



# LAKIREDDY BALIREDDY COLLEGE OF ENGINEERING

(AUTONOMOUS)

L B Reddy Nagar, Mylavaram, Krishna District, Andhra Pradesh-52123

Affiliated to JNTUK, Kakinada & Approved by AICTE, New Delhi.

## DEPARTMENT OF CSE (ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)

### Six Days Online Faculty Development Program Report

*On*

## AI-DRIVEN CYBERSECURITY FOR SECURE FINANCIAL TRANSACTION

**Organized by:**

**DEPARTMENT OF CSE (ARTIFICIAL INTELLIGENCE AND  
MACHINE LEARNING)**

**DEPARTMENT OF INFORMATION TECHNOLOGY  
DEPARTMENT OF MASTER OF BUSINESS ADMINISTRATION**

### Date & Venue

- **Date:** 27-04-2026 to 02-05-2026
- **Mode:** Online
- **Organized by:** Department of CSE (AI & ML), IT, MBA

### Objective of the FDP

The six-day Faculty Development Program (FDP) on “**AI-Driven Cybersecurity for Secure Financial Transaction**” was organized to provide participants with comprehensive knowledge of emerging cybersecurity threats, AI-based defense mechanisms, secure digital payment systems, and modern financial security frameworks. The FDP aimed to enhance the technical competence of faculty members, researchers, industry professionals, and students in the domain of AI-enabled cybersecurity technologies for secure financial ecosystems.

### The program focused on:

- Understanding cybersecurity challenges in digital financial transactions.
- Exploring Artificial Intelligence and Machine Learning applications in cybersecurity.
- Learning secure transaction protocols and fraud detection techniques.
- Developing awareness about blockchain security, data privacy, and cyber laws.
- Encouraging research and innovation in secure financial technologies.

### Outcomes of the FDP

After completing the FDP, participants were able to:

- Understand cybersecurity challenges in digital financial systems.

- Apply AI and ML techniques for fraud detection and secure transactions.
- Gain knowledge of blockchain technology and secure payment architectures.
- Implement cryptographic methods and data protection mechanisms.
- Analyze cyber threats and incident response strategies.
- Explore research opportunities in AI-driven cybersecurity.

**DAY1: 27-04-2026**

**LAKIREDDY BALI REDDY**  
**COLLEGE OF ENGINEERING(A)**

**Resource Person**

**Dr.N.Vijayaraj**  
Assistant Professor  
VelTech University

**27-04-2026**

**Online FDP On**

**1:30 PM : 4:00 PM**

**AI-DRIVEN CYBERSECURITY FOR SECURE FINANCIAL TRANSACTIONS**

**Jointly Organized by Department of CSE(AI&ML), IT and MBA**

Digital financial systems have transformed the way people and organizations conduct transactions, manage accounts, and access financial services. Online banking, mobile payment applications, digital wallets, cryptocurrencies, and cloud-based financial platforms provide speed, convenience, and global connectivity. However, the rapid growth of digital finance has also increased cybersecurity risks. Financial institutions are prime targets for cybercriminals because they handle sensitive customer information and large volumes of money.

One major cybersecurity challenge is **data breaches**. Hackers attempt to gain unauthorized access to financial databases containing personal and banking information such as account numbers, passwords, and credit card details. A successful breach can lead to identity theft, financial fraud, and loss of customer trust. Financial organizations must therefore invest heavily in encryption, secure authentication systems, and continuous monitoring to protect data.

Another significant issue is **phishing attacks**. Cybercriminals often use fake emails, websites, or messages to trick users into revealing confidential information. Since many customers rely on digital banking and online transactions, phishing attacks have become more sophisticated and difficult to detect. Employees and customers need regular cybersecurity awareness training to identify suspicious activities and avoid scams.

**Ransomware attacks** also pose a serious threat to digital financial systems. In these attacks, malicious software locks or encrypts important files and systems until a ransom is paid. Financial institutions may experience service disruptions, financial losses, and reputational damage if their systems are compromised. Strong backup systems, network security, and rapid incident response strategies are essential to minimize the impact of ransomware.

The rise of **mobile banking and digital payment systems** has created additional vulnerabilities. Mobile applications can be targeted through malware, insecure Wi-Fi connections, or weak passwords. If proper security measures are not implemented, attackers may intercept transactions or

steal user credentials. Multi-factor authentication and secure mobile app development help reduce these risks.

