

Report : Expert Lecture
Artificial Intelligence in Cyber Security
01.04.2022

The Department of Computer Engineering, J. C. Bose University of Science and Technology, YMCA organized an online expert lecture on **Artificial Intelligence in Cyber Security** for the students of B.Tech 6th Sem (CE, IT) students. The lecture was conducted on 1st April 2022 and was attended by more than 100 participants. Dr. Preeti and Dr. Shivi, Assistant Professors of the department, were the Program Coordinators of this expert lecture.

Dr. Shivi Garg welcomed the resource person, Ms. Priyanka Tomar and extended gratitude for sparing valuable time to deliver an online lecture to the students. She further acquainted the audience about the rich experience of the Ms. Priyanka Tomar. She is having 20 years' experience into various IT fields including Cyber Security & Cyber Forensics. She is also an author of Cyber Crime & Preventive Measures. She is also a founder of newerasystem.com (customized software development) and petalherbs.com (premium ayurvedic skin care products manufacturing). She is also a Cyber Security & Forensics Blogger – www.cyberpathshalaindia.com (A cyber awareness initiative Chosen as India's Dynamic Women changing the face of Indian Cyber Space).

Ms. Tomar started with the introduction to Artificial Intelligence (AI) quoting real-world examples where AI can be used efficiently. To make the session more interactive, she posed some quiz questions in between also. She further discussed different use cases where AI applications are prominent. As cited by Ms. Tomar, "AI emphasizes the development of intelligent machines and thinking and working like humans".

Session continued with applications of AI in day-to-day life such as face recognition in Apple devices. She also stated that there is large amount of data everywhere, which is always under threat by hackers and attackers. So, there is a need to make systems secure. She elaborated the need of AI in cyber security and illustrated various examples such as Phishing, zero-day exploits, Supply chain exploits, speech recognition, Learning and planning, etc. She also demonstrated how computer vision can be used cyber security.

Finally, Ms. Tomar discussed the various drawbacks of AI technology. Expert Lecture was concluded with a Q&A session.

The session concluded with the vote of thanks by Dr. Shivi Garg and Dr. Preeti Sethi. This fruitful session was appreciated by one and all present.

This screenshot shows a Zoom meeting interface. At the top, a status bar indicates 'You are viewing Priyanka Tomar's screen'. The main window displays a PowerPoint presentation titled 'AI in Cyber Security-Practical Instances'. The slide is titled 'Agenda' and lists three points: 1. AI & its applications in Cyber Security, 2. Use Cases of AI in Cyber Security, and 3. AI Drawbacks and Limitations. The slide features a graphic of three overlapping circles with a face in the center. The Zoom interface includes a top bar with participant names (Priyanka Tomar, JCBUSTYMICA, and others), a bottom bar with controls like 'Unmute', 'Start Video', 'Share Screen', and 'End', and a taskbar at the very bottom showing various system icons and the date 'Fri 1 Apr 2:07 PM'.

This screenshot shows a Zoom meeting interface, similar to the one above. The main window displays the same PowerPoint presentation titled 'AI in Cyber Security-Practical Instances' with the 'Agenda' slide. The Zoom interface includes a top bar with participant names (Priyanka Tomar, JCBUSTYMICA, and others), a bottom bar with controls like 'Unmute', 'Start Video', 'Share Screen', and 'End', and a taskbar at the very bottom showing various system icons and the date 'Fri 1 Apr 2:08 PM'. A small video window in the bottom right corner shows a participant named Priyanka Tomar.

Zoom Meeting

You are viewing Priyanka Tomar's screen View Options

Priyanka Tomar JCBUST YMCA 19001003080 PARAG ... 19001003054 KALPES ... 19001003084 PRAJW ... 19001003023 ASHISH ...

Recording...

PowerPoint File Edit View Insert Format Arrange Tools Slide Show Window Help

Home Insert Draw Design Transitions Animations Slide Show Review View

Play From Start Play From Current Slide Presenter View Custom Show Set Up Slide Show Hide Slide Rehearse Timings Record Show Show Media Controls

1 2 3 4 5 6 7 8 9 10

What is Artificial Intelligence

Feed the human experience to the machine in the form of data.
AI emphasizes the development of intelligent machines, thinking and working like humans.

We need ideal approach such as systems should think and act rationally.

Use Case :

Slide 6 of 22 English (United States) Accessibility: Investigate

Unmute Start Video Security Participants Chat Share Screen Raise Hand Pause/Stop Recording Apps More

Type here to search

36°C 14:11 01-04-2022

Zoom Meeting

You are viewing Priyanka Tomar's screen View Options

Priyanka Tomar JCBUST YMCA 19001003080 PARAG ... 19001003054 KALPES ... 19001003084 PRAJW ... 19001003023 ASHISH ...

Recording...

