IIT MADRAS
Indian Institute of Technology Madras

Technology Transfer Office
TTO IPM Cell

Industrial Consultancy & Sponsored Research (IC&SR)

Group Anonymous Dynamic Slice enabled 5G Systems with Privacy Preserving Service Access

IITM Technology Available for Licensing

Problem Statement

- Existing networks lack the **adaptability** to **securely manage diverse services** across industries within a 5G infrastructure, leading to **vulnerabilities and potential breaches**.
- Current authentication methods **compromise user privacy** very often, especially in Device-to-Device (**D2D**) communications, **hindering** secure interaction and limiting service access.
- Hence, there is a need for a **robust method** to enable **secure independent formation and management of network slices**, ensuring authenticity, and **resistance against attacks or unauthorized access.**

Technology Category/ Market

Category: 5G & Next Generation Networks

Industry: Telecommunications, Network Security

Applications: It focuses on privacy-preserving authentication, secure slice formation, Network Slicing Management, dynamic association between network elements, addressing critical security needs in evolving telecommunications Services, Device-to-Device D2D Communication

Market: The global 5G services market size was valued at **USD 60.61 Bn in 2022.** It is expected to grow at **59.4%** CAGR of from **2023 to 2030**.

Technology

The present patent invention discloses a **Group Anonymous Dynamic Slice enabled 5G Systems with Privacy Preserving Service Access.** It revolves around creating secure, private, efficient communication in 5G network, emphasizing privacy and authentication.

TRL (Technology Readiness Level)

TRL-3: Proof of Concept established

Intellectual Property

IITM IDF No.: **1789** | IP No.: **478604 (Granted)**

Research Lab

Prof. Siva Ram Murthy C
Dept. of Computer Science and Engineering

Key Features / Value Proposition

User perspective:

- Ensures secure and private service access, preserving user anonymity and usage behavior.
- Enables reliable and authenticated connections, fostering trust in network interactions.
- Facilitates customized offerings while safeguarding user data-identity.

Industrial perspective:-

- Supports industry requirements via customizable network slices, ensuring optimized service supply.
- Enhances network security and integrity for to deal with sensitive data and critical operations.
- Enables dynamic associations while maintaining stringent security protocols, optimizing resources.

Technology perspective:

- Implements elliptic curve and proxy re-encryption techniques for robust and private authentication.
- Offers agile creation and management of network slices, improving scalability.
- Protects user identities, usage history, and slice associations for robust privacy safeguards.

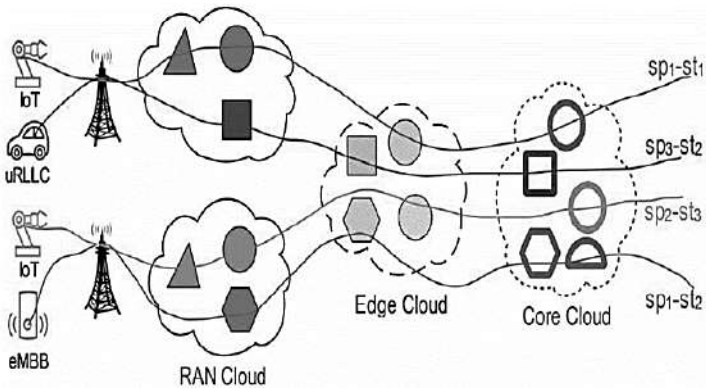


FIG. 1 shows an exemplary NFV enabled 5G mobile network architecture

CONTACT US
Dr. Dara Ajay, Head
Technology Transfer Office,
IPM Cell IC&SR, IIT Madras

IITM TTO Website:
https://ipm.icsr.in/ipm/

Email: smipm-icsr@icsrpis.iitm.ac.in
sm-marketing@imail.iitm.ac.in
Phone: +91-44-2257 9756/ 9719

Group Anonymous Dynamic Slice enabled 5G Systems with Privacy Preserving Service Access

IITM Technology Available for Licensing

Technology Description

- **Secure Network Slicing:**
  - Utilizes NFV in 5G to create diverse network slices for different industries.
  - Ensures each slice meets specific requirements efficiently.
- **Dynamic Distributed Associations:**
  - Establishes secure links between Network Slice Components (NSCs).
  - Allows NSCs within a slice to securely authenticate without a centralized authority.
- **Privacy-Preserving Authentication:**
  - Implements mutual authentication for entities like service providers and user devices.
  - Maintains user anonymity in interactions and device-to-device (D2D) services.
- **Key Management and Encryption:**
  - Uses cryptographic methods like proxy re-encryption to manage and secure communication.
  - Utilizes elliptic curve cryptography for encryption purposes.
- **Role of Network Components:**
  - Orchestrator, slice manager, & infrastructure manager ensure secure network slice operation.
  - Focuses on security, management, and efficient utilization of resources.
- **Defense against Attacks:**
  - Guards against topology learning attacks via unique key generation.
  - Ensures group anonymity within the network for legitimate entities.

