**One Week Faculty Development Program on**

# Recent Trends in Data Security (RTDS)

**Technically sponsored by**

**Computer Society of India**
**The Institution in Engineering and Technology**
**Indian School of Ethical Hacking**

**28th June- 2nd July, 2021**

**Organized by**

**Department of Information Technology**
**RCC Institute of Information Technology**
Canal South Road, Beliaghata, Kolkata – 700015, West Bengal, INDIA

## Objective of RTDS:

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It’s a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.

When properly implemented, robust data security strategies will protect an organization’s information assets against cybercrime, but they also guard against threats from insider and human error, which are among the leading causes of data breaches today. Data security involves deploying tools and technologies that enhance the organization’s visibility into where its critical data resides and how it is used. Ideally, these tools should enable protections like encryption, data masking and redaction of sensitive files and should automate reporting to streamline audits and adhering to regulatory requirements.

The primary aim of data security is to protect the data that an organization collects, stores, creates, receives or transmits. Compliance is also a major consideration. It doesn't matter which device, technology or process is used to manage, store or collect data; it must be protected. Data breaches can result in litigation cases and huge fines, not to mention damage to an organization's reputation. The importance of shielding data from security threats is more important today than it has ever been. Also, in this pandemic situation the world is compelled to move for remote work, as a result more and more sensitive information are being distributed over the communication channel. Security of those data is another prime requirement of the time.

## Committee Members of RTDS:

### *Chief Patron*

**Shri. Pranabesh Das**, DTE, Govt. of WB and Chairman (BOG), RCCIIT

### *Advisory Committee*

**Prof. (Dr.) Anirban Mukherjee**, Principal (O), RCCIIT
**Dr. Abhishek Basu**, FIC (Academics), RCCIIT

### *Convener*

**Ms. Moumita Deb**, Assistant Professor, IT, RCCIIT

### *Coordinators*

**Dr. Shaswati Roy**, Assistant Professor, IT, RCCIIT
**Dr. Shyantani Maiti**, Assistant Professor, IT, RCCIIT

### *Organizing Committee*

**Dr. Hrishikesh Bhaumik**, Associate Professor, IT, RCCIIT
**Dr. Abhijit Das**, Associate Professor, IT, RCCIIT
**Dr. Indrajit Pan**, Associate Professor & HOD, IT, RCCIIT
**Ms. Abantika Choudhury**, Assistant Professor, IT, RCCIIT
**Mr. Ranjan Jana**, Assistant Professor, IT, RCCIIT
**Mr. Jayanta Datta**, Assistant Professor, IT, RCCIIT
**Mr. Hiranmoy Roy**, Assistant Professor, IT, RCCIIT
**Mr. Soumyadip Dhar**, Assistant Professor, IT, RCCIIT
**Mr. Pankaj Pal**, Assistant Professor, IT, RCCIIT
**Mr. Amit Khan**, Assistant Professor, IT, RCCIIT
**Mr. Sudarsan Biswas**, Assistant Professor, IT, RCCIIT
**Ms. Jayanti Das**, Assistant Professor, IT, RCCIIT
**Ms. Ahana Patra**, Assistant Professor, IT, RCCIIT

