security-related events, and access to network resources.



Secure Over-the-Air (OTA) Updates

- An over-the-air (OTA) update is the wireless delivery of new software, firmware or other data to mobile devices.
- Wireless carriers and original equipment manufacturers (OEMs) typically use over-the-air updates to deploy firmware and configure phones for use on their networks over Wi-Fi or mobile broadband. The initialization of a newly purchased phone, for example, requires an over-the-air update.
- With the rise of smartphones, tablets, and Internet of Things (IoT) devices, carriers and manufacturers have turned to different over-the-air update architecture methods for deploying new OSes to these devices.

Secure Over-the-Air (OTA) Updates



A device management system issues the software or firmware updates.

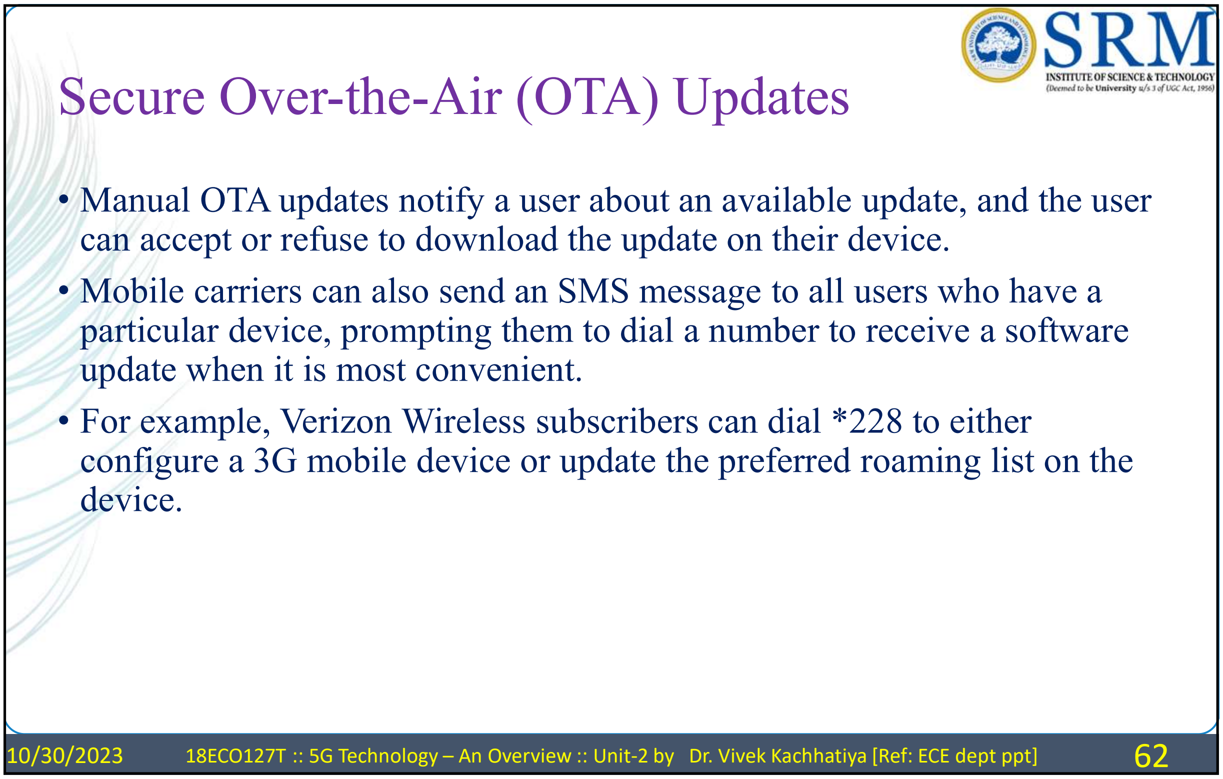
The update is sent through the cloud to the devices.

Firmware and software updates download the new code on an embedded device

- Original equipment manufacturers (OEMs) can deliver OTA updates to users in a few ways.
- From the end user's perspective, the OTA update can either be automatic or manual.

