CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY
An Autonomous Institute | Affiliated to Osmania University
Kokapet Village, Gandipet Mandal, Hyderabad, Telangana-500075, www.cbit.ac.in
Approved by | Affiliated to | UGC Autonomous | 12 Programs Accredited by NBA | Grade A++ in NAAC | All India Ranking 151-200 Band nirf | Certified by ISO 21001 : 2018
COMMITTED TO RESEARCH, INNOVATION AND EDUCATION
47 years

Department of Computer Engineering & Technology

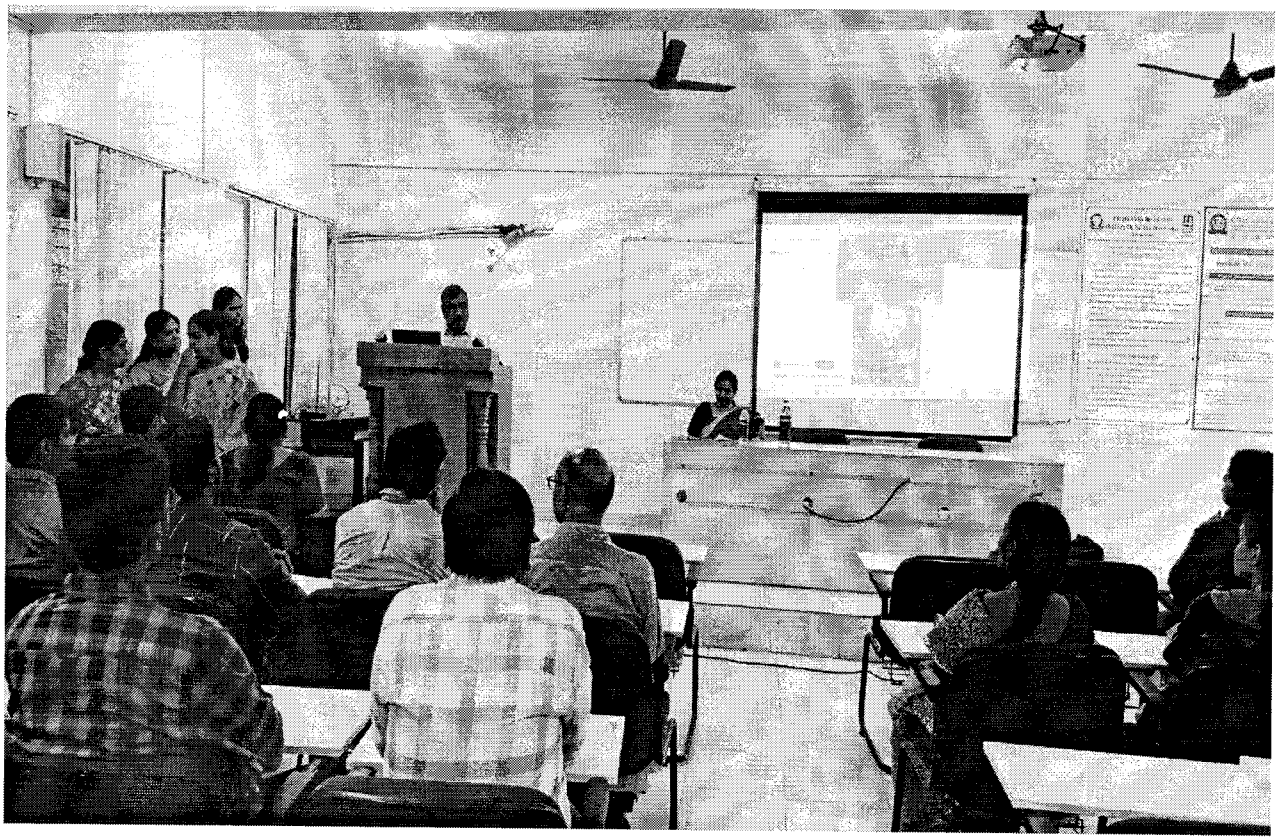
One Week National Level Faculty Development Programme

on

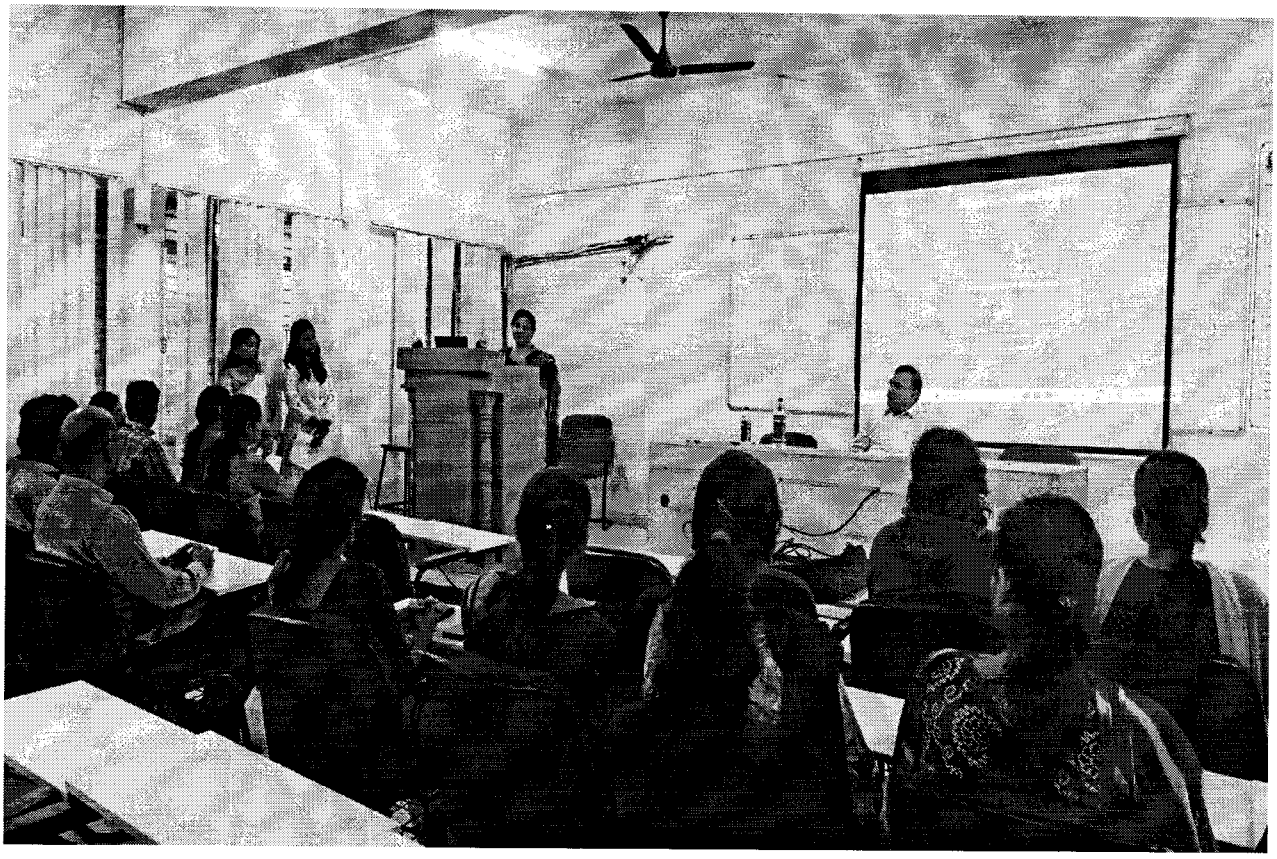
Integrating Quantum Computing in Emerging Technologies

Inaugural of FDP

Date/Time: 05/01/2026; 9:15 AM – 9:30 AM



The Inaugural session of the FDP was graced by the Honorable Principal Prof. C.V. Narasimhulu and addressed the gathering with a insightful words.



