



Telecommunications
Standards Development
Society, India

TECH DEEP DIVE

TTDD 2025 CONFERENCE (8th EDITION)

STANDARDISING 6G:

ARCHITECTING INTELLIGENT, SECURE AND SUSTAINABLE NETWORKS & SERVICES

 **Date:** 15-18 July 2025

Media Partner

COMMUNICATIONS TODAY

Session #4 - Security in a hyper connected world, especially for 6G

16 July 2025

<AI building resiliency for 6G >

by

<Dr Debabrata Nayak>, <Director telecom cyber security>

Potential to Transform Lives of 125 crore+ by 6G and AI

Healthcare



- Remote monitoring
- Telemedicine
- Remote surgery

Education



- Track objects, students, staff
- Instructional design
- AR/VR based lessons

Agriculture



- Monitoring crop yields, rainfall, pesticide, soil, etc.
- Environmental control

Safety



- Women and child safety
- Alarms and surveillance
- Connected cameras

Logistics



- Fleet management and optimization
- Navigation and fuel management

Financial Service



- Remote sales management
- Mobile point of sales

Power & Utilities



- Smart Meter, Smart Grid
- Facilities Management
- Equipment management

Automotive

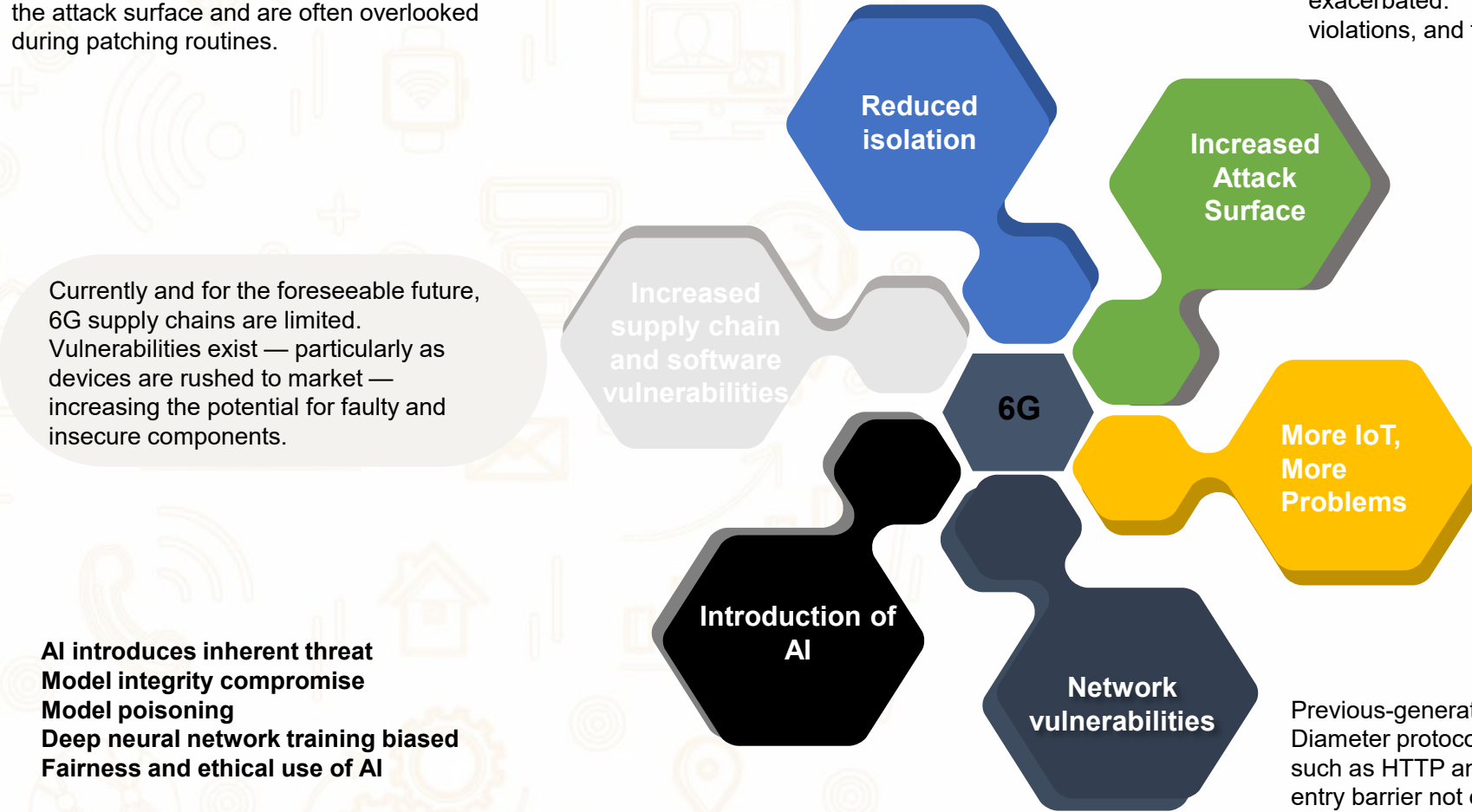


- Infotainment and positioning services
- In-car emergency systems
- Remote diagnostics

Security Risks around 6G

Network functions (NFs) previously performed by physical appliances are virtualized in 6G networks. NFs reduce network component isolation as NVFs communicate with each other directly and may share resources. Edge appliances in SD-WANs broaden the attack surface and are often overlooked during patching routines.

With millions and even billions more connected devices, 6G makes it possible for larger and more dangerous attacks. Current and future vulnerabilities of the existing internet infrastructure are only exacerbated. The risk of more sophisticated botnets, privacy violations, and faster data extraction can escalate with 6G



Previous-generation networks relied primarily on SS7 and Diameter protocols. 6G uses common internet protocols (IP) such as HTTP and TLS. These open-web protocols lower the entry barrier not only for operators but also for hackers