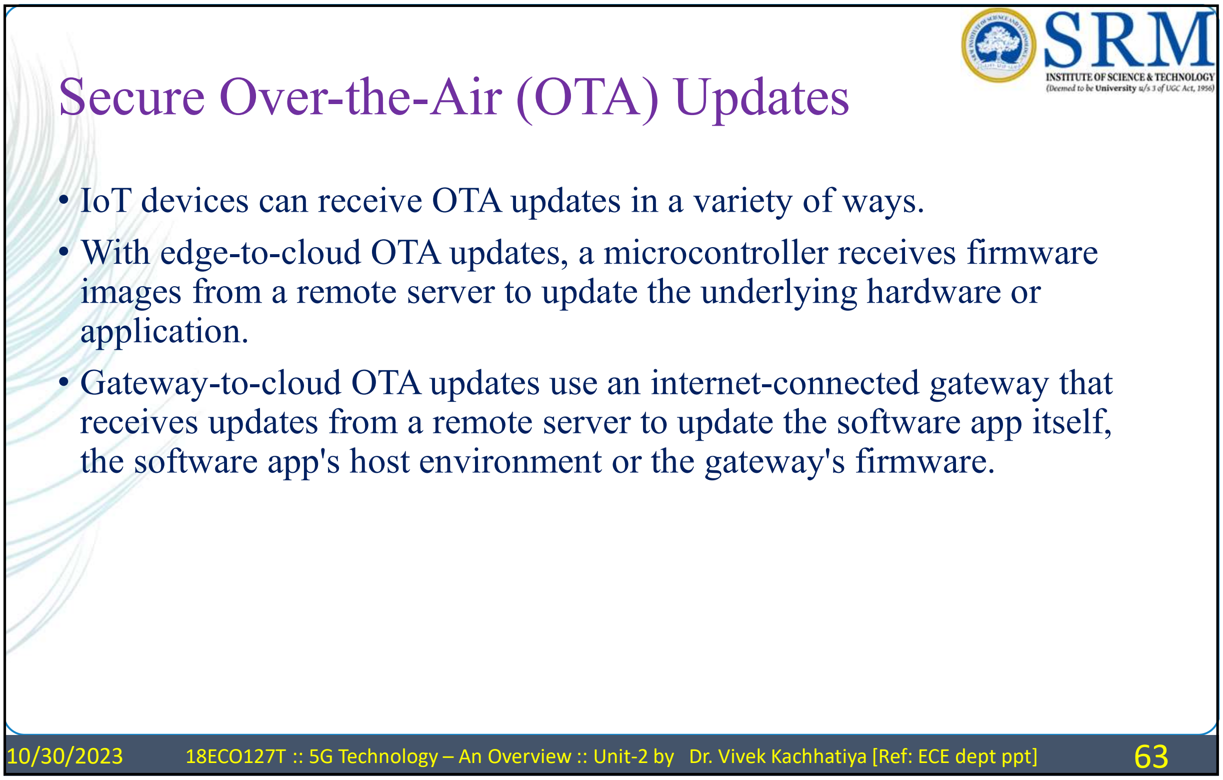
Secure Over-the-Air (OTA) Updates

- With an automatic OTA update, the back-end system of a mobile operator can push a firmware update to the end user's device.
- OEMs can use products that automate OTA updates, such as platforms from Smith Micro and Akamai, to manage and deploy OTA updates to their end users' devices.
- Devices that are in remote locations, such as IoT sensors, or devices that don't have frequent human contact, such as an autonomous vehicle, are good contenders for automatic OTA updates.