The Head of the Department Dr. Sangeeta Gupta addressed the gathering, highlighting the relevance of the FDP.

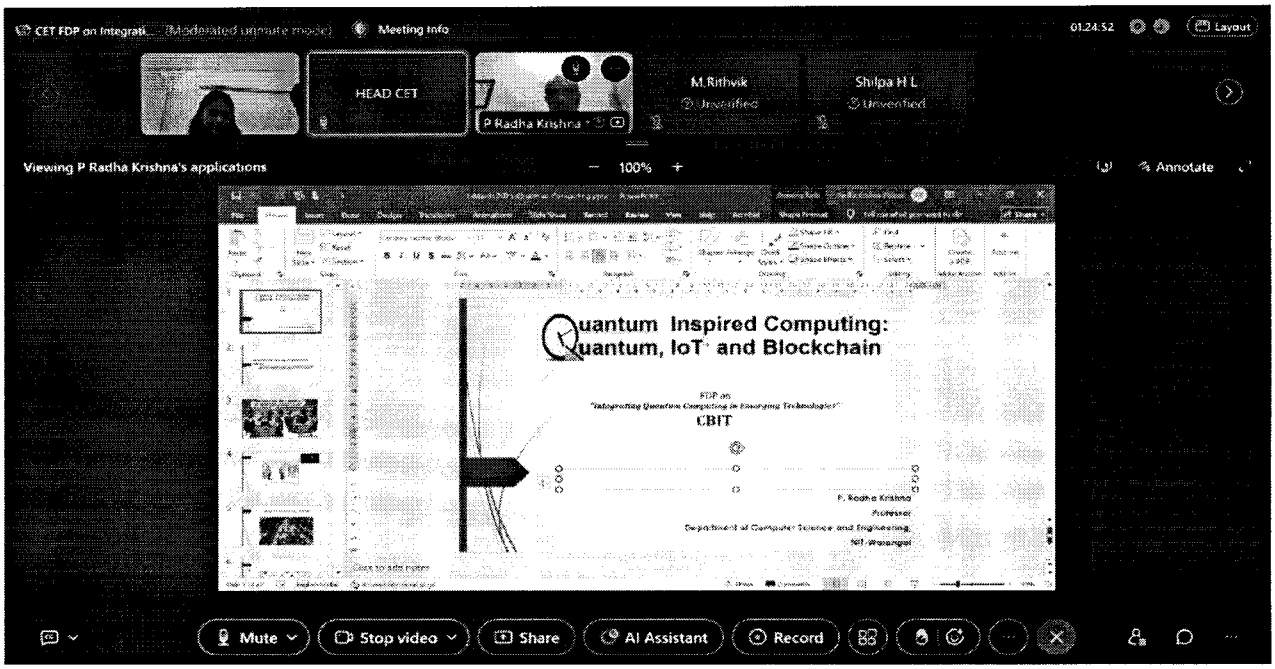
SESSION 1

Date/Time: 05/01/2026; 9:30 AM – 11:00 AM

Resource Person: Prof. P. Radhakrishna, Dean, NIT Warangal

Topic for the session: Introduction to Emerging Technologies (Keynote Address).

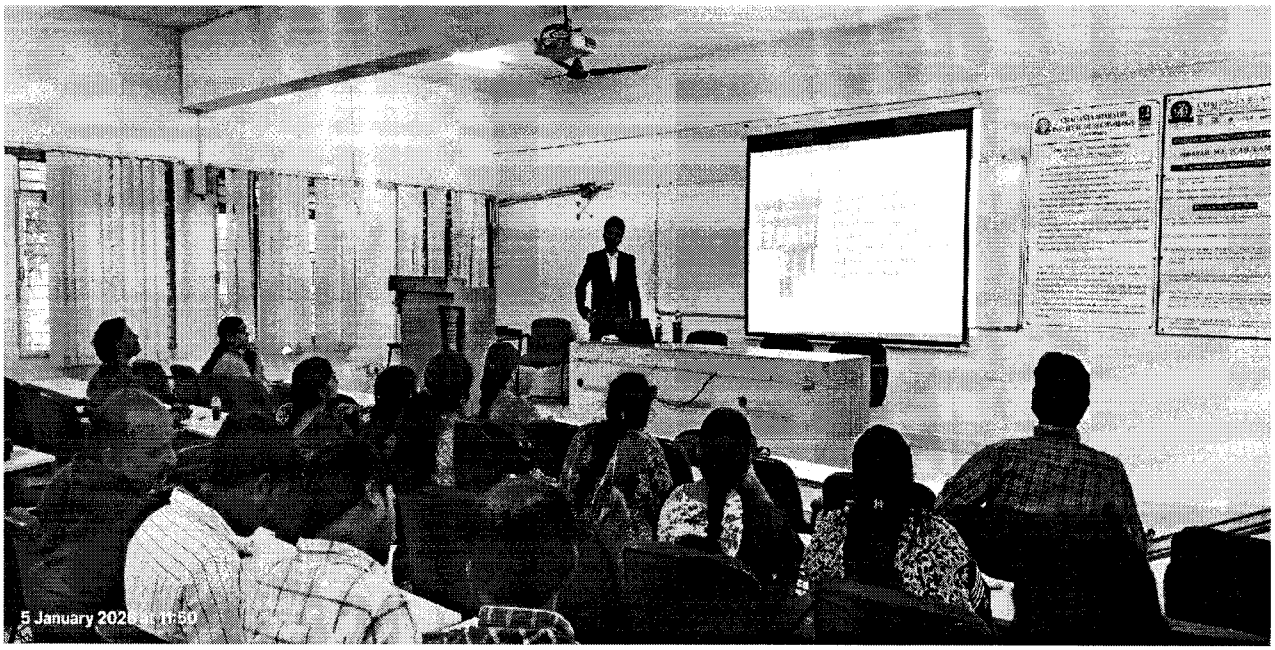
Prof. P. Radhakrishna, Dean at NIT Warangal, delivered a compelling keynote address that set the foundation for the entire program. He provided a comprehensive overview of how quantum computing integrates with IoT, AI, blockchain, and cybersecurity to drive revolutionary changes across industries like healthcare, finance, transportation, and smart cities. The speaker emphasized practical real-world examples such as quantum-enhanced drug discovery, secure financial transactions, and intelligent traffic management systems. He also addressed key challenges including error rates in current quantum hardware, the need for hybrid quantum-classical systems, and workforce skilling requirements. Participants gained a clear strategic vision of quantum technology's transformative potential over the next decade.



SESSION 2

Date/Time: 05/01/2026; 11:15 AM – 12:45 PM
Resource Person: Dr. B. Venkata Raman, IIIT Basara

Topic for the session: Introduction to Quantum Computing along with Qiskit 2.0 & Introduction to Machine Learning.



Dr. B. Venkata Raman from IIIT Basara delivered an enlightening session on Introduction to Quantum Computing with Qiskit 2.0 and Machine Learning fundamentals. He explained qubits, superposition, entanglement, and quantum gates alongside Qiskit installation and basic circuits. ML concepts like supervised learning were linked to quantum advantages in optimization. A live Qiskit demo helped participants grasp practical quantum-ML integration.