## Details of RTDS:

### *Details of Talk Delivered:*

**Date:** 28-Jun-2021

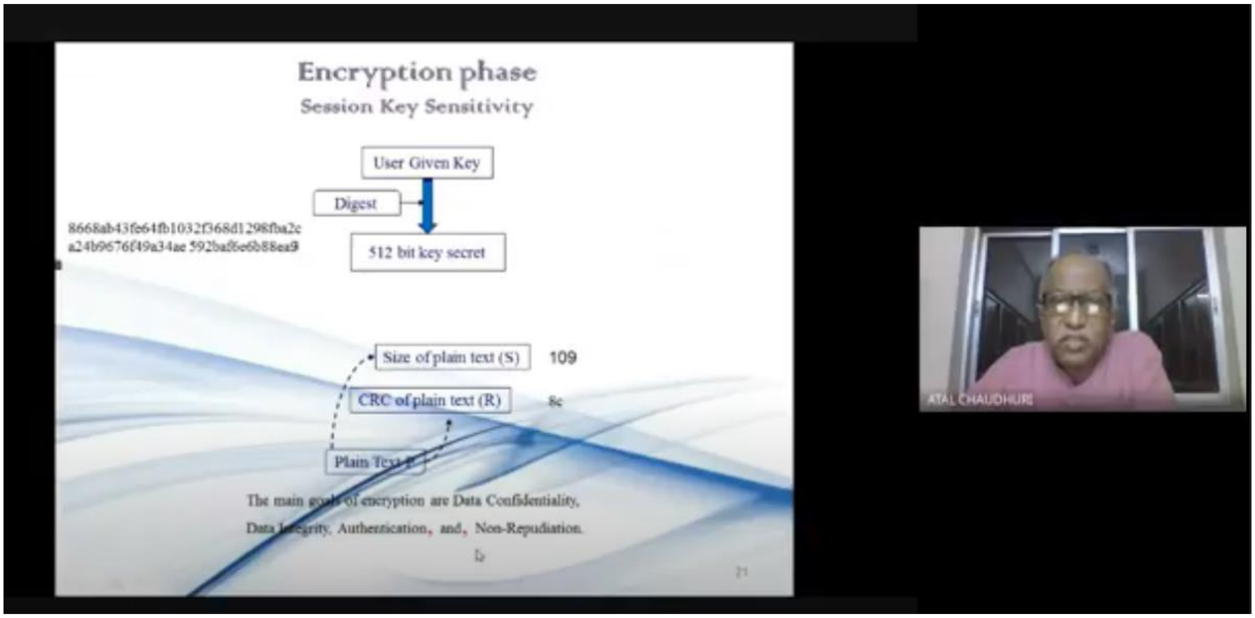
**Speaker Name:** **Dr. Atal Chaudhuri**, Professor, Department of Computer Science and Engineering, Jadavpur University

**Talk Title:** Crack the Cipher

**Talk Abstract:** This talk discussed about the secured data communication over internet being most important concern nowadays. One of the common security process is data encryption. One main aim is to build an apparently attack resistant encryption model.

Session key may be one solution where new encryption key is used in every session but that needs key exchange prior to every communication. Common solution is the new key be the function of the previous key as well as the function of the previous plain-text. Here after every communication one needs to extract the next session key and to remember till the next communication.

**Number of Attendees:** 36



Encryption phase

Session Key Sensitivity

The main goals of encryption are Data Confidentiality, Data Integrity, Authentication, and, Non-Repudiation.

