

# ***Report of Faculty Development Programme***

---

*Recent Trends and Future Directions in  
Information Security*

Organized by

Computer Engineering Department, L.D. College of Engineering

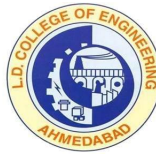
21-Mar-2022 to 26-Mar-2022

**Patron:** Dr. Rajul Gajjar

**Convener:** Dr. Sanjay Shah

**University coordinator:** Dr. Sarika Srivastava

**Programme coordinators:** Dr. Jay Dave, Dr. Nikunj Domadiya



## Day 1 (21-Mar-2022)

---

### **Session 1: Inaugural Function (11:00 to 12:00)**

*Summary:* The inaugural ceremony of the Faculty Development Programme on “Recent Trends and Future Directions in Information Security” commenced with virtually lighting of lamps followed by Saraswati-Vandana. Dr. Jay Dave (Program Coordinator) formally welcomed Principal - Dr. Rajul Gajjar madam, Head of Department - Dr. Sanjay Shah sir, and participants. He discussed the significance of Information Security. He stated that "Businesses, governments, and individuals around the world rely on the expertise and innovations of information security specialists, without which global communications systems would grind to a halt."

Dr. Sanjay Shah briefed about the sessions and our esteemed resource persons. He encouraged the participants to gain knowledge as much as possible by attending all sessions and discussing your queries with our experts. Dr. Rajul Gajjar briefed about research activities going on at LDCE. She wished for the success of the FDP and inspired the participants.

Dr. Jay Dave offered a vote of thanks to all including Dr. Rajul Gajjar (Principal, LDCE) and Dr. Sanjay Shah (HoD, Computer Engineering, LDCE). He thanked all the invited guests and participants for gracing the occasion by their solemn presence. He also thanked AICTE and GTU for providing all kind of support to conduct such FDP.

### **Session 2: Malware detection techniques a machine learning approach (01:00 to 02:30)**

*Speaker: Dr. Vinod P, Professor, Cochin University of Science and Technology*

*Summary:* Dr. Vinod presented recent malware detection techniques. He explained malware and categories of malware. Malware is any software intentionally designed to cause disruption to a computer, server, client, or computer network. Dr. Vinod explained antivirus and its evolution. He also discussed the taxonomy of antivirus using machine learning process. Dr. Vinod cleared the queries of audience during the talk.

### Session 3: Privacy Preservation Approaches in Data Publishing (3:00 to 4:30)

Speaker: Dr. Kamal Macwan, Postdoc. Research Fellow, Loria-France

Summary: The session had focus on Privacy issues while publishing social network data to third parties for analysis. Graph Representation of Social Network has been discussed. Attacks such as Identity and Attribute disclosure discussed at length. Preventive measures to prevent such attacks had also been discussed in detail. He also took questions from the audience during this session.