SESSION 3

Date/Time: 05/01/2026; 1:30 PM – 3:30 PM
Resource Person: Dr. B. Venkata Raman, IIIT Basara

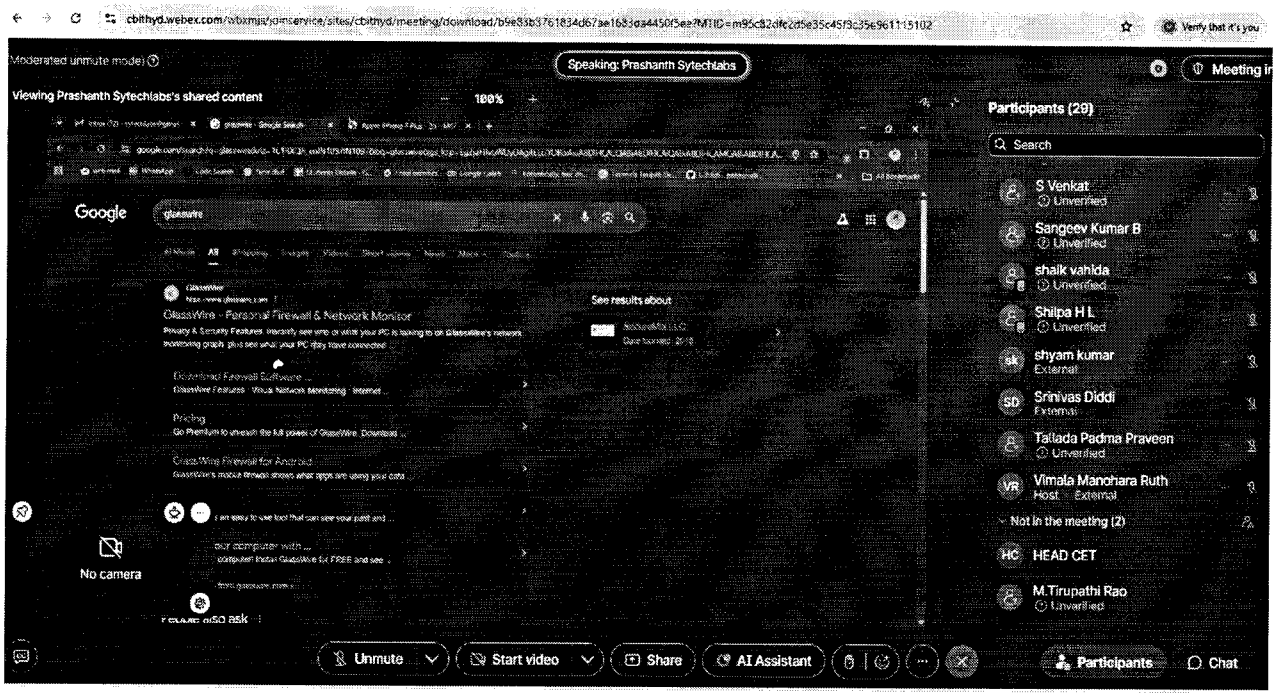
Topic for the session: Hands-on Session on Classification using Quantum Computing

Dr. B. Venkata Raman conducted an intensive hands-on laboratory session where participants implemented quantum machine learning algorithms using real quantum hardware access. Attendees built quantum support vector machines and variational quantum classifiers from scratch, encoding classical datasets into quantum states through amplitude encoding techniques. The session covered feature mapping to quantum kernels, optimization using classical-quantum hybrid loops, and measurement-based classification. Real-time debugging of quantum circuits and interpretation of probabilistic measurement outcomes were practiced extensively. Participants left with working Jupyter notebooks demonstrating quantum advantage in classification tasks over classical baselines.

SESSION 4

Date/Time: 06/01/2026; 9:30 AM – 11:00 AM
Resource Person: Mr. Prashanth, Manager, Sytech Labs, Cyber Crime Analyst & Forensic Investigator

Topic for the session: Basics of Cybersecurity for IoT in the Quantum Era



Mr. Prashanth from Sytech Labs provided an in-depth analysis of IoT cybersecurity challenges specifically vulnerable to quantum computing threats. He detailed how Shor's algorithm can efficiently factor large numbers breaking RSA and ECC encryption widely used in IoT device authentication. The session covered quantum threat modeling including harvest now decrypt later attacks where adversaries store encrypted IoT traffic for future quantum decryption. Current cryptographic inventories in typical IoT deployments were assessed with migration roadmaps to quantum-safe alternatives. Real case studies of quantum-vulnerable IoT botnets and smart home breaches illustrated the urgency of proactive security transformations.

SESSION 5

Date/Time: 06/01/2026; 11:15 AM – 12:45 PM

Resource Person: Mr. Prashanth, Manager, Sytech Labs

Topic for the session: Common Cyber Attacks on IoT & Blockchain Systems

Mr. Prashanth conducted a thorough examination of the most prevalent attack vectors targeting IoT ecosystems and blockchain networks. He dissected Mirai-style botnet infections, MQTT protocol exploits, and Zigbee network hijacking with live packet captures. Blockchain-specific threats including double-spend attempts, smart contract reentrancy vulnerabilities like the DAO hack, and 51% attacks on proof-of-work chains were analyzed deeply. Attendees learned forensic investigation techniques for compromised IoT firmware and blockchain transaction tracing. Comprehensive defense frameworks combining network segmentation, behavioral anomaly detection, and decentralized identity management were presented with implementation checklists.

SESSION 6

Date/Time: 06/01/2026 ; 1:30 PM – 3:30 PM

Resource Person: Mr. Prashanth, Manager, Sytech Labs

Topic for the session: Introduction to Quantum-Safe Security: Protecting IoT and Blockchain from Future Quantum Threats