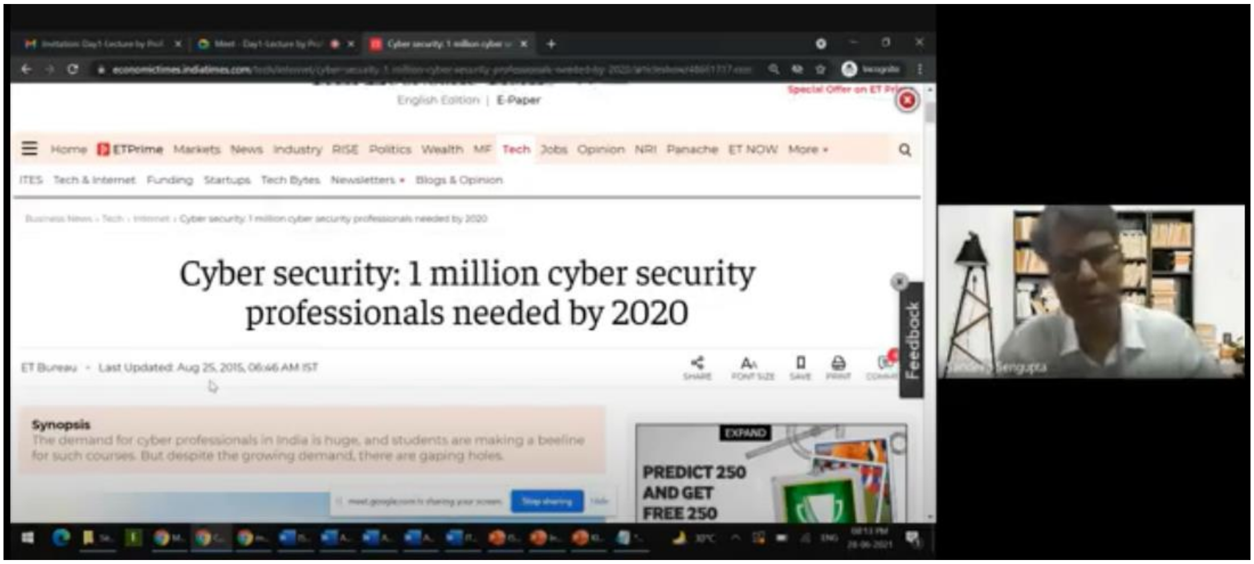
**Date:** 28-Jun-2021

**Speaker Name:** **Mr. Sandeep Sengupta**, Director, Indian School of Ethical Hacking

**Talk Title:** Industry Trends and Data Security Awareness

**Talk Abstract:** The talk mainly gives the overview of early warning service. Whenever there is antivirus, firewall, and other devices alert us when attack starts. However, there are many companies who can not wait till the attack starts. These companies take proactive actions. Generally, when there is a malware attack and this attack would be reported to the antivirus companies. Then the antivirus companies do the analysis of virus pattern and then this pattern is added into the .dat file and that .dat file is updated in the virus database. In early engine service, the companies monitor different websites and pattern is analyzed and send the alerts to the users. This talk also discussed on other various aspects of current industry trends on data security.

**Number of Attendees:** 36


English Edition | E-Paper

Cyber security: 1 million cyber security professionals needed by 2020

ET Bureau • Last Updated: Aug 25, 2015, 06:46 AM IST

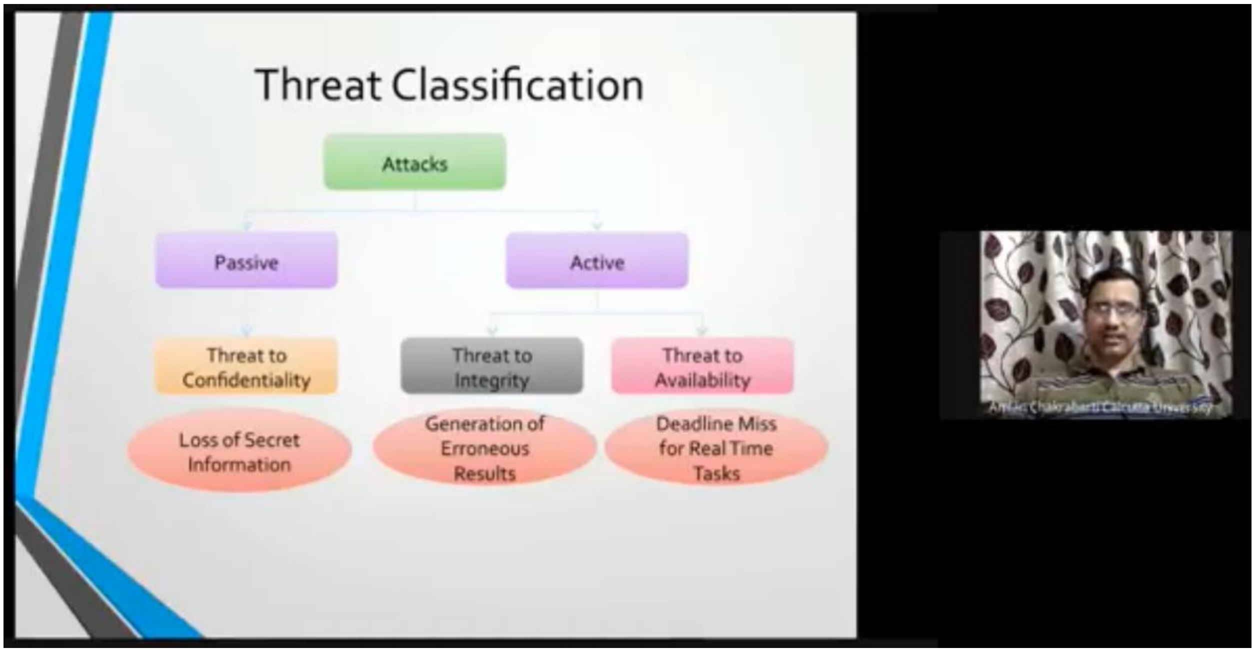
Synopsis

The demand for cyber professionals in India is huge, and students are making a beeline for such courses. But despite the growing demand, there are gaping holes.

**Date:** 29-Jun-2021

**Speaker Name:** **Dr. Amlan Chakrabarti**, Professor and Director, A. K. Choudhury School of I.T., University of Calcutta

**Talk Title:** Self-Aware Strategies for Embedded Security


Threat Classification

Attacks
Passive
Active
Threat to Confidentiality
Threat to Integrity
Threat to Availability
Loss of Secret Information
Generation of Erroneous Results
Deadline Miss for Real Time Tasks
Amlan Chakrabarti Calcutta University

**Talk Abstract:** The talk discussed regarding the exposure of so many machines on the web that provides a veritable playground for hackers to test their skills – bringing down websites, stealing data , or committing fraud. It is generally termed as cybercrime.