Examples of 5G security use cases

5G Network Slicing

- Security Isolation of Slices
- Privacy Violation Mitigation
- Slice Authentication and access controls
- End-to-end network segregation and interdependency protection
- Security for service based interfaces
- Control and Monitoring of Slice by a Service Provider

Cloud/ Virtualization Security

- Monitoring and control of the virtualized 5G network
- Virtualisation Isolation, and interdependency
- New Node integration or setup expansion
- Traffic segregation in virtualized network
- Verification of the Virtualized Node and the Virtualization Platform

Interworking and Roaming

- Interconnection security
- Roaming protection and secure handover
- Privacy in Context-Aware Services
- Authentication of New Network Elements
- Serving network authorization by the home network
- Restrict network exposure

User Equipment's Security

- Identity Management
- Authentication of IoT Devices in 5G
- Network-based Key Management for End-to-End Security
- Authorization for End-to-End IP Connections
- Enhanced Communication Privacy

Radio Interface Protection

- Unprotected User Plane on Radio Interface
- Air Interface security
- Rogue station prevention
- IoT/MIoT DDoS – RAN Resource Utilization
- Access Stratum Security
- Authentication - AKA Protection

Core Network Security

- Core interface security
- Backhaul link security
- Mobility Management
- MNO Identity Management Service
- Lawful Interception in a Dynamic 5G Network
- Denial-of-Service Protection

Examples of 5G security use cases

5G Network Slicing

- Security Isolation of Slices
- Privacy Violation Mitigation
- Slice Authentication and access controls
- End-to-end network segregation and interdependency protection
- Security for service based interfaces
- Control and Monitoring of Slice by a Service Provider

Cloud/ Virtualization Security

- Monitoring and control of the virtualized 5G network
- Virtualisation Isolation, and interdependency
- New Node integration or setup expansion
- Traffic segregation in virtualized network
- Verification of the Virtualized Node and the Virtualization Platform