Another challenge is the increasing use of **cloud computing** in financial services. While cloud platforms improve scalability and efficiency, they also introduce concerns related to data privacy, access control, and third-party security. Financial institutions must ensure that cloud service providers comply with strict cybersecurity standards and regulatory requirements.

**Insider threats** are also important cybersecurity concerns. Employees or contractors with access to sensitive systems may intentionally or unintentionally expose confidential information. Organizations need strict access controls, monitoring systems, and clear cybersecurity policies to reduce insider risks.

In addition, the rapid growth of **cryptocurrency and blockchain technologies** has introduced new cybersecurity issues. Although blockchain offers transparency and security, cryptocurrency exchanges and digital wallets are often targeted by hackers. Weak security protocols can result in major financial losses.

To address these cybersecurity challenges, financial institutions must adopt a comprehensive cybersecurity strategy. This includes implementing advanced technologies such as artificial intelligence for threat detection, conducting regular security audits, updating software systems, and ensuring compliance with financial regulations. Collaboration between governments, financial institutions, and cybersecurity experts is also necessary to strengthen the security of digital financial ecosystems.

In conclusion, cybersecurity is a critical aspect of digital financial systems. As technology continues to evolve, cyber threats are becoming more advanced and frequent. Protecting digital financial systems requires continuous innovation, strong security practices, and increased awareness among both organizations and users. Effective cybersecurity measures are essential to maintain trust, stability, and safety in the digital financial world.

The screenshot shows a Zoom meeting interface. At the top, the time is 21:55. The meeting controls include 'Take control', 'Chat', 'People' (18), 'Raise', 'React', 'View', 'More', 'Camera', 'Mic', 'Share', and 'Leave'. The main content is a slide titled 'What is Cryptocurrency?' with the NAAC A++ logo on the left and a university logo on the right. The slide text reads: 'A cryptocurrency is not a type of currency that can be used in the real world. It can be used to perform transactions only in the digital world. So in order to buy/sell using a cryptocurrency, it has to be converted from a digital form to some existing currency that is used in the real world. For example, Dollars, Rupees, etc. Cryptocurrencies don't have a central issuing authority instead using a decentralized system to record transactions and issue new units.' Below the text is a diagram: a circle with the Rupee symbol (₹) labeled 'Virtual Money', a padlock labeled 'Cryptography Algorithm', a circle with three people icons labeled 'Decentralized Network Design', and a Bitcoin symbol (₿) labeled 'Cryptocurrency'. The diagram is connected by plus signs and an equals sign. The source 'Fintra.co.in' is at the bottom right of the slide. On the right side of the Zoom window, there is a grid of participant avatars: MK (Michael Vi...), AN (Annam-Na...), V (vijaycseraj...), DB (Dr Rajend...), DM (Dr.Chaitan...), PV (PILLI VEER...), NV (Narendre...), DJ (Dr.RAJEN...), MR (Mr. Torlap...), and D (Dr.Salma...).

44:47

Take control Chat People Raise React View More Camera Mic Share Leave

## Types of Blockchain

The diagram illustrates four types of blockchain in two overlapping circles: Permissionless (left) and Permissioned (right).

- Public** (in the Permissionless circle): Administered by no single entity.
- Hybrid** (in the intersection): Administered by single entity with some public oversight.
- Private** (in the Permissioned circle): Administered by single entity.
- Consortium** (in the Permissioned circle): Administered by group of organizations.

SR Sandiredd... DB Dr Rajend...  
 AN aswini net... VB venkalah c...  
 V vijaycseraj... NV Narendra...  
 D Dr.sesikal... S Sumalatha...  
 AN Annam Na...  
 D Dr.Salma

vijaycseraj@gmail.com

34:36

Take control Chat People Raise React View More Camera Mic Share Leave

## What is Blockchain Technology

- Bitcoin stores all its transactions onto a public database called as Blockchain
- There are many definitions available, from each one lookout, as this is not Physics. However, the simplest in layman's term is:
- Blockchain is a distributed ledger available as replicated copies with the members of the Peer to Peer Network. The ledger entries are immutable, tamperproof, secured, transparent and auditable. The ledger entries are chained according to timestamp; can be accessed by anyone who has appropriate permissions
- Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, a car, cash, land) or intangible (intellectual property, patents, copyrights, branding).

The diagram shows a sequence of three blocks. Each block contains 'Transactions and other data' and is linked to the previous block by a 'Previous hash'. The first block is labeled '(Genesis Block)'.