FIG. 3 show the procedure for mutual authentication method used for secure distributed NSCs association

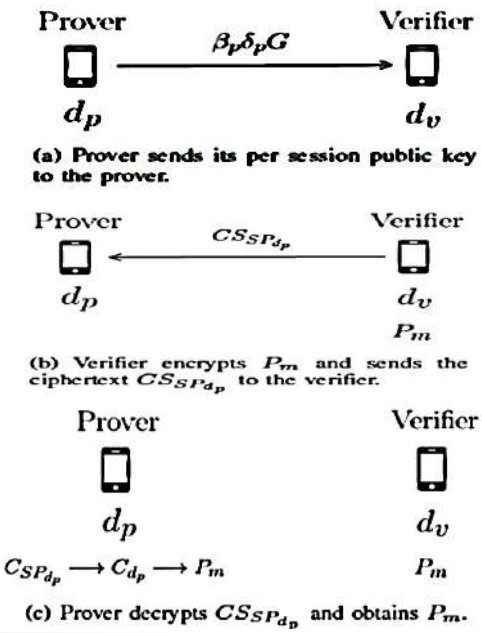
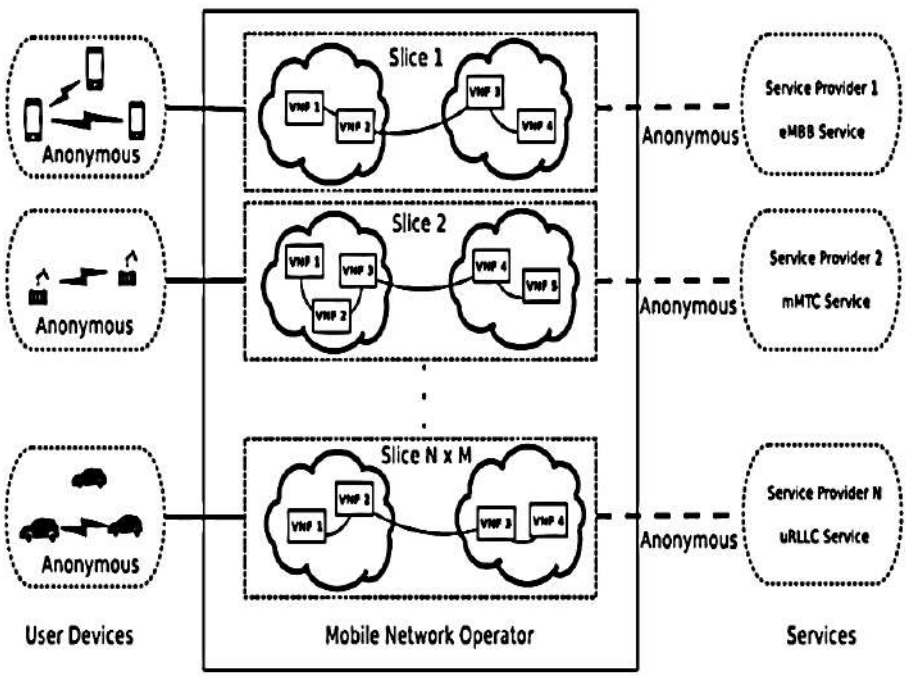


FIG. 2 shows the way in which the OR supplies re-encryption keys to NSCs of a slice for mutual authentication between them



CONTACT US
Dr. Dara Ajay, Head
Technology Transfer Office,
IPM Cell IC&SR, IIT Madras

IITM TTO Website:
https://ipm.icsr.in/ipm/

Email: smipm-icsr@icsrpis.iitm.ac.in
sm-marketing@imail.iitm.ac.in
Phone: +91-44-2257 9756/ 9719