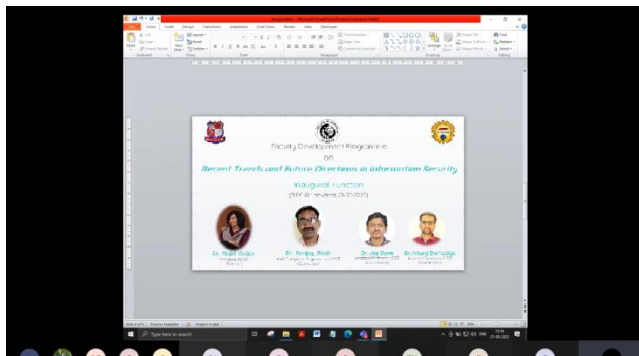


Figure 1: Day 1 Session 1

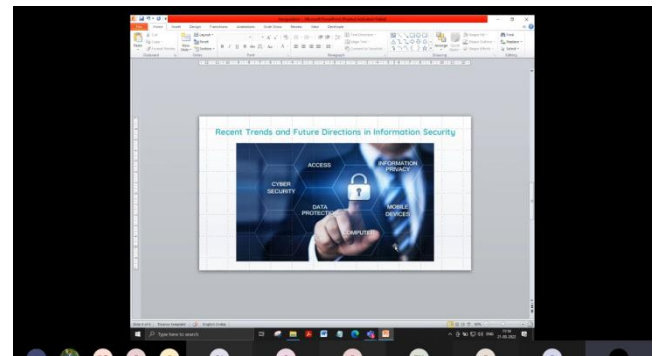


Figure 2: Day 1 Session 1

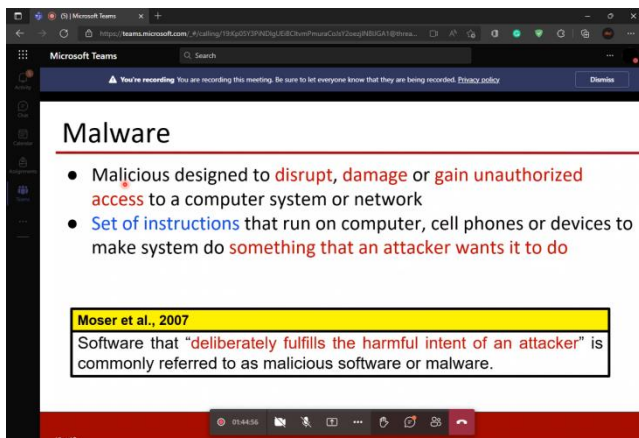


Figure 3: Day 1 Session 2

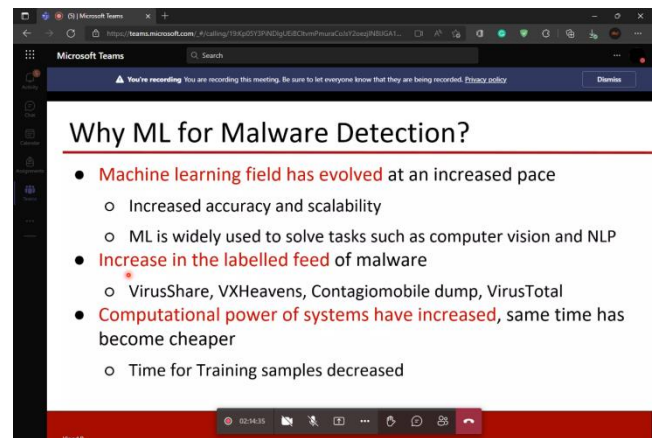


Figure 4: Day 1 Session 2

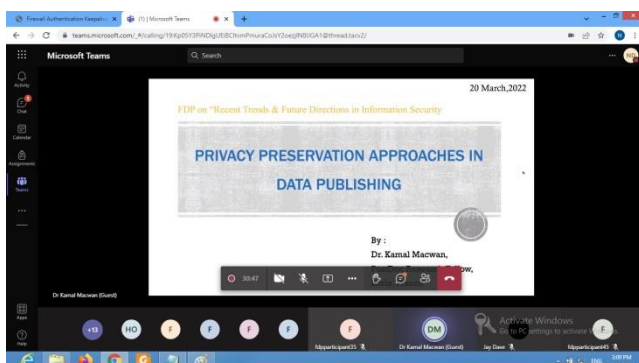


Figure 5: Day 1 Session 3

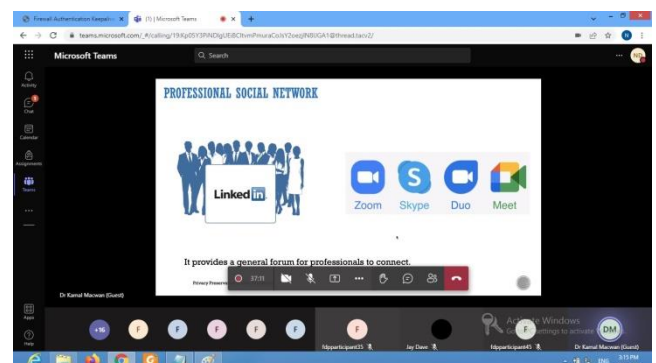
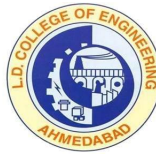


Figure 6: Day 1 Session 4



## Day 2 (22-Mar-2022)

---

### **Session 1: Security Concerns Regarding Cloud and Virtualization**

**(10:30 to 12:00)**

*Speaker: Dr. Bhavesh Borisaniya, Asst. Prof., Shantilal Shah Engineering College*

*Summary:* This session covered the following major points: What is cloud computing, Virtualization and its types, Role of virtualization in the cloud, How IaaS works in cloud? Security issues at different layers of the cloud, Security issues with virtualization, Security group as a firewall of cloud IaaS. During this session, he also fielded questions from the participants.

### **Session 2: Classification of IOT Devices Based on Network Traffic**

**Characteristics (01:00 to 02:30)**

*Speaker: Dr. Gaurav Singhal, Asst. Prof., NSIT Delhi*

*Summary:* In this session, Dr. Gaurav has discussed about IoT and security issues with IoT. IoT. A wide range of embedded devices applies to the Internet of Things (IoT) internet-connected, allowing them to send and exchange information in intelligent environments for one another. Since these IoT devices transmit their network traffic in broadcast mode due to wireless media, it is simple for an intruder to collect data by analyzing the network traffic of IoT devices. In addition, malicious network traffic can be generated by malicious IoT devices that other IoT devices can be corrupted, Denial of Service (DoS) attacks can be initiated, installing using malware, etc. Therefore, it is necessary for an administrator to evaluate the network traffic for security management and allocation of resources. Dr. Gaurav has also cleared doubts of participants regarding IoT security during the session.