Cybersecurity can be termed as combating this in a multi-disciplinary affair that spans hardware and software through to policy and people – all of it aimed at both preventing cybercrime occurring in the first place, or minimizing its impact when it does.

Previously, software security was the prime concern and the underlying hardware was considered trusted. However, we have entered the embedded regime direct task processing on hardware is the trend. Present day objectives of semiconductor design industry – 1) meet stringent marketing deadlines, and 2) reduce design cost. To meet such objectives, a globalization technique of SoC designing is adopted.

**Number of Attendees:** 35

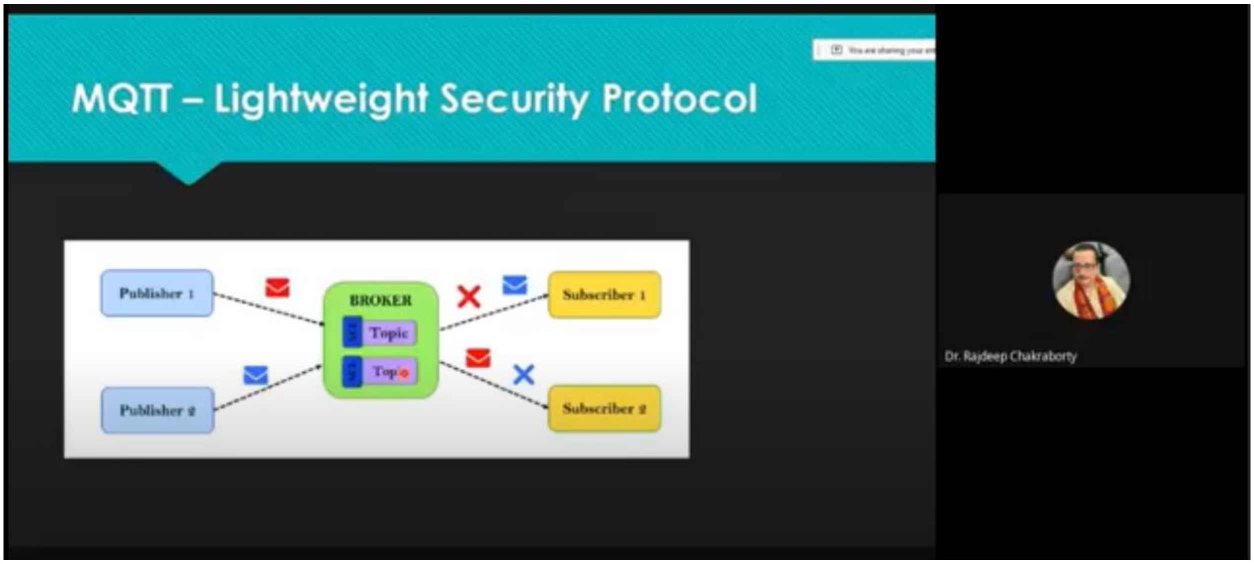
**Date:** 30-Jun-2021

**Speaker Name:** **Dr. Rajdeep Chakraborty**, Assistant Professor, Department of Computer Science and Engineering, Netaji Subhash Engineering College, Kolkata.

**Talk Title:** Design Issues and Challenges of Lightweight Ciphers and IoT Security

**Talk Abstract:** This talk was organized into three main parts – 1) the first briefly discusses on lightweight cryptography and its application for IoT security, 2) the second introduces different attack models and discusses some common attacks on lightweight cryptography, 3) the last part presents several design issues for lightweight ciphers.