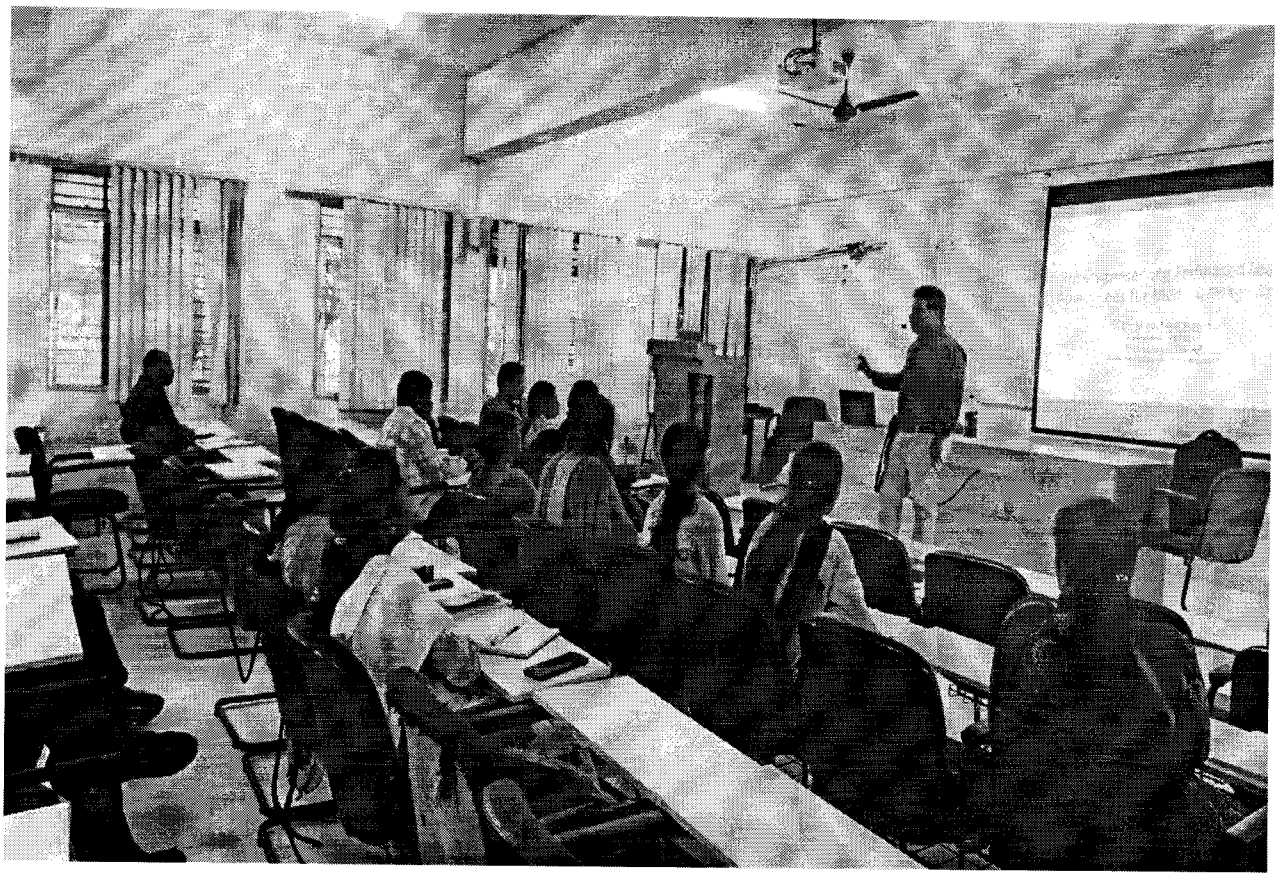
Mr. Prashanth delivered an authoritative session on NIST-standardized post-quantum cryptographic algorithms ready for IoT and blockchain deployment. Detailed comparisons of lattice-based Kyber for key encapsulation, Dilithium for digital signatures, and hash-based SPHINCS+ were presented with performance benchmarks on resource-constrained devices. Quantum key distribution protocols using BB84 and device-independent schemes were explained with practical QKD network topologies. Hybrid cryptography schemes combining classical and post-quantum algorithms for backward compatibility were demonstrated. The session included crypto-agility architecture design principles essential for long-term security resilience.

SESSION 7

Date/Time: 07/01/2026; 9:30 AM – 11:00 AM

Resource Person: Dr. M. Mahesh Kumar, Assistant Professor, SRM University

Topic for the session: Privacy-Preserving Federated Learning Approaches for Collaborative Medical Image Analysis



Dr. M. Mahesh Kumar from SRM University presented cutting-edge federated learning techniques specifically optimized for collaborative medical imaging across distributed hospitals. He demonstrated differential privacy mechanisms adding calibrated noise to gradient updates preventing individual patient data reconstruction. Secure multi-party computation protocols enabled model aggregation without exposing raw medical scans. Real chest X-ray and MRI datasets showed federated models achieving comparable accuracy to centralized training while guaranteeing regulatory compliance. Quantum neural network enhancements for federated optimization were explored as future research directions.

SESSION 8

Date/Time: 07/01/2026; 11:15 AM – 12:45 PM
Resource Person: Dr. M. Mahesh Kumar, Assistant Professor, SRM University

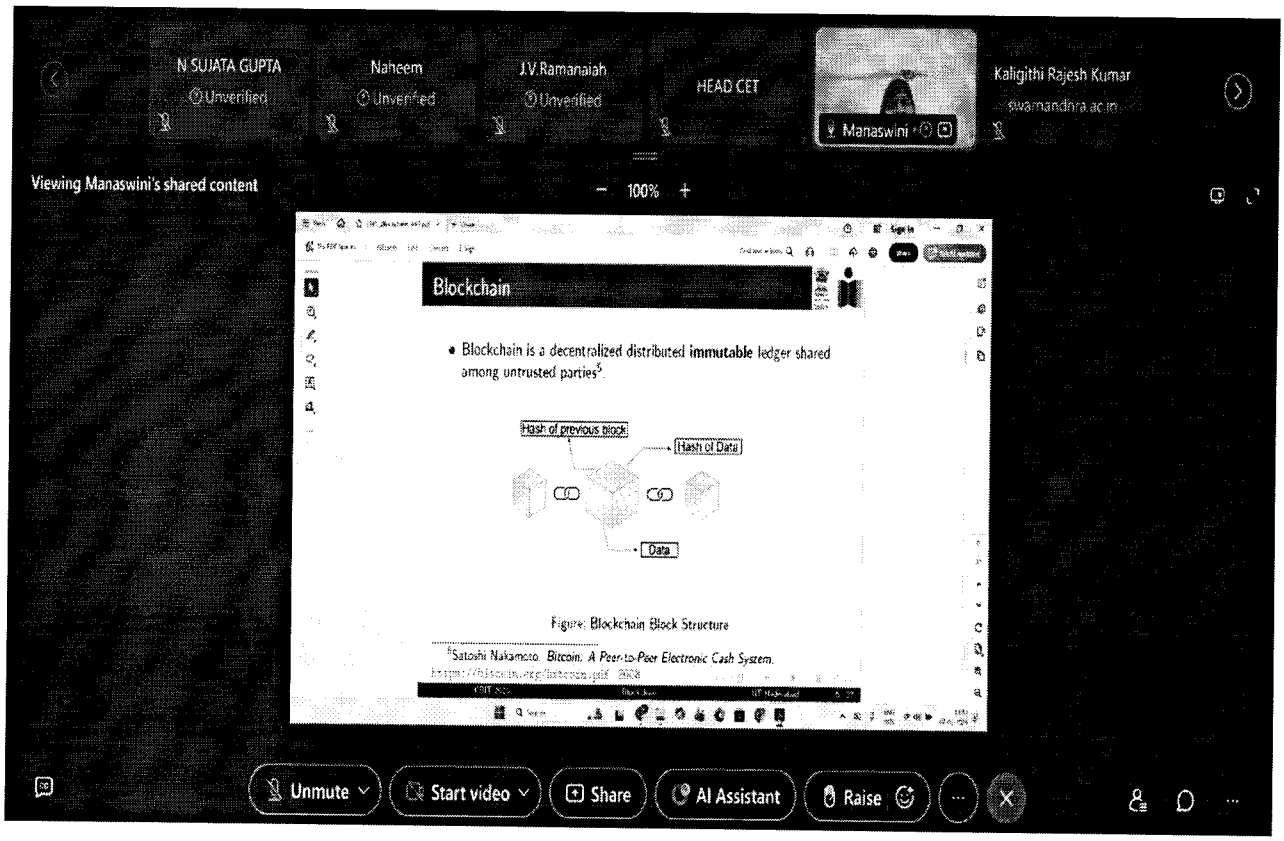
Topic for the session: Privacy-Preserving Biometric Authentication

Dr. M. Mahesh Kumar detailed advanced biometric protection schemes using homomorphic encryption allowing computations on encrypted fingerprint and iris templates. Zero-knowledge proof protocols verified biometric authenticity without revealing template details to service providers. Quantum-resistant fuzzy extractors generated stable cryptographic keys from noisy biometric readings. Multi-modal fusion architectures combining face, voice, and behavioral biometrics achieved high accuracy with strong privacy guarantees. The session included template protection against hill-climbing and cross-matching attacks prevalent in centralized biometric databases.