Interworking and Roaming

- Interconnection security
- Roaming protection and secure handover
- Privacy in Context-Aware Services
- Authentication of New Network Elements
- Serving network authorization by the home network
- Restrict network exposure

User Equipment's Security

- Identity Management
- Authentication of IoT Devices in 5G
- Network-based Key Management for End-to-End Security
- Authorization for End-to-End IP Connections
- Enhanced Communication Privacy

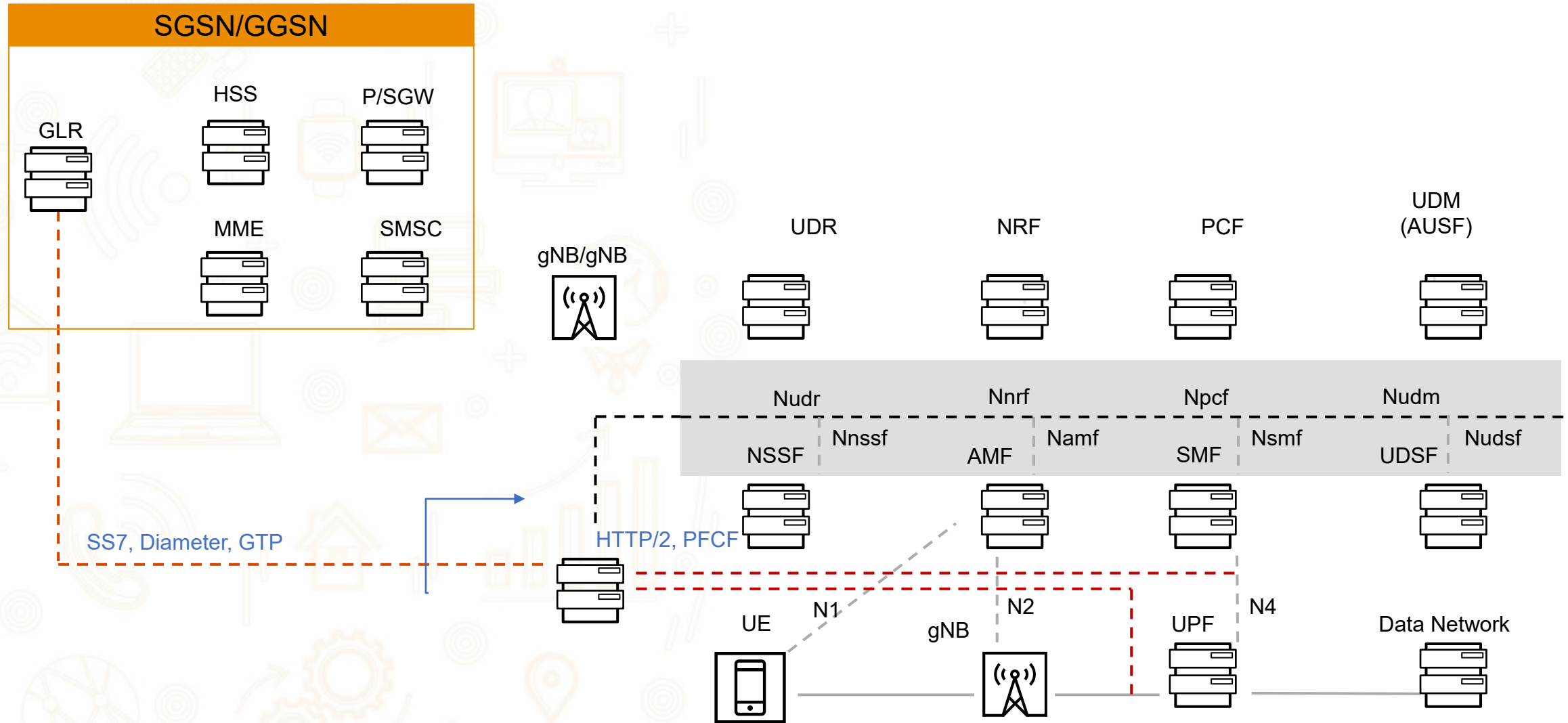
Radio Interface Protection

- Unprotected User Plane on Radio Interface
- Air Interface security
- Rogue station prevention
- IoT/MIoT DDoS – RAN Resource Utilization
- Access Stratum Security
- Authentication - AKA Protection