PowerPoint File Edit View Insert Format Arrange Tools Slide Show Window Help

Home Insert Draw Design Transitions Animations Slide Show Review View

Play From Start Play From Current Slide Presenter View Custom Show Set Up Slide Show Hide Slide Rehearse Timings Record Show Show Media Controls

1 2 3 4 5 6 7 8 9 10

What does it indicate?

Artificial Intelligence

Machine Learning

Deep Learning

Slide 7 of 22 English (United States) Accessibility: Investigate

Unmute Start Video Security Participants Chat Share Screen Raise Hand Pause/Stop Recording Apps More

Type here to search

36°C 14:14 01-04-2022

Zoom Meeting You are viewing Priyanka Tomar's screen View Options

Participants (100)

Q Find a participant

- JCBUST YMCA (Host, me)
- Priyanka To... (Co-host)
- LM Lalit Mohan Goyal (Co-host)
- P 18001003085_Parth Munshi
- A 19001003005_AJAY
- 1A 19001003006_Ajay Kumar
- 1S 19001003009_Anjali Singh
- 1A 19001003011_Ankit Kumar
- 19001003012_Ankur
- 1A 19001003013_Ankush Bhan
- A 19001003014_ANSHUL DHANK...
- A 19001003015_Anshul Miglani
- 1A 19001003017_ANUPAMA
- 1A 19001003019_arpit garg

Slide 18 of 32 English (United States) Accessibility Investigate

Why do we need AI in Cyber Security

Example-
Phishing
Zero day exploits
Supply chain exploits
Speech recognition
Learning and planning
chess-playing computers to self-driving cars,
voice assistants (alexa, siri etc),
image recognition for face unlock in mobile phones,
ML-based financial fraud detection
Search Engines
Automated stock trading :

Unmute Start Video Security Participants Chat Share Screen Raise Hand Apps More End

Type here to search 35°C ENG IN 14:29 01-04-2022

Zoom Meeting You are viewing Priyanka Tomar's screen View Options

Participants (100)

Q Find a participant

- JCBUST YMCA (Host, me)
- Priyanka To... (Co-host)
- LM Lalit Mohan Goyal (Co-host)
- P 18001003085_Parth Munshi
- A 19001003005_AJAY
- 1A 19001003006_Ajay Kumar
- 1S 19001003009_Anjali Singh
- 1A 19001003011_Ankit Kumar
- 19001003012_Ankur
- 1A 19001003013_Ankush Bhan
- A 19001003014_ANSHUL DHANK...
- A 19001003015_Anshul Miglani
- 1A 19001003017_ANUPAMA
- 1A 19001003019_arpit garg

Slide 19 of 32 English (United States) Accessibility Investigate

How can AI Help Us?

For cyber security We need to focus more on certain things such as

- Automated two way factor authorization – 80% breaches due to weak pwd so we need TFA
- Zero trust mechanisms for devices
- File less malware detection

Unmute Start Video Security Participants Chat Share Screen Raise Hand Pause/Stop Recording Apps More End

Type here to search 35°C ENG IN 14:31 01-04-2022

Zoom Meeting

You are viewing Priyanka Tomar's screen

View Options

Priyanka Tomar

JCBUST.YMCA

19001003021_Ashish

19001003046_harsh H

19001003005_AJAY

19001003014_ANSHU...

Recording...

PowerPoint

File Edit View Insert Format Arrange Tools Slide Show Window Help

Home Insert Draw Design Transitions Animations Slide Show Review View

Play from Start Play from Current Slide Presenter View Custom Show Set Up Slide Show Hide Slide Rehearse Timings Record Slide Show Play Narrations Use Timings Show Media Controls

Applications of AI in Cyber security

- Password Protection and Authentication
- Phishing Detection and Prevention Control
- Vulnerability Management
- Network Security
- Behavioral Analytics

Slide 26 of 32 English (United States) Accessibility Investigate

Unmute Start Video Security Participants Chat Share Screen Raise Hand Pause/Stop Recording Apps More

Type here to search

35°C 14:44 01-04-2022

Zoom Meeting

You are viewing Priyanka Tomar's screen

View Options

Priyanka Tomar

JCBUST.YMCA

19001003021_Ashish

19001003046_harsh H

19001003005_AJAY

19001003014_ANSHU...

Recording...

PowerPoint

File Edit View Insert Format Arrange Tools Slide Show Window Help

Home Insert Draw Design Transitions Animations Slide Show Review View

Play from Start Play from Current Slide Presenter View Custom Show Set Up Slide Show Hide Slide Rehearse Timings Record Slide Show Play Narrations Use Timings Show Media Controls

Drawbacks and Limitations

AI technology presents some limitations that prevent it from becoming a mainstream security tool.

- Expensive Resources
- Data sets
- Hackers use AI
- Deterioration of digital privacy
- Neural fuzzing

Slide 28 of 32 English (United States) Accessibility Investigate

Unmute Start Video Security Participants Chat Share Screen Raise Hand Pause/Stop Recording Apps More

Type here to search

35°C 14:49 01-04-2022