SESSION 9

Date/Time: 07/01/2026; 1:30 PM – 3:30 PM
Resource Person: Ms. Manaswini, IIT Hyderabad

Topic for the session: Advanced Topics in Privacy and Secure AI Systems

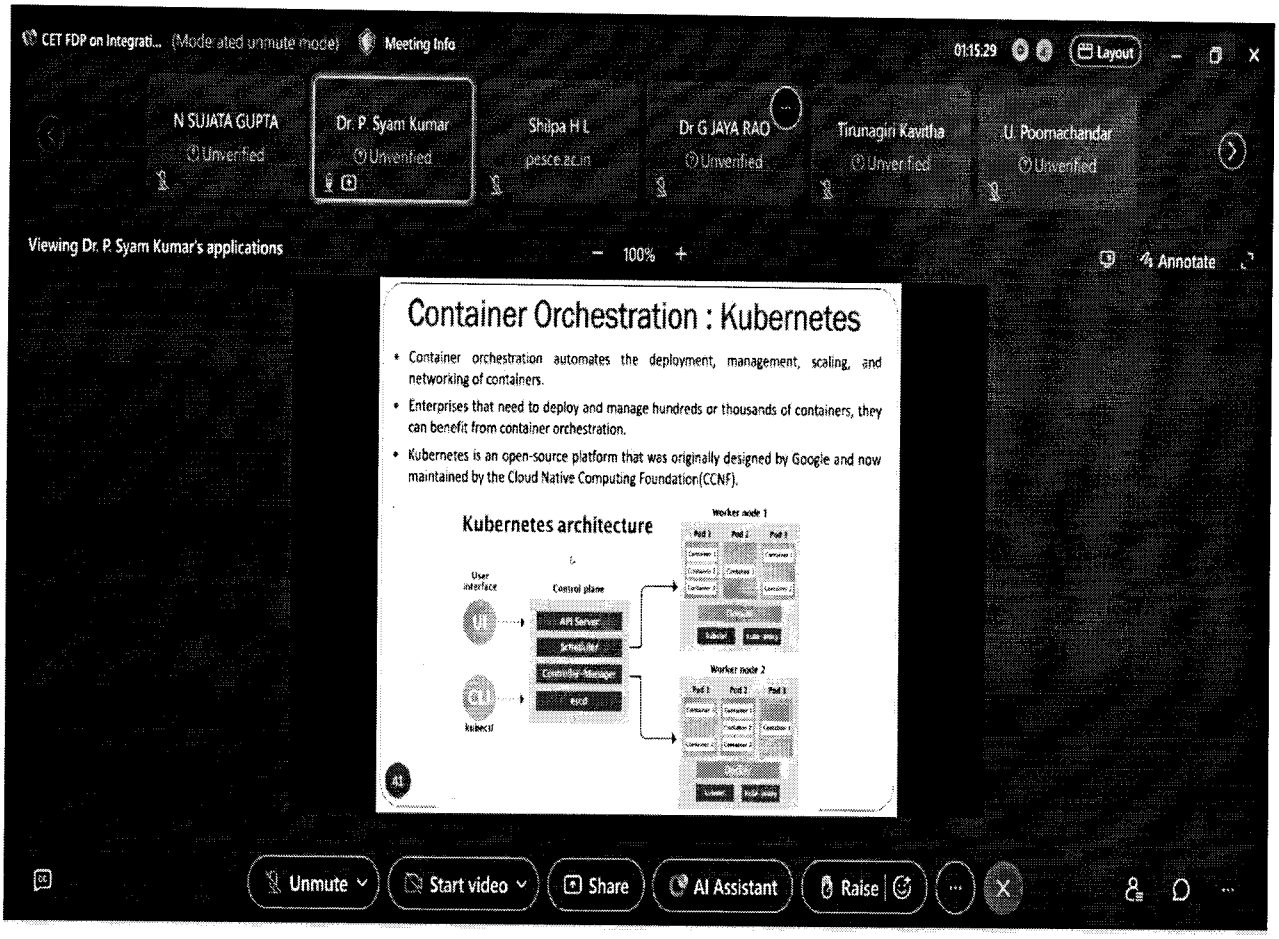


Ms. Manaswini from IIT Hyderabad delivered a sophisticated treatment of secure AI systems incorporating quantum-resistant multiparty computation and confidential computing. Intel SGX and AWS Nitro Enclaves were demonstrated for trusted execution environments protecting AI model inference. Differential privacy libraries and secure aggregation protocols for federated analytics were implemented live. Quantum side-channel attacks on AI hardware accelerators were analyzed with countermeasures including constant-time implementations and masking techniques. The session bridged theoretical cryptography with practical secure AI deployment strategies.

SESSION 10

Date/Time: 08/01/2026; 9:30 AM – 11:00 AM
Resource Person: Dr. P. Syam Kumar

Topic for the session: Containerization



Dr. P. Syam Kumar provided expert guidance on containerization technologies optimized for quantum computing workloads and hybrid classical-quantum applications. Docker security best practices including non-root containers, image vulnerability scanning with Trivy, and runtime protection using Falco were thoroughly covered. Kubernetes orchestration for scalable quantum circuit execution across multi-cloud environments was demonstrated. Service mesh architectures with Istio provided zero-trust networking essential for quantum data pipelines. Participants deployed production-ready containerized Qiskit environments with comprehensive security hardening.

SESSION 11

Date/Time: 08/01/2026; 11:15 AM – 12:45 PM
Resource Person: Dr. P. Syam Kumar

Topic for the session: Cloud Security

Dr. P. Syam Kumar explored comprehensive cloud security architectures designed for quantum-integrated computing platforms. Zero-trust identity frameworks using OAuth 2.0 with mTLS ensured fine-grained access control for quantum resources. Network micro-segmentation with service mesh and eBPF-based observability provided defense-in-depth. Quantum key distribution integration with cloud HSMs established information-theoretic secure communication channels. Compliance frameworks including SOC2, ISO27001, and quantum-ready FedRAMP requirements were mapped to technical controls with implementation templates.