SR Sandiredd... DB Dr Rajend...  
 AN aswini net... VB venkalah c...  
 V vijaycseraj... NV Narendra...  
 D Dr.sesikal... MJ MOTIPALL...  
 PV PILLI VEER...  
 D Dr.Salma

vijaycseraj@gmail.com

03:27

Take control Chat People Raise React View More Camera Mic Share Leave

The diagram illustrates two types of Denial of Service (DoS) attacks:

- Direct DoS Attack:** An Attacker sends a direct DoS attack to a Target.
- Distributed Denial of Service (DDoS) Attack:** An Attacker sends traffic through the Internet to multiple ZOMBIES, which then attack the Target Server.

Unmute mic (Ctrl+Shift+M)

SR Sandiredd... DB Dr Rajend...  
 AN aswini net... VB venkalah c...  
 V vijaycseraj... NV Narendra...  
 D Dr.sesikal... MJ MOTIPALL...  
 PV PILLI VEER...  
 D Dr.Salma

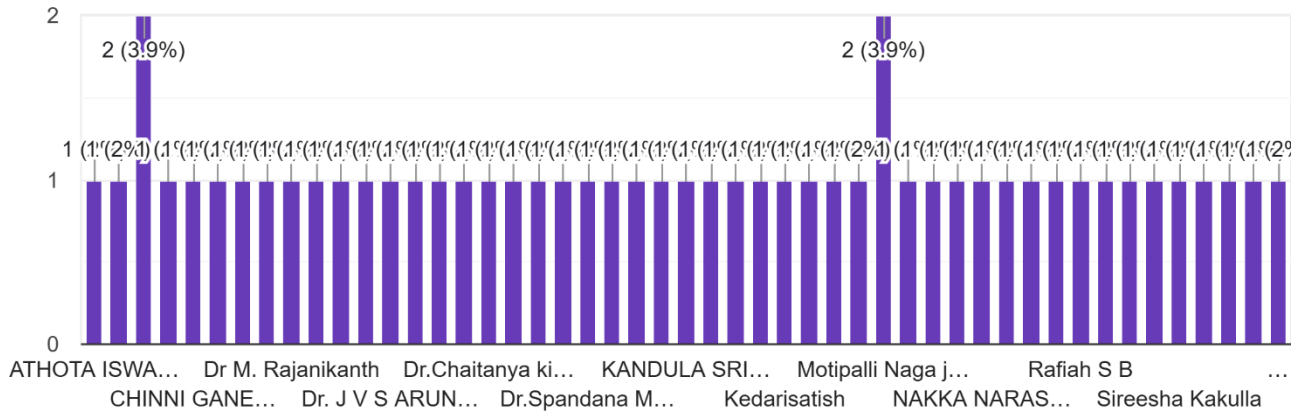
vijaycseraj@gmail.com 27/2026

13

# Feedback

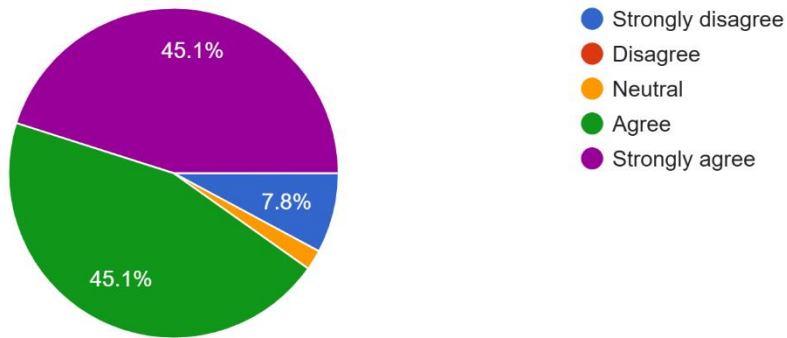
## Name of the Faculty

51 responses



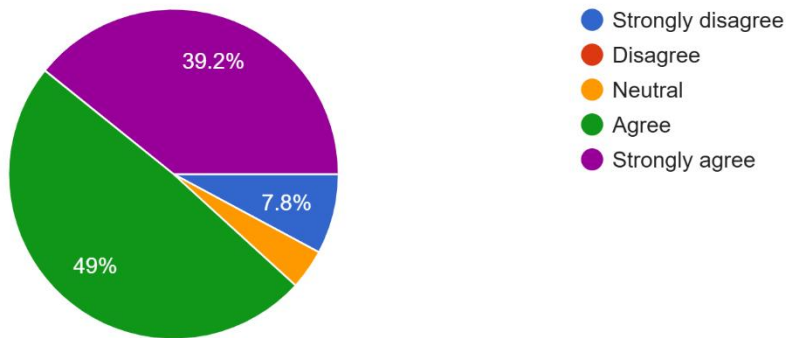
## The course contents met with your expectations