### **Session 3: Authentication Techniques for Device to Device Communication in IOT (3:00 to 4:30)**

*Speaker: Dr. Ankur Gupta, Asst. Prof, Bennett University*

*Summary:* Dr. Ankur discussed authentication technique for IoT communication in this session. The speaker covered the following points during his talk: (1) A high-level discussion of the fundamental challenges and issues/characteristics of IoT and cloud computing, (2) Identify a few security and privacy issues within this framework, (3) Proposed approaches to addressing these issues. Dr. Ankur discussed the future directions of research in IoT security. He has also answered the queries of participants.



Figure 7: Day 2 Session 1

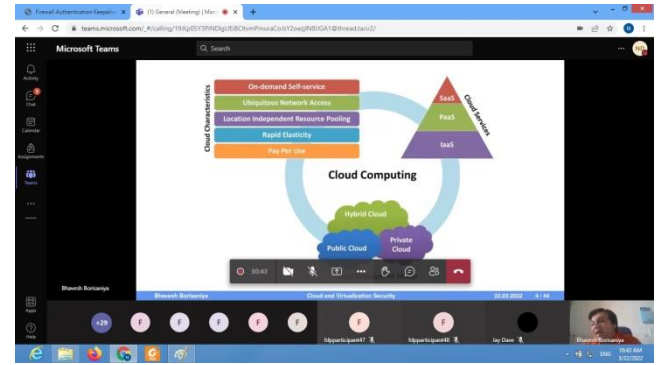


Figure 8: Day 2 Session 1

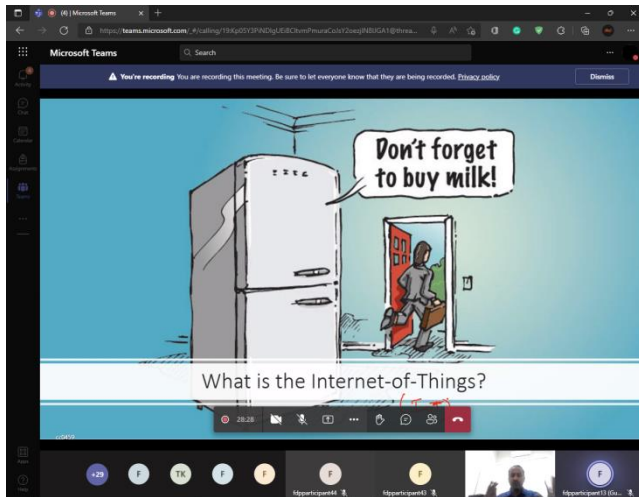


Figure 9: Day 2 Session 2

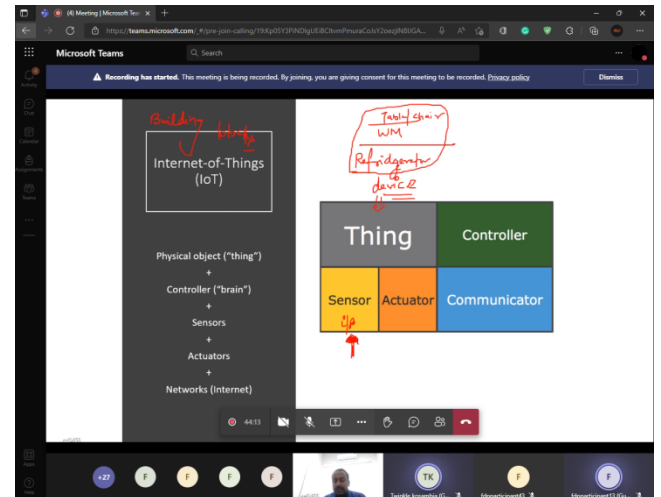


Figure 10: Day 2 Session 2



Figure 11: Day 2 Session 3

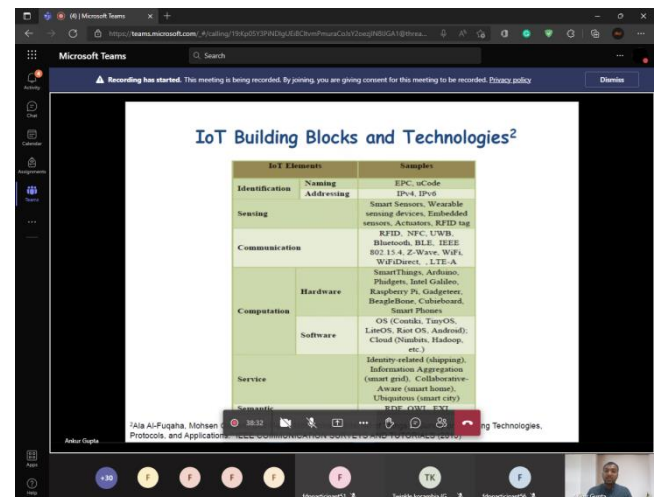
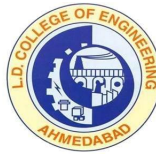