Core Network Security

- Core interface security
- Backhaul link security
- Mobility Management
- MNO Identity Management Service
- Lawful Interception in a Dynamic 5G Network
- Denial-of-Service Protection

Managed Security Service for both 5G NSA and 5G SA Core



Why Gen AI in 6G

1. Why Gen AI in Cyber Défense

2. Real-Life Transforming Use Cases

3. Case Studies



Why Gen AI in Cyber Defense

Gen AI Key Approach

- 24*7 automated threat hunting.
- Real-time action on alerts
- Behavioral Analysis
- Enhanced Useability and Availability

Traditional Reactive Defense

- Trouble in matching SLAs for action on critical and high alerts.
- Challenging 24*7 in-person monitoring.
- Manual analysis to detect false positive and true positive events.
- Hassles in impersonating each of the SIEM alerts throughout the clock.



Real-Time Transforming Use Cases

Transforming Approaches of Gen AI in Cyber Defense

- **Auto containment/isolation of possible breaches** – Proactive measure of responses after auto-detection of malware, and traffic from malicious sources or contain malicious payloads.
- **Auto-hunt the hidden APTs** – Though cross-correlate 10K logs/endpoints in near real-time, uncover Zero-day threats by behavioral analysis.
- **Patch smarter, not harder** – AI prioritizes critical vulnerability detection and auto-deployment of fixes.
- **Turn SIEM noise (alerts) into action** – by cutting false positives by 80% and auto-rank alerts by analyzing business risk.
- **Simulated stress test of defense mechanism** – AI-driven simulated attacks, based on outcomes provide the possible fixes blueprint.



Case Studies

Outcomes of Gen AI-based defense

- **Cloud Strike** AI slashes actionable triage time on detected mal-operation by 50%
- **Darktrace's** AI stops novel phishing (APT variant) attacks in real time.
- One of the Big4 consulting firms archives nearly 70% faster and more effective patching through the **NVIDIA** stack.