51 responses



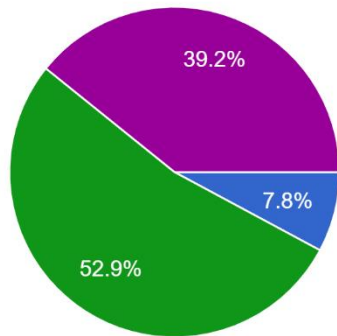
## The lecture sequence was well planned

51 responses



The course exposed you to new knowledge and practices

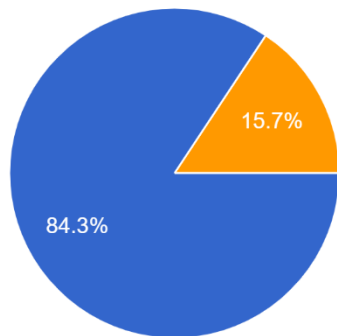
51 responses



- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

Will you recommend this course to your colleagues?

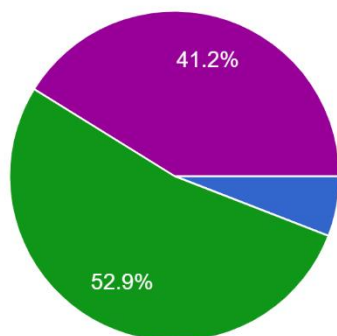
51 responses



- Yes
- No
- Maybe

The lectures were clear and easy to understand

51 responses



- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

**LAKIREDDY BALI REDDY**  
**COLLEGE OF ENGINEERING(A)**

**Resource Person**

**Dr. T. Kamaleshwar**  
Associate Professor  
VelTech University

**28-04-2026**

**Online FDP On**

**1:30 PM : 4:00 PM**

**AI-DRIVEN CYBERSECURITY FOR SECURE FINANCIAL TRANSACTIONS**

**Jointly Organized by Department of CSE(AI&ML), IT and MBA**

### Zero Trust Vulnerability

Zero Trust is a cybersecurity model based on the principle of “**never trust, always verify.**” It assumes that threats can exist both inside and outside an organization’s network. Therefore, every user, device, application, and connection must be continuously authenticated and authorized before access is granted. Although the Zero Trust model significantly improves security, it also has certain vulnerabilities and challenges that organizations must address.

One major vulnerability in Zero Trust systems is **misconfiguration**. Zero Trust environments involve complex policies, identity controls, and access management settings. If administrators incorrectly configure permissions or security rules, attackers may exploit these weaknesses to gain unauthorized access. Human error remains a significant cybersecurity risk.

Another challenge is **identity-based attacks**. Since Zero Trust relies heavily on user authentication and identity verification, compromised credentials can become a major vulnerability. Cybercriminals may use phishing, password theft, or social engineering techniques to steal login information. If multi-factor authentication is weak or bypassed, attackers can impersonate legitimate users.

**Insider threats** also remain a concern in Zero Trust architecture. Employees or trusted users with legitimate access may intentionally or unintentionally misuse sensitive information. Although Zero Trust limits unnecessary access, insiders with approved permissions can still cause damage if monitoring systems are insufficient.

A further vulnerability involves **endpoint security**. Zero Trust assumes that devices connecting to the network are secure, but infected or outdated devices may still introduce malware or ransomware into the system. Organizations must continuously monitor and update all endpoints, including laptops, smartphones, and IoT devices.

**Third-party integrations and cloud services** can also create weaknesses. Many organizations depend on external vendors and cloud providers for applications and infrastructure. If these third-party services have security flaws, attackers may exploit them to bypass Zero Trust protections.

Another issue is **performance and complexity**. Implementing Zero Trust requires continuous authentication, monitoring, and verification of all network activities. This can increase system

complexity and create delays in access or communication. Poor implementation may reduce productivity and encourage users to bypass security controls.

Additionally, **advanced persistent threats (APTs)** may still evade Zero Trust systems. Skilled attackers can move slowly within a network, using stolen credentials and legitimate tools to avoid detection. Without strong behavioral analytics and real-time monitoring, such attacks may remain unnoticed.