Figure 12: Day 2 Session 3





## Day 3 (23-Mar-2022)

---

### **Session 1: An Exploration to Location Based Service and its Privacy Preserving Techniques (10:30 to 12:00)**

*Speaker: Dr. Ruchika Gupta, PostDoc, IIT Guwahati*

*Summary:* The widespread use of Location Based Services (LBS), in which any informative service is provided simply based on the user's present location, has generated serious concerns about the user's location privacy. For example, if a customer wants to know "where is the nearest ATM machine?" she must provide her exact geographical coordinates in order to receive the location-based informative services she requested. Although Location Based Services open up a wide range of markets and give remarkable convenience to the end user, they also bring minor privacy threats to the user's location data. The requirement that the user inform the LBS provider of their current location in order to get connected services exposes the system to a risk of privacy invasion. Because the volume of data collected from moving or stationary mobile users utilizing LBS may be large, it's critical to design safe frameworks and systems that keep location information private. In the session, solution aspect of this has been discussed. She also talked with the participants about their questions.

### **Session 2: Empirical Analysis of Authentication Protocols in IoT Security (01:00 to 02:30)**

*Speaker: Dr. Nishant Doshi, Asso. Prof., PDEU*

*Summary:* Internet of Things (IoT) based services connect the user with sensing devices through intermediary devices like a gateway. The authentication with secure key exchange assures security trio of confidentiality, integrity, and availability for the complete IoT based system. It also ensures trusted privacy of communicated information. In this talk, we start from basics of authentication to the various authentication models as well as security attacks. He also discussed the participants' questions during the talk.

### **Session 3: Healthcare Data Mining and Privacy Issues (3:00 to 4:30)**

*Speaker: Dr. Nikunj Domadiya, Asst. Prof., LDCE*

*Summary:* In this session, Dr. Nikunj Domadiya has discussed the benefits of data mining in the field of healthcare domain. He showed various methodology for improving healthcare services and disease prediction. Different county's privacy laws prevent healthcare data sharing in the plain form to any other organizations. He has

discussed some privacy preserving solutions which preserve data privacy while performing data mining on the distributed healthcare data.