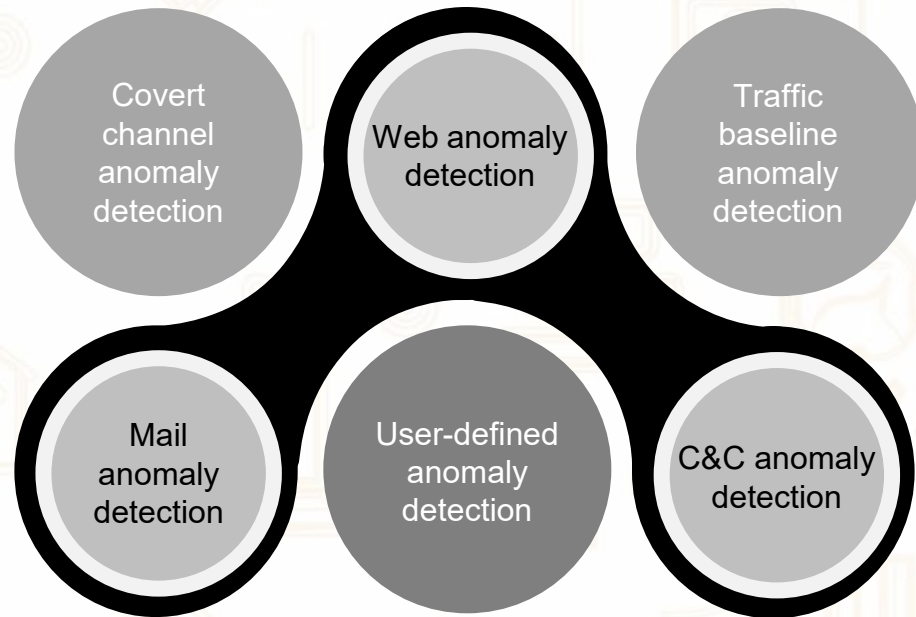
Why this matters now

- 59% of the enterprises are piloting Gen AI (2025 Data).
- The early adopters are achieving 2X faster responses to threats.
- In the era of AI-powered social engineering and threats, autonomous defense isn't an option - it's existential.