To reduce Zero Trust vulnerabilities, organizations should:

- Use strong multi-factor authentication (MFA)
- Regularly update and patch systems
- Conduct continuous security monitoring
- Apply least-privilege access controls
- Train employees on cybersecurity awareness
- Perform regular security audits and penetration testing

In conclusion, Zero Trust is an effective cybersecurity framework that enhances protection in modern digital environments. However, it is not completely immune to vulnerabilities. Proper implementation, continuous monitoring, and strong security practices are necessary to ensure the effectiveness of a Zero Trust security model.

The screenshot shows a presentation slide titled "The Future of Cyber-Resilient Finance" with the subtitle "// SUMMARY & KEY TAKEAWAYS". The slide features six key takeaways in a 2x3 grid:

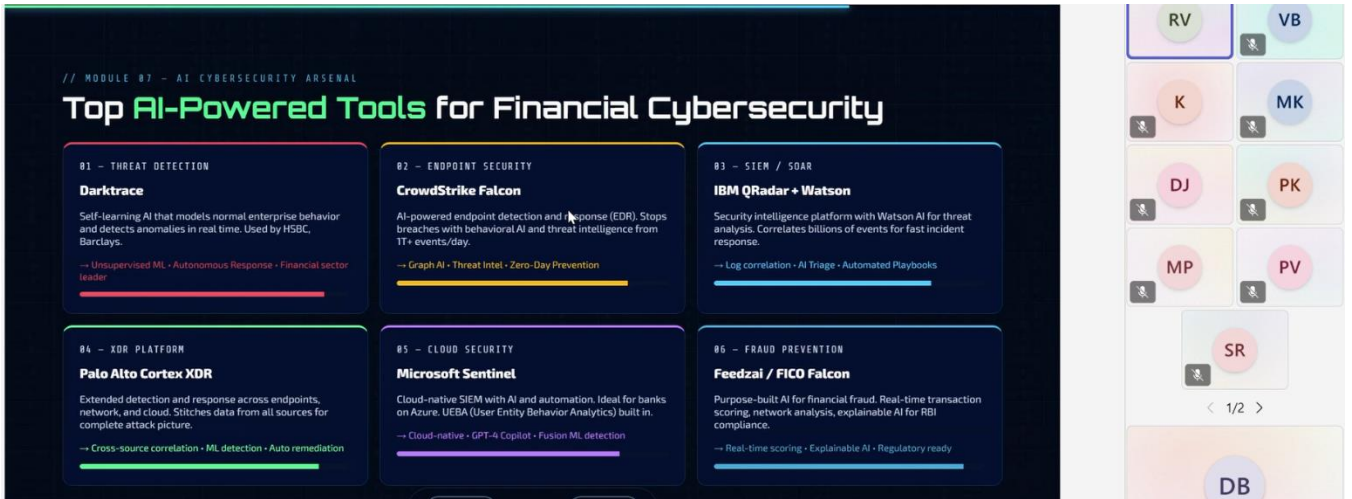
- AI is Both Risk & Remedy**: AI enables sophisticated attacks — but also our most powerful defense layer.
- Zero Trust is Non-Negotiable**: Every bank must move from perimeter to identity-centric Zero Trust architecture.
- Govern Shadow AI Now**: Employees are already using AI. Build governance before a breach forces your hand.
- Zero-Click is Real**: Traditional user training won't stop zero-click. AI behavioral monitoring is the only defense.
- Automate the SOC**: Human analysts can't scale. AI-powered SOAR cuts response time from days to seconds.
- Build AI-Sec Talent**: India needs 1M+ cybersecurity professionals. Engineering curriculum must evolve now.

At the bottom, it says "[ QUESTIONS & DISCUSSION OPEN ] - Thank you for attending" and lists several frameworks: RBI Cybersecurity Framework, CERT-In Guidelines, FCI DSS 4.0, SEBI Cybersecurity Circular, and NIST CSF 2.0.