SESSION 12

Date/Time: 08/01/2026; 1:30 PM – 3:30 PM
Resource Person: Dr. P. Syam Kumar

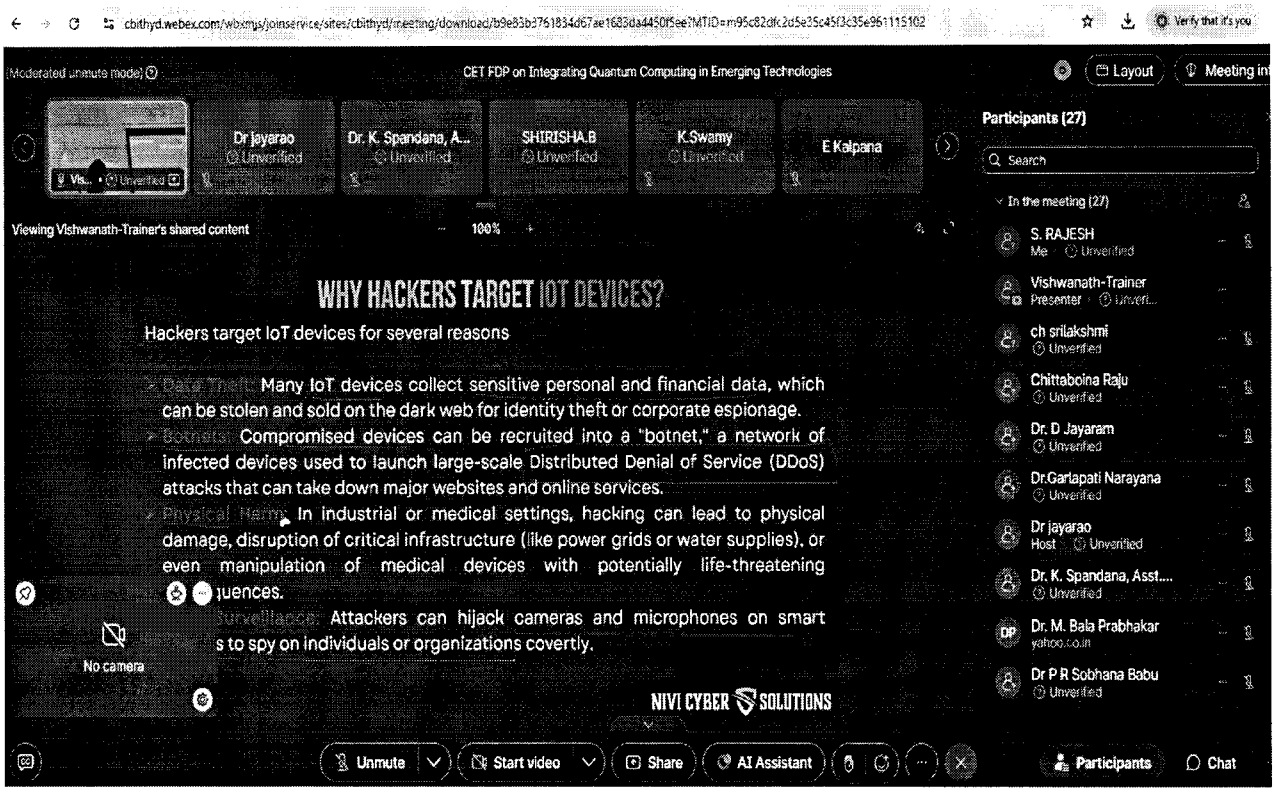
Topic for the session: Post-Quantum Cryptography

Dr. P. Syam Kumar delivered an exhaustive survey of NIST PQC standardization finalists and alternate candidates. Detailed performance analysis compared CRYSTALS-Kyber, SABER, NTRU for key encapsulation against FrodoKEM. Dilithium, Falcon, and SPHINCS+ digital signature schemes were benchmarked across speed, signature size, and security levels. Side-channel resistance evaluations and constant-time implementations were demonstrated. Comprehensive migration strategies from classical PKI to quantum-safe certificate authorities were outlined with enterprise deployment playbooks.

SESSION 13

Date/Time: 09/01/2026; 9:30 AM – 11:00 AM
Resource Person: Mr. Chinthakundi Vishwanath, CEO, Nivi Cyber Solutions & Ethical Hacker

Topic for the session: IoT Hardware Hacking – Attacks, Demonstrations & Defense



Mr. Chinthakundi Vishwanath executed live hardware hacking demonstrations on commercial IoT devices revealing JTAG debug interfaces, UART backdoors, and firmware extraction techniques. Power analysis and electromagnetic side-channel attacks recovered AES keys from IoT chipsets. Rowhammer and glitch attacks bypassed hardware root-of-trust mechanisms. Quantum-resistant hardware security modules using Physically Unclonable Functions provided defense-in-depth. Secure boot chains and remote attestation protocols ensured device integrity throughout deployment lifecycle.

SESSION 14

Date/Time: 09/01/2026; 11:15 AM – 12:45 PM
Resource Person: Mr. Chinthakundi Vishwanath

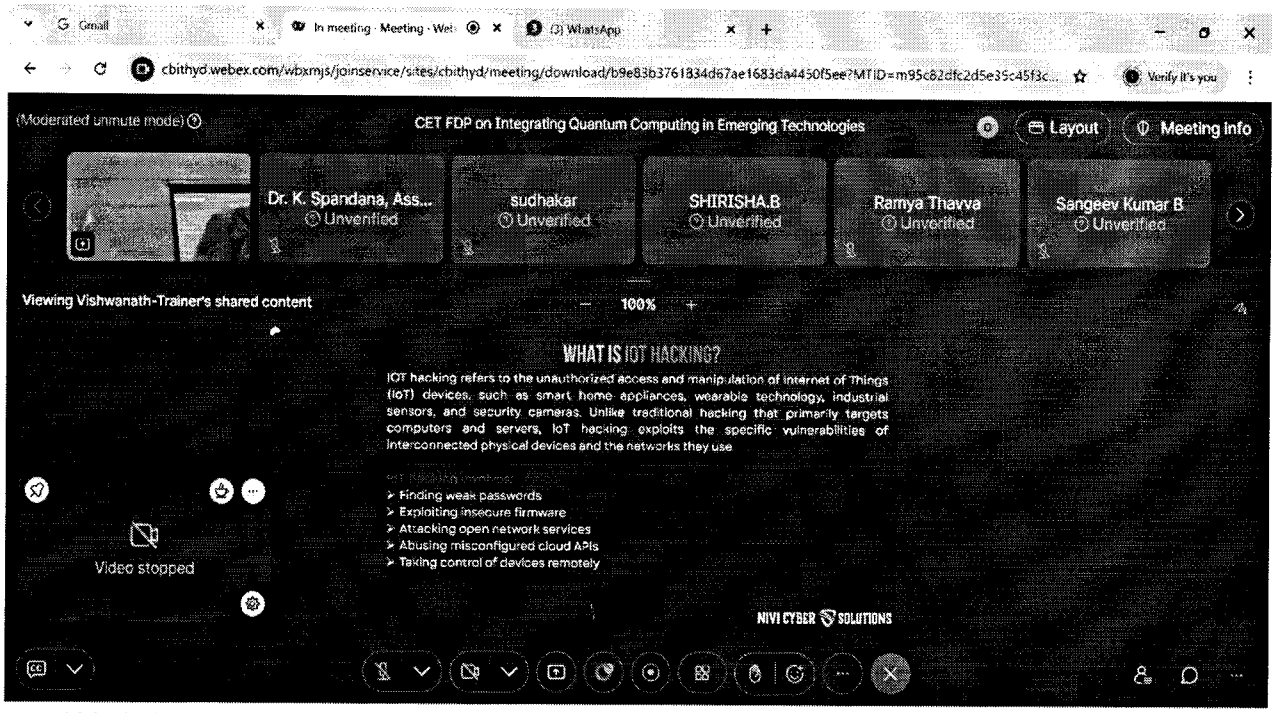
Topic for the session: Mobile Hacking, USB Attacks & Dark Web Awareness

Mr. Chinthakundi Vishwanath demonstrated advanced mobile exploitation chains combining social engineering with zero-click vulnerabilities. USB Rubber Ducky and BadUSB attacks delivered persistent backdoors through HID emulation. Dark web OSINT techniques mapped threat actor infrastructure and credential markets. Endpoint detection and response platforms using ML behavioral analytics countered advanced persistent threats. Secure coding standards and input validation frameworks prevented common mobile vulnerabilities exploited in supply chain attacks.