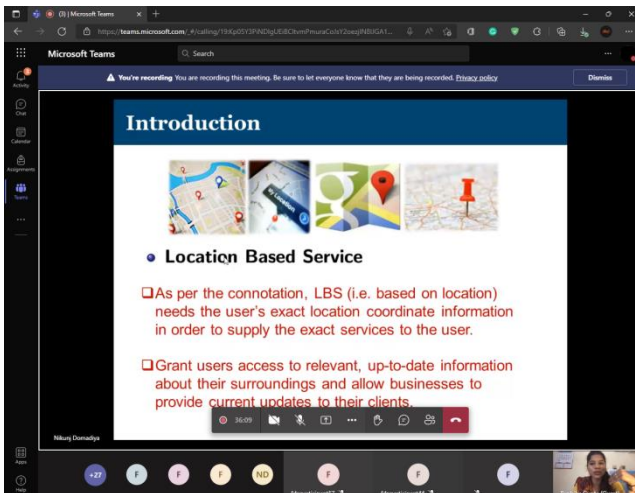


Figure 13: Day 3 Session 1

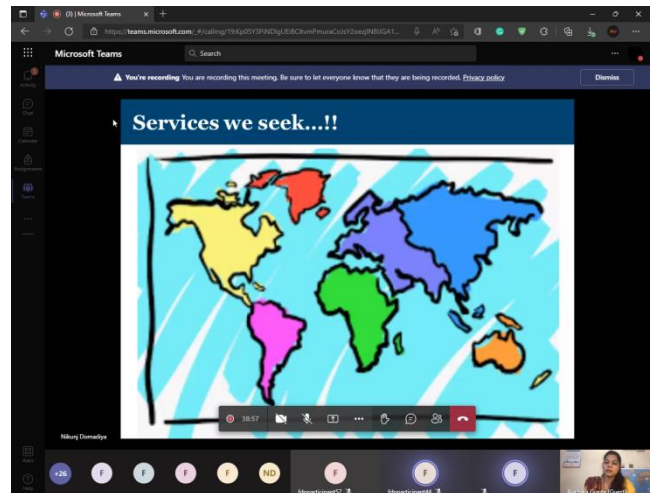


Figure 14: Day 3 Session 1

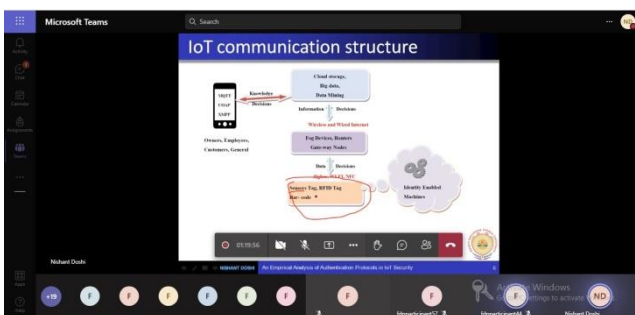


Figure 15: Day 3 Session 2

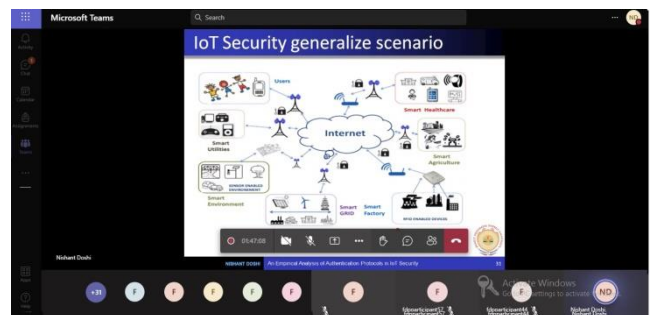


Figure 16: Day 3 Session 2

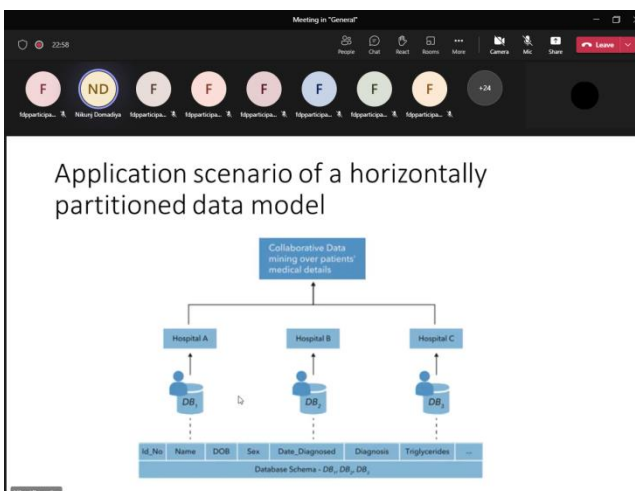
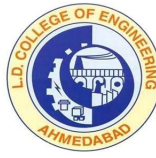


Figure 17: Day 3 Session 3



Figure 18: Day 3 Session 3



## Day 4 (24-Mar-2022)

---

### **Session 1: A Walk in the Forest of Blockchain and Bitcoin (10:00 to 12:00)**

*Speaker: Dr. Avijit Dutta, Lecturer cum PostDoc, TCG CREST Kolkata*

*Summary:* Dr. Avijit explained blockchain and cryptocurrency. Cryptocurrency is one of the trendy topics across the globe. Bitcoin is one of the popular cryptocurrencies that we widely investigated in the market. In some part of the world (e.g., US, Japan, UK, etc.), bitcoin has been legalized and has been considered as an acceptable currency. In this talk, he had focused on the technicalities of bitcoin and the backbone of it, called the blockchain. Dr. Avijit also answered the queries of participants during the session.

### **Session 2: Secure and Efficient Data Deduplication for Cloud Storage (01:00 to 02:30)**

*Speaker: Dr. Jay Dave, Asst. Prof., LDCE*

*Summary:* Dr. Jay Dave covered deduplication and its security issues during the talk. Deduplication is a data compression technique for eliminating storage of duplicate copies. efficiency as client does not need to transmit the data if it is available on the storage. Deduplication improves the efficiency of data backup and recovery process since less data is to be transferred. It reduces the electricity requirements to access and cool down the disks or tape drives. In this way, deduplication helps the ecosystem by reducing global warming issues. However, deduplicated cloud computing system faces serious security challenges such as confidentiality and ownership verification. Dr. Jay has discussed about these security challenges and proposed solutions to these challenges in detail.

### **Session 3: Basics about Digital Forensics with Case Studies (3:00 to 4:30)**

*Speaker: Dr. Jyoti Gajrani, HoD CSE, Govt. Engineering College Ajmer*

*Summary:* The talk was focused on Volatility tools for analysis of two real-world malware namely Cridex and Zeus. Dr. Jyoti presented the analysis of memory images captured from victim systems using the Volatility tool in detail. We use forensic analysis to extract information about running processes, open network sockets and network connections, DLLs loaded for each process, cached registry entries, process Ids, and more. She discussed cybercrime from a criminal point of view and how he uses various techniques to hide the footprints of crime. Dr. Jyoti also communicated with participants regarding their questions.