Security Analysis and Threat Detection on the AI Platform

Anomaly detection based on behaviour and content

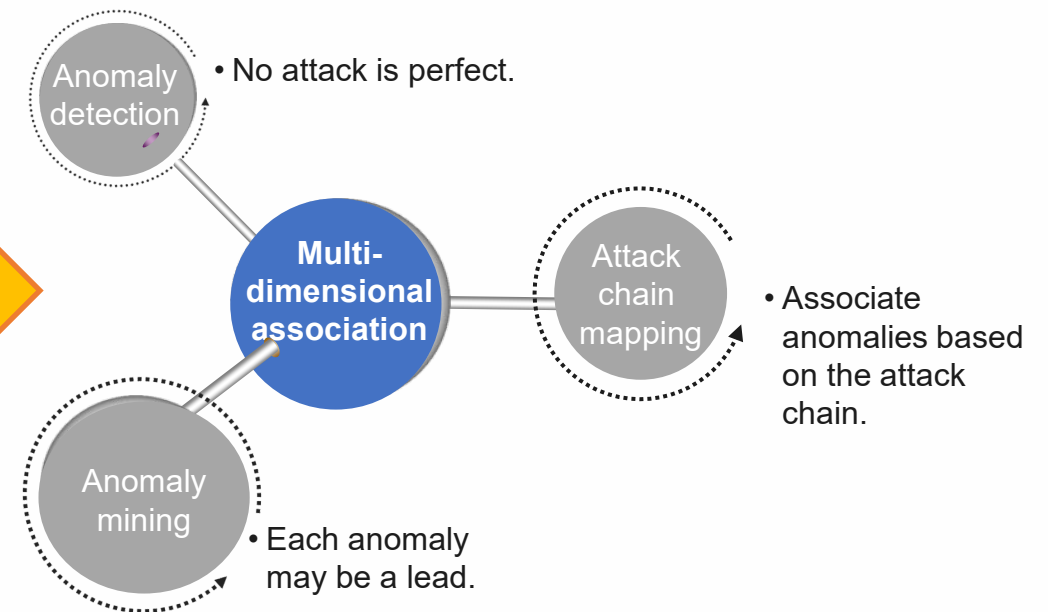


Number of abnormal behaviours that can be detected:
higher

Latency of intelligent search: shortest

Early warning: fastest

Anomaly correlation based on attack chains



Industry

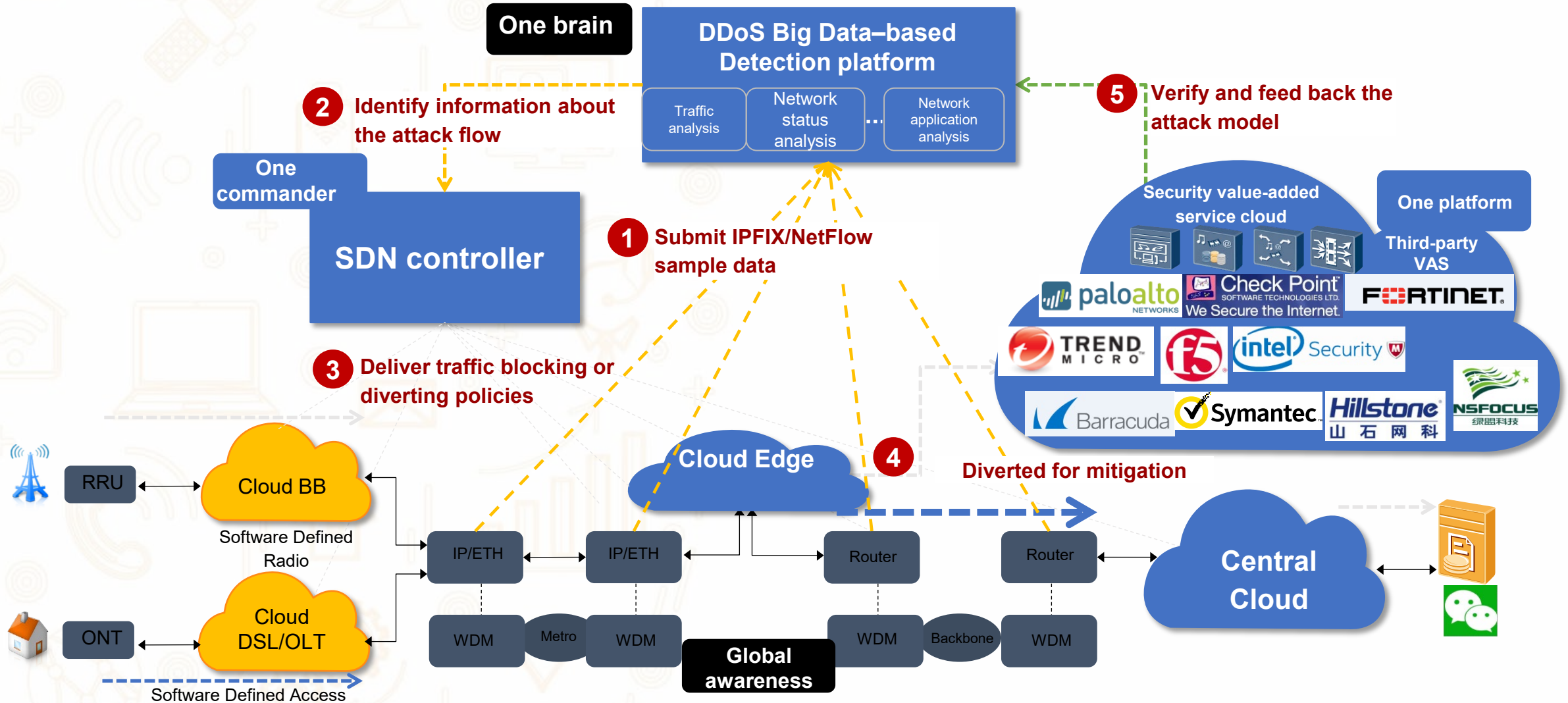
170+

Industry

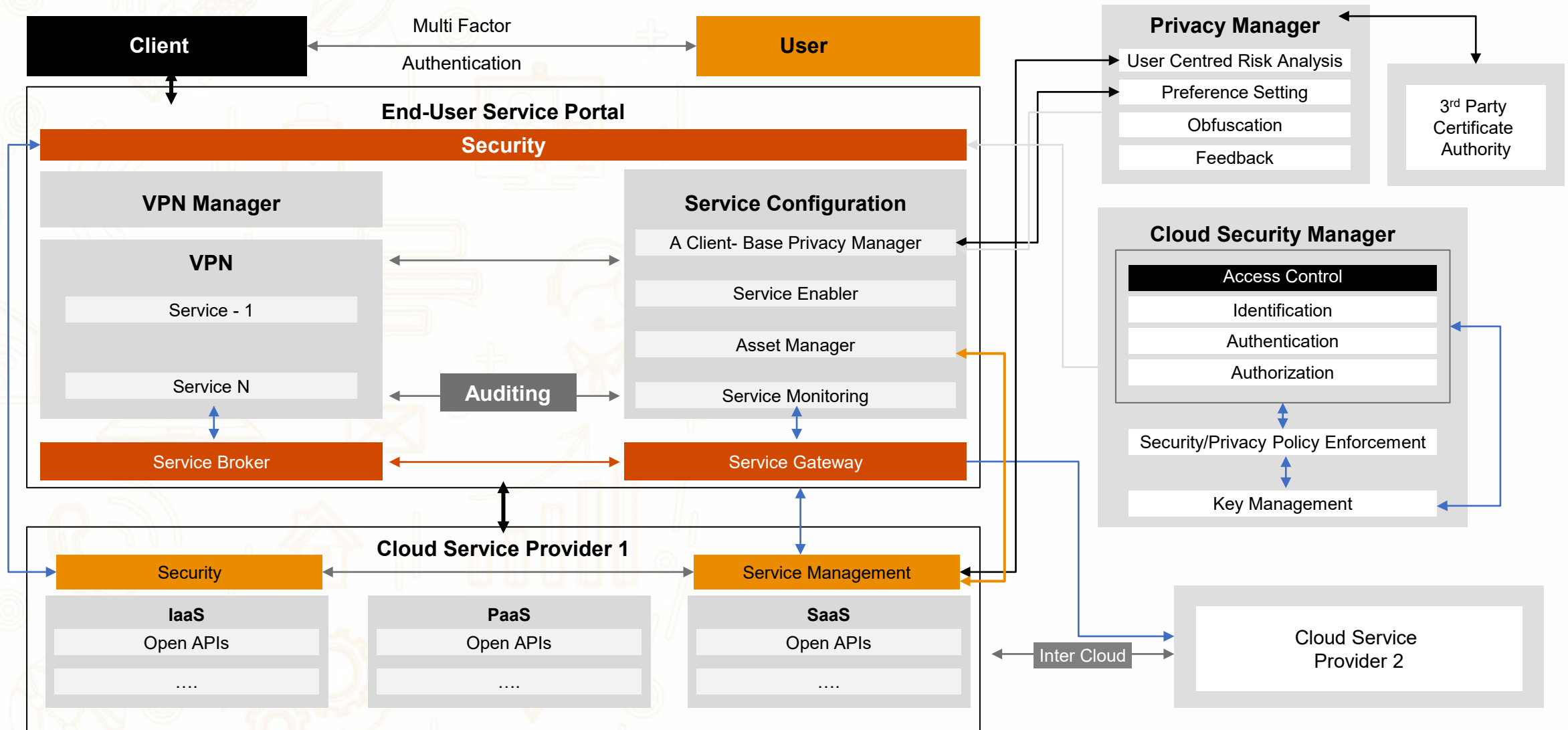
< 10s

Elastic scale-out of hundreds of devices is supported. AI-based analytics helps carriers and enterprise customers realize security posture awareness and implement optimal security defense policies.

Security Collection, Intelligent Analysis, Near-Source Scrubbing, and Flexible Connection for 6G



Cloud Security Framework envision for 6G

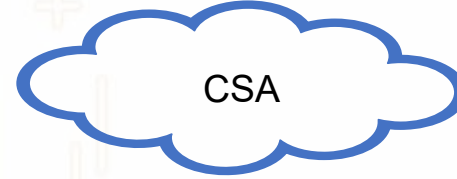


Conclusion

- Integration of AI and Machine Learning in 6G
- Distributed architecture for poisoning attack
- Early isolation of malicious parts
- Preserving privacy while retaining model integrity
- Implementing Zero Trust based Architecture
- Deep neural network training

Standard Bodies Referenced/followed

NIST



tsdsi
India's Telecom SDO

ARIB



Thank You
<Debabrata.nayak@pwc.com>