**Number of Attendees:** 35



MQTT – Lightweight Security Protocol

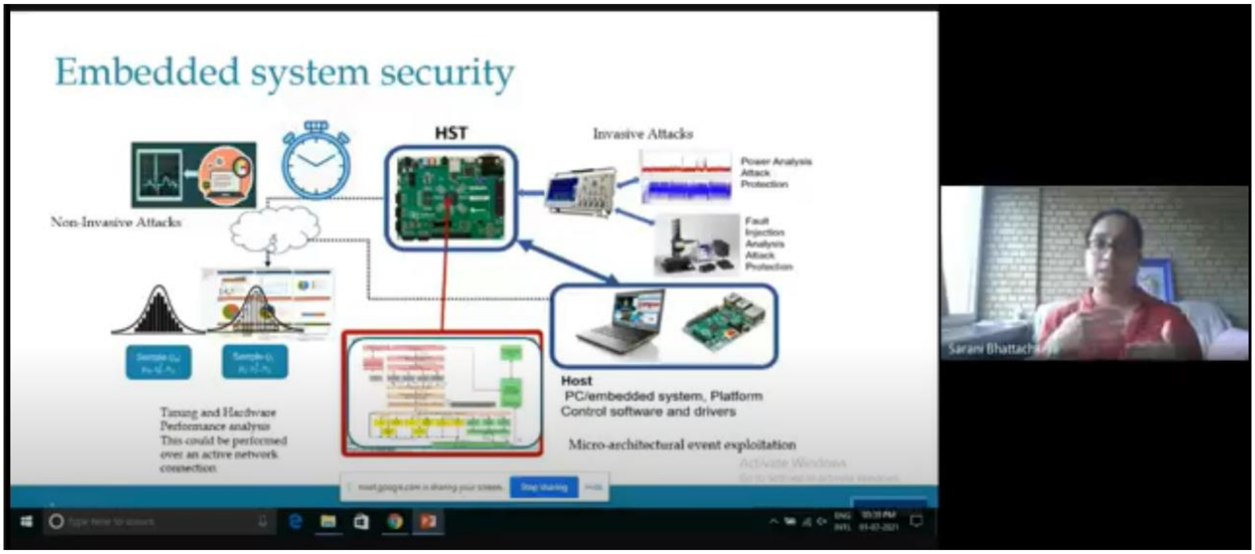
**Date:** 01-Jul-2021

**Speaker Name:** **Dr. Sarani Bhattacharya**, Postdoctoral Researcher, imec-COSIC, KU Leuven

**Talk Title:** Micro-Architectural Security for  the Design of Secure Systems

**Talk Abstract:** This talk focused on microprocessor research for improving performance over the last four decades. Various micro architectural features such as cache memories, branch prediction, superscalar, speculative and out-of-order execution, were developed to facilitate this. Side-by-side, features such as multiprogramming, multicore and hardware multithreading were incorporated to increase throughput. These features allowed multiple users to simultaneously share a processor. To isolate one user's program from another, rudimentary security schemes such as protection rings and page table access controls bits were used. Very soon it was realized that these security schemes were insufficient. Vulnerabilities in software permitted user space programs to gain privileged access. Shared hardware became a source of information leaks that could undermine the isolation provided. The very features in the processor that were incorporated to boost performance and throughput have now become a security liability.

**Number of Attendees:** 34



Embedded system security

HST

Invasive Attacks

Power Analysis Attack Protection

Fault Injection Analysis Attack Protection

Non-Invasive Attacks

Timing and Hardware Performance analysis This could be performed over an active network connection