SESSION 15

Date/Time: 09/01/2026 ; 1:30 PM – 3:30 PM
Resource Person: Mr. Chinthakundi Vishwanath

Topic for the session: Cybersecurity with Quantum Computing – Present & Future & Hands-on Practicals with Hardware-Level Devices

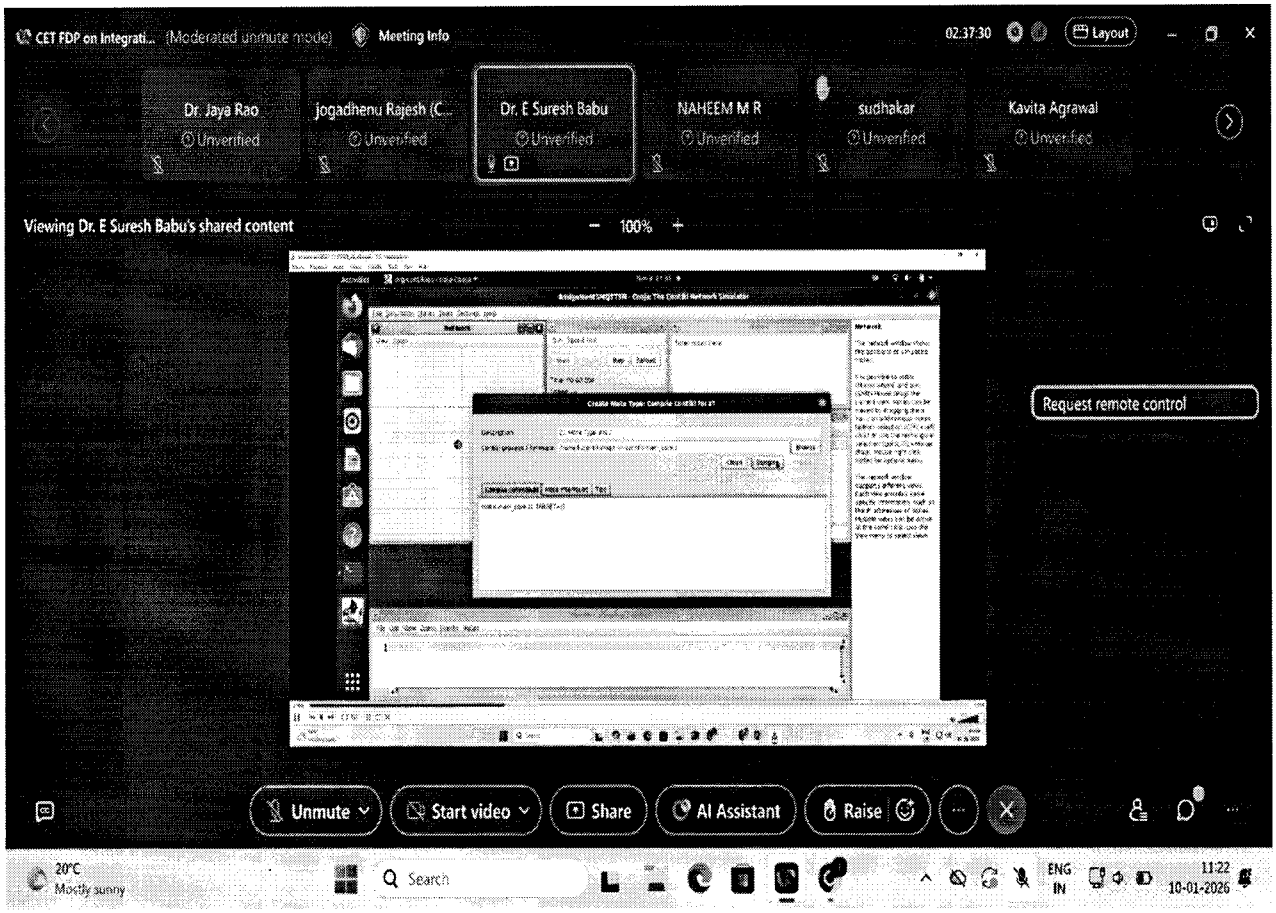


Mr. Chinthakundi Vishwanath conducted extensive hands-on laboratories using actual quantum hardware and photonics testbeds. Grover's algorithm implementations demonstrated quadratic speedup in database search relevant to cybersecurity monitoring. Shor's algorithm factored realistic RSA moduli on NISQ devices revealing encryption timeline pressures. Quantum random number generators enhanced cryptographic key material entropy. Future fault-tolerant quantum cybersecurity applications including quantum honeypots and provably secure multiparty computation were prototyped live.

SESSION 16

Date/Time: 10/01/2026; 9:30 AM – 11:00 AM
Resource Person: Mr. Suresh Babu, NIT Warangal