The screenshot shows a presentation slide titled "Shadow AI – The Threat Within" with the subtitle "// MODULE 04 – EMERGING THREAT". The slide is divided into four main sections:

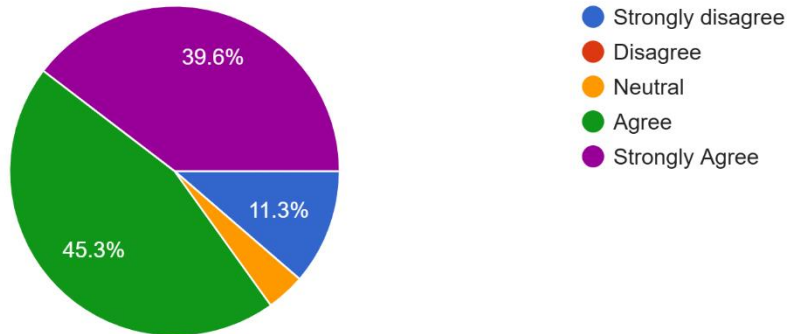
- What is Shadow AI?**: Unauthorized AI tools used by employees **without IT department approval**. Just as "Shadow IT" brought personal devices and cloud storage, Shadow AI introduces uncontrolled AI into the enterprise.
- Security Risks**:
  - **Data Exfiltration**: Sensitive data used to train external models
  - **Regulatory Violation**: RBI, SEBI, GDPR, PCI-DSS breaches
  - **Model Poisoning**: Bad data via unauthorized tools corrupts internal AI
  - **IP Theft**: Proprietary algorithms exposed to third parties
  - **Loss of Audit Trail**: No logging, no oversight, no accountability
- Real-World Examples**:
  - Analyst pastes **customer financial records** into ChatGPT for a quick summary
  - Developer uses personal AI coding tool on **proprietary banking algorithm**
  - Loan officer uses AI chatbot that **stores PII data on external servers**
  - HR uses unauthorized AI to **process payroll data** violating GDPR/RBI norms
- How to Combat Shadow AI**:
  - AI Usage Policy & approved tool list
  - DLP (Data Loss Prevention) tools monitoring AI traffic
  - Network-level blocking of unauthorized AI endpoints
  - Employee awareness training on Shadow AI risks

At the bottom, it lists the "AI Governance Framework".



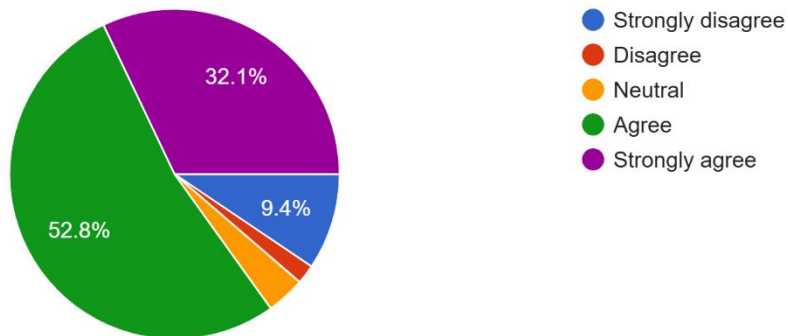
The content were relevant to the sessions within the program

53 responses



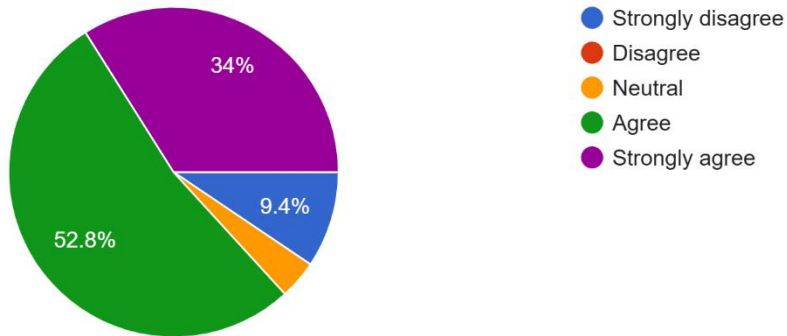
The presentations were effective

53 responses



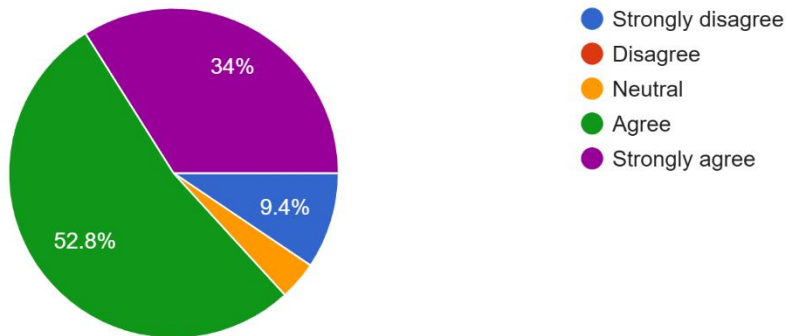