Host
PC/embedded system, Platform Control software and drivers

Micro-architectural event exploitation

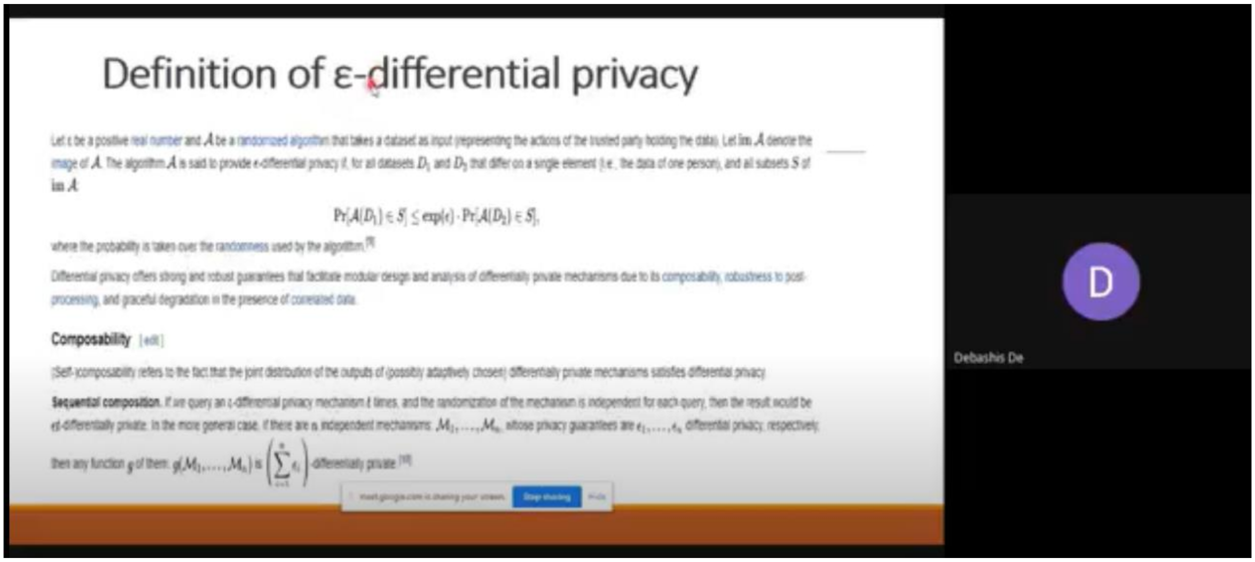
**Date:** 02-Jul-2021

**Speaker Name:** Dr. Debashis De, Professor, Department of Computer Science and Engineering, MAKAUT, W.B

**Talk Title:** Privacy-Preserving Data Sharing

**Talk Abstract:** This talk focused on privacy preserving technique for training, inference, and disclosure in large scale data analysis, both in the distributed and centralized settings. It discussed increasing interest of the machine learning community in leveraging cryptography techniques such as multi-party computation and homomorphic encryption for privacy preserving training and inferences as well as differential privacy for disclosure.

**Number of Attendees:** 31



## Definition of ε-differential privacy

Let ε be a positive real number and $\mathcal{A}$ be a randomized algorithm that takes a dataset as input (representing the actions of the trusted party holding the data). Let im $\mathcal{A}$ denote the image of $\mathcal{A}$. The algorithm $\mathcal{A}$ is said to provide ε-differential privacy if, for all datasets $D_1$ and $D_2$ that differ on a single element (i.e., the data of one person), and all subsets $S$ of im $\mathcal{A}$

$$\Pr[\mathcal{A}(D_1) \in S] \leq \exp(\epsilon) \cdot \Pr[\mathcal{A}(D_2) \in S],$$

where the probability is taken over the randomness used by the algorithm.[9]

Differential privacy offers strong and robust guarantees that facilitate modular design and analysis of differentially private mechanisms due to its composability, robustness to post-processing, and graceful degradation in the presence of correlated data.

**Composability** [edit]

(Self-)composability refers to the fact that the joint distribution of the outputs of (possibly adaptively chosen) differentially private mechanisms satisfies differential privacy.

**Sequential composition.** If we query an ε-differential privacy mechanism $t$ times, and the randomization of the mechanism is independent for each query, then the result would be $\epsilon t$-differentially private. In the more general case, if there are $n$ independent mechanisms: $\mathcal{M}_1, \dots, \mathcal{M}_n$, whose privacy guarantees are $\epsilon_1, \dots, \epsilon_n$ differential privacy, respectively, then any function $g$ of them: $g(\mathcal{M}_1, \dots, \mathcal{M}_n)$ is $\left(\sum_{i=1}^{n} \epsilon_i\right)$-differentially private.[10]

***Program Schedule of RTDS***

| Date | Time | Description |
|---|---|---|
| **28-Jun-21** | 6:00 PM - 6:30 PM | Inauguration of the Program |
| | 6:30 PM - 8:00 PM | Talk by **Prof. Atal Chaudhuri**, Jadavpur University |
| | 8:00 PM - 9:30 PM | Talk by **Mr. Sandeep Sengupta**, Director, ISOEH |
| | | |
| **29-Jun-21** | 7:00 PM - 8:30 PM | Talk by **Prof. Amlan Chakrabarti**, University of Calcutta |
| | | |
| **30-Jun-21** | 7:00 PM - 8:30 PM | Talk by **Dr. Rajdeep Chakraborty**, Netaji Subhash Engineering College |
| | | |
| **01-Jul-21** | 7:00 PM - 8:30 PM | Talk by **Dr. Sarani Bhattacharya**, imec-COSIC, KU Leuven |
| | | |
| **02-Jul-21** | 7:00 PM - 8:30 PM | Talk by **Prof. Debashis De**, MAKAUT, W.B |
| | 8:30 PM - 9:30 PM | Valedictory |