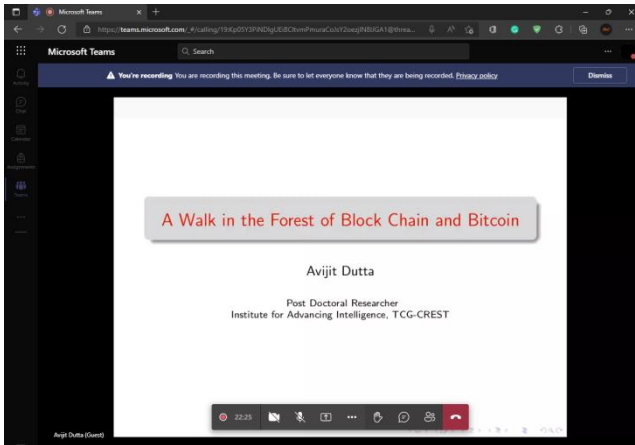


Figure 19: Day 4 Session 1

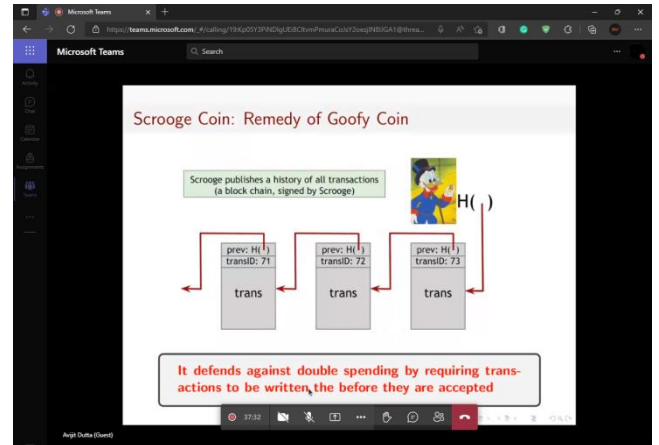


Figure 20: Day 4 Session 1

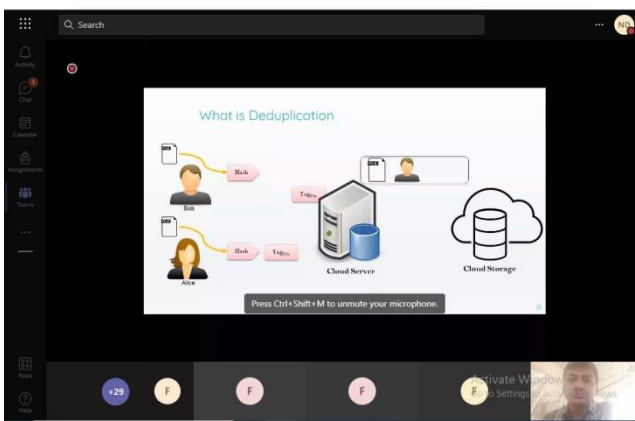


Figure 21: Day 4 Session 2

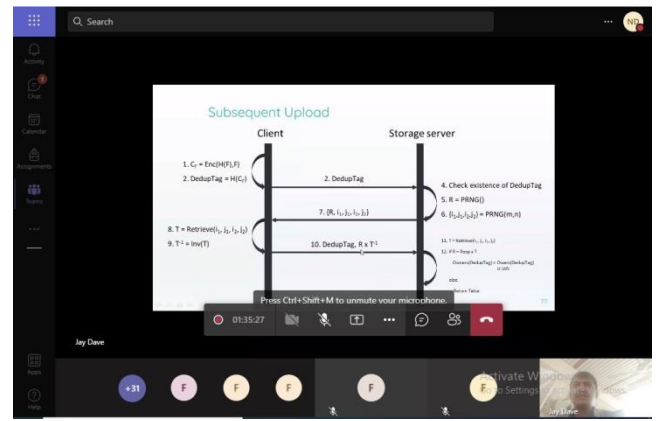


Figure 22: Day 4 Session 2

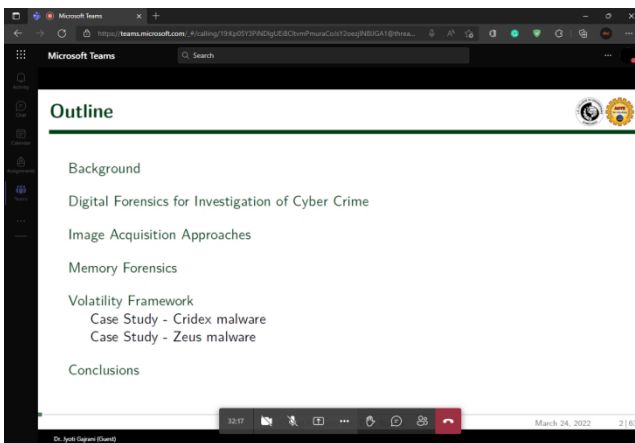


Figure 23: Day 4 Session 3

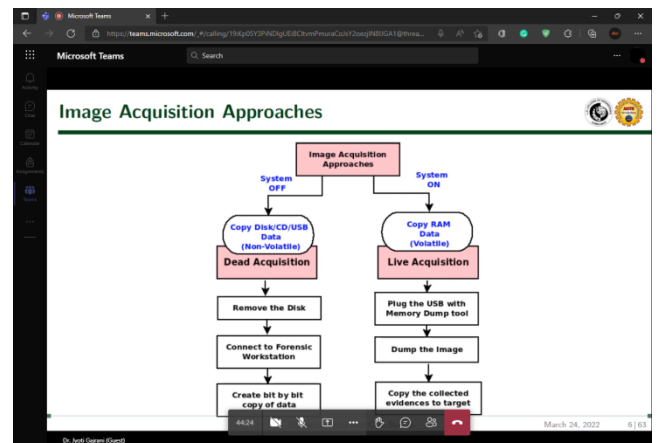
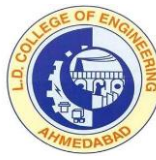