Topic for the session: The Role of AI and Blockchain in IoT

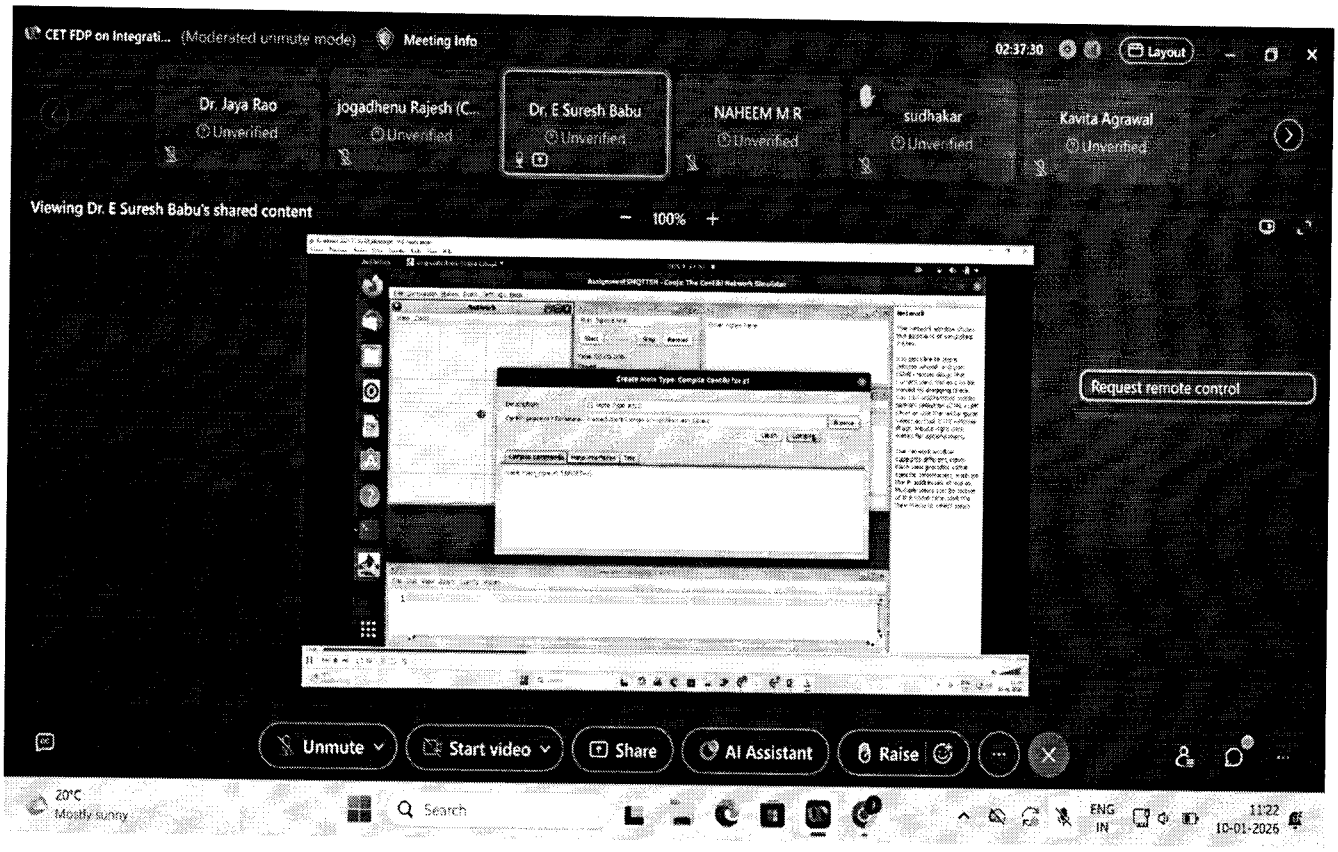


Mr. Suresh Babu from NIT Warangal analyzed sophisticated AI-blockchain integration patterns enhancing IoT ecosystem resilience. Decentralized AI inference using blockchain oracles provided tamper-proof data feeds for edge analytics. Smart contract auto-execution triggered by AI anomaly detection enabled autonomous incident response. Quantum-secure threshold signature schemes protected multi-party IoT data aggregation. Zero-knowledge proofs verified AI model training integrity without exposing proprietary datasets.

SESSION 17

Date/Time: 10/01/2026 ; 11:15 AM – 12:45 PM
Resource Person: Mr. Suresh Babu, NIT Warangal

Topic for the session: A Trust-Aware Multi-Tier DDoS Detection Architecture for IoT Networks Using Blockchain



Mr. Suresh Babu presented his patented blockchain-based DDoS mitigation framework with hierarchical trust scoring across IoT edge, fog, and cloud tiers. Practical Byzantine Fault Tolerance consensus optimized for intermittent IoT connectivity achieved sub-second detection latency. Sharding and state channels minimized blockchain storage overhead for high-velocity attack telemetry. Reinforcement learning agents dynamically adjusted detection thresholds based on real-time threat intelligence. Live simulations validated 99.8% detection accuracy against volumetric and application-layer DDoS.

SESSION 18

Date/Time: 10/01/2026; 1:30 PM – 3:30 PM

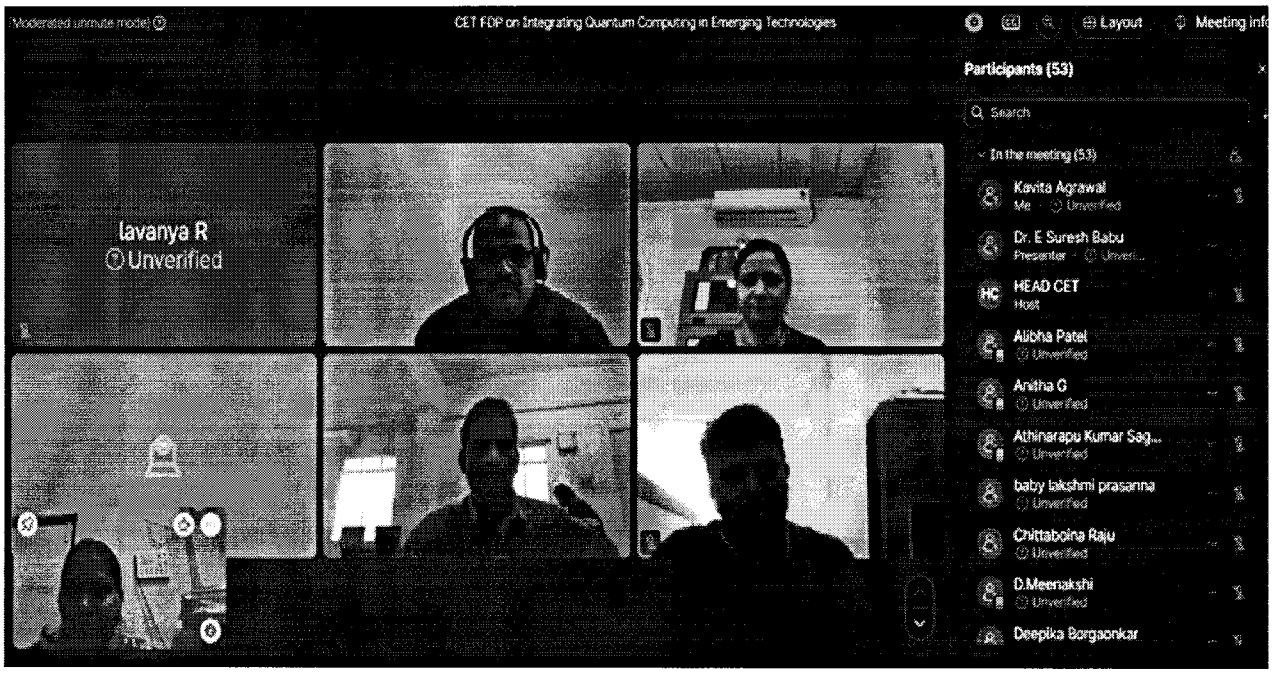
Resource Person: Mr. Suresh Babu, NIT Warangal

Topic for the session: DDoS Attacks in IoT Networks

Mr. Suresh Babu provided exhaustive analysis of IoT-specific DDoS attack amplification techniques exploiting Memcached, DNS, and NTP protocols. Botnet C2 architectures using Tor and I2P were reverse-engineered revealing persistence mechanisms. Machine learning classifiers distinguished flash crowds from malicious floods using flow statistics and packet entropy. Blockchain-based collaborative threat intelligence sharing accelerated global blacklist propagation. Quantum-enhanced anomaly detection leveraging Grover search identified zero-day attack signatures in real-time across distributed IoT deployments.

VALEDICTORY

Date/Time: 10/01/2026; 3 PM - 4:00 PM



The Valedictory Session of the One Week National Level Faculty Development Programme on "Integrating Quantum Computing in Emerging Technologies" was conducted on 10th January 2026, organized by the Department of Computer Engineering and Technology, Chaitanya Bharathi Institute of Technology (Autonomous), Hyderabad.

The session commenced with a brief welcome, followed by a comprehensive summary of the FDP, highlighting the objectives, day-wise technical sessions, and key outcomes of the programme. The valedictory address emphasized the relevance of quantum computing and its integration with emerging technologies, encouraging participants to continue exploring and applying the knowledge gained in their academic and research activities.

Participants shared their feedback during the session and expressed their appreciation for the well-structured sessions, technical depth, and effective delivery by the resource persons. The programme witnessed active participation throughout the week, benefiting a total of 99 participants from Telangana and other states, making it truly national in scope.

The session concluded with a formal vote of thanks, acknowledging the efforts of the management, Principal, Head of the Department, resource persons, coordinators, student volunteers, and support staff for their contributions to the successful conduct of the FDP. The FDP concluded on a successful and enthusiastic note, marking a meaningful academic engagement for all involved.

Head of the Department
Dept. of Computer Engineering and Tech.
CBIT(A), Gandipet, Hyderabad-50...

HoD, Dept. of CET