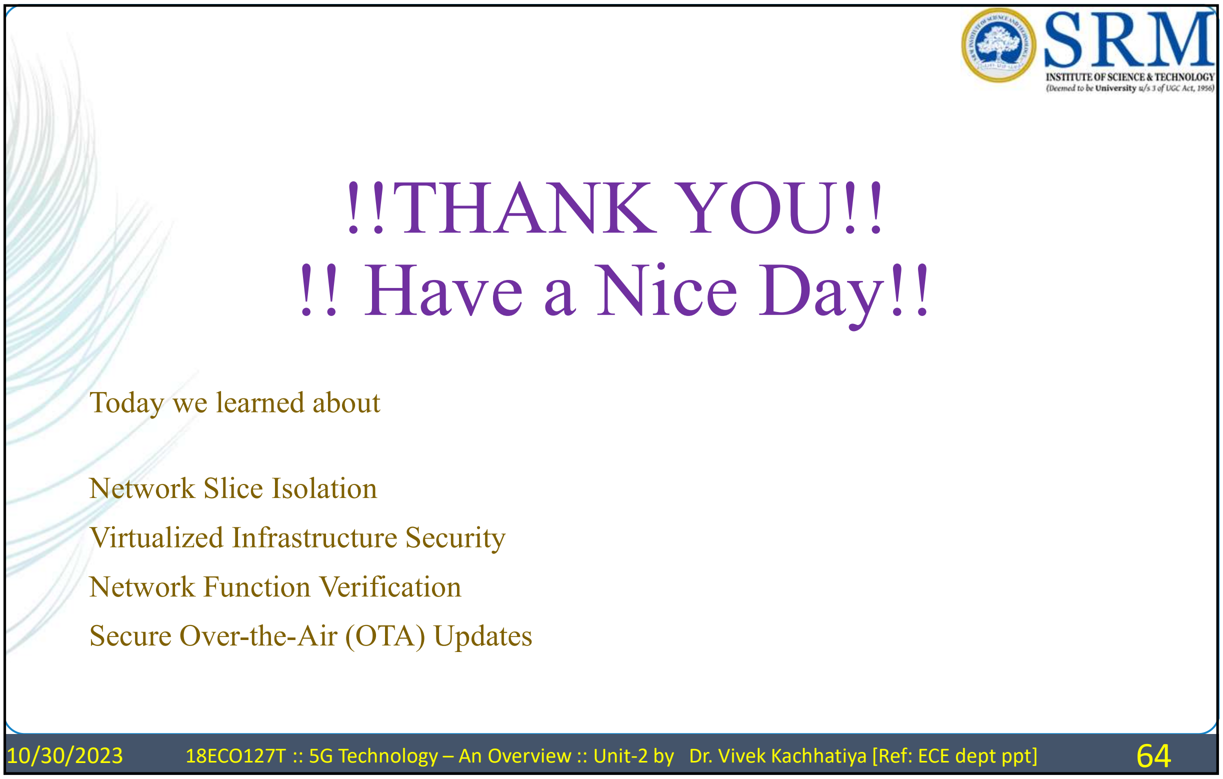
Secure Over-the-Air (OTA) Updates

- Manual OTA updates notify a user about an available update, and the user can accept or refuse to download the update on their device.
- Mobile carriers can also send an SMS message to all users who have a particular device, prompting them to dial a number to receive a software update when it is most convenient.
- For example, Verizon Wireless subscribers can dial *228 to either configure a 3G mobile device or update the preferred roaming list on the device.



Secure Over-the-Air (OTA) Updates

- IoT devices can receive OTA updates in a variety of ways.
- With edge-to-cloud OTA updates, a microcontroller receives firmware images from a remote server to update the underlying hardware or application.
- Gateway-to-cloud OTA updates use an internet-connected gateway that receives updates from a remote server to update the software app itself, the software app's host environment or the gateway's firmware.



SRM INSTITUTE OF SCIENCE & TECHNOLOGY (Deemed to be University u/s 3 of UGC Act, 1956)

!!THANK YOU!!
!! Have a Nice Day!!

Today we learned about

Network Slice Isolation

Virtualized Infrastructure Security

Network Function Verification

Secure Over-the-Air (OTA) Updates