Figure 24: Day 4 Session 3



## Day 5 (25-Mar-2022)

---

### **Session 1: Security architecture against Sybil attack in RPL-based IoT networks: a focus on smart home use case (10:00 to 12:00)**

*Speaker: Dr. U P Rao, Asst. Prof., SVNIT*

*Summary:* Internet of things (IoT) is renowned for being a massive revolution led by business leaders and researchers. Routing protocol for low-power and lossy network (RPL) is a standardized protocol that serves the routing need of the IPv6-based low-power and lossy networks, which are the significant enablers of the IoT technology. Despite its many outstanding features, RPL offers very low protection against different routing attacks. In this respect, Dr. U. P. Rao has mainly emphasized the sybil attack. Specifically, focus on three different types of sybil attacks on a realistic smart home network topology. Considering the involvement of resource-constraint devices, he has discussed RPL's multi-instance property to integrate the decentralized architecture into the exiting RPL protocol.

### **Session 2: NEP 2020 - Quality Education, Accreditation and Teacher Development (01:00 to 02:30)**

*Speaker: Dr. S. D. Panchal, Director, GTU-Graduate School of Engg & Technology*

*Summary:* Dr. Panchal discussed about quality education, accreditation, and teachers development from school level to higher education level. He also discussed the vision of the NEP 2020. National Education Policy 2020 envisions an India-centric education system. By delivering high-quality education to all, it contributes directly to our nation's long-term transformation towards an equal and thriving knowledge society. Dr. Panchal presented highlights of NEP 2020 in detail. He also answered the questions of participants during the talk.

### **Session 3: Privacy and Security Challenges in Smartphones (3:00 to 4:30)**

*Speaker: Dr. Shweta Bhandari, Asst. Prof., LNMIIT*

*Summary:* Dr. Shweta discussed security and privacy problem related to smartphones during the talk. In today's world, ignoring data privacy issues is like a sailor turning a blind eye to rising seas and a falling barometer. The speed and convenience of technology lure users to share their private and sensitive information. With the advent of smartphones, sharing, storing, and processing of private, sensitive, and confidential data reached the next level. The talk helps in understanding the importance of digital privacy in the era of smartphones. She conceptualized the notion of Privacy and the misunderstanding related to it. It also throws light on the notions of Privacy and Security challenges that can serve as the directions to future research. Dr. Shweta also discussed with participants regarding their doubts.

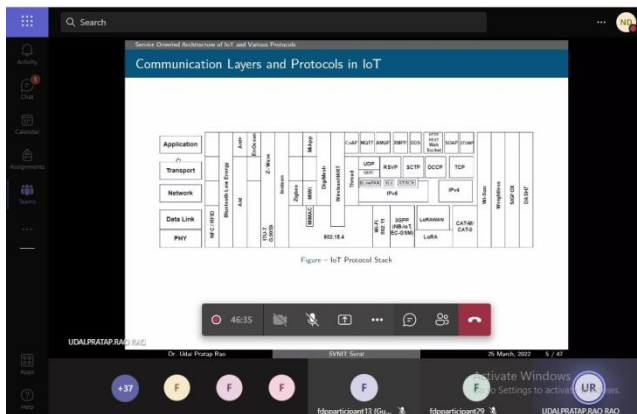


Figure 25: Day 5 Session 1

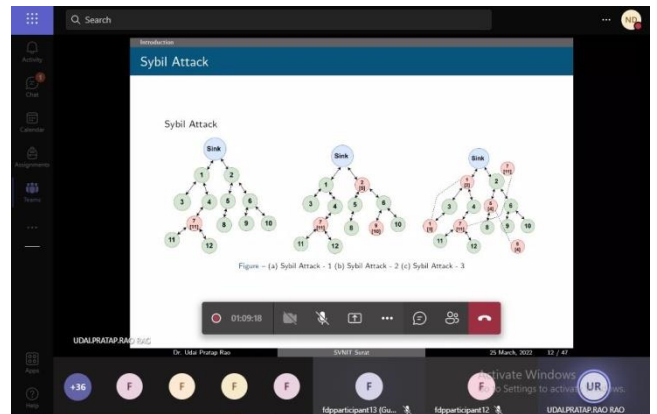


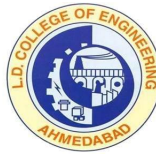
Figure 26: Day 5 Session 1

Figure 27: Day 5 Session 2

Figure 28: Day 5 Session 2

Figure 29: Day 5 Session 3

Figure 30: Day 5 Session 3



## Day 6 (26-Mar-2022)

---

### **Session 1: Confidentiality Computing (09:00 to 10:30)**

*Speaker: Dr. Maniklal Das, Dean-Academic Programs, DAIICT*

*Summary:* During this talk, Dr. Das discussed about confidentiality computing. Confidential computing is an emerging research area where data protection is emphasized when data is in use for computing. Trusted Execution Environment (TEE) is commonly used for ensuring data confidentiality while data is in use during execution. Dr. Das focused on confidential computing using TEE and other variants for data protection. He has also solved the queries of participants during the session.

### **Session 2: Feedback and Examination (1:00 to 2:30)**

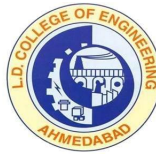
*Summary:* In this session, all participants appeared in an online exam using the MS team platform. A total of 45 MCQ type questions were asked in this exam. Google form link was also shared with all participants to collect the feedback of FDP.

### **Session 3: Valedictory (3:00 to 4:30)**

*Summary:* One-Week Online Faculty Development Program on “Recent Trends and Future Directions in Information Security” from 21<sup>st</sup> to 26<sup>th</sup> March, 2022 was successfully organized by the Computer Engineering Department, L. D. College of Engineering-Ahmedabad.

Dr. Sanjay Shah, Professor and HoD of Computer Engineering Department was the Chief Guest for the Valedictory Ceremony of the One-Week Online Faculty Development Program. Dr. S. M. Shah, in his valedictory addressing, congratulated the Program Coordinator Dr. Jay Dave and Dr. Nikunj Domadiya for organizing the FDP in a successful manner. Further, he appreciated the Teaching Staff Members of Computer Department for promoting such kind of development programme for the faculties. He also motivated the researchers and faculties about how to keep continuous interest in the research.





At the end of the valedictory session, vote of thanks was given by Dr. Nikunj Domadiya, Coordinator of the FDP in which he has been paid his gratitude towards all the dignitaries who have spared their valuable time to share their expertise with the participants. He also expressed gratitude to all participants of the FDP for active participation during all the sessions. He has given thanks to sponsoring body of this FDP, i.e., AICTE-GTU with these words, “We are highly thankful to the AICTE-GTU for providing financial assistance to organize this FDP and hope we will find the support in future also for organizing such kind of activities.”

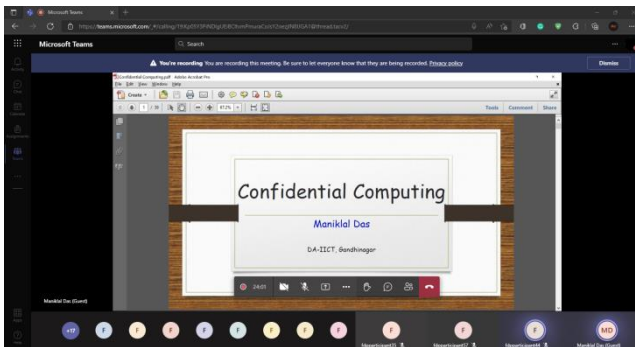


Figure 31: Day 6 Session 1

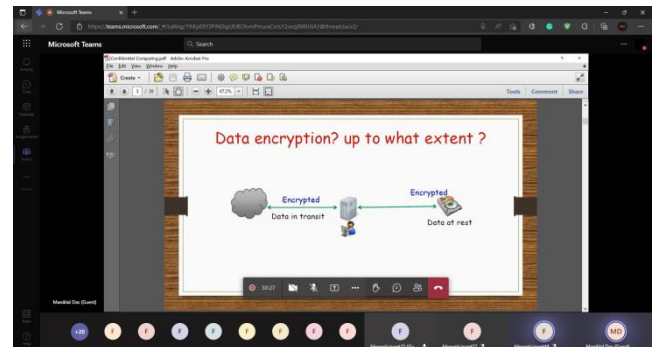
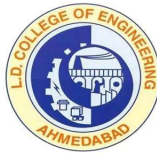


Figure 32: Day 6 Session 1



## Outcome of the program

---

The participants found the event interactive and effective. They understood various research areas of information security. The participants also gained awareness on importance of protecting their personal information. All the resource persons engage participants in meaningful, relevant scenarios that clarify many of the complexities involved in information security. All FDP attendees have acquired a deeper understanding of the need to conduct research in the field of information security, and got the knowledge about various tools. Through discussions, FDP offered attendees an opportunity to ask questions, as well to share ideas and information on the latest and best security solutions and services available. We summaries the outcome of FDP as follows.

- Understood the methods and techniques for information security.
- Identified the problems and challenges of information security.
- Gained knowledge on applications of cryptography in information security.
- Identified the novel research areas in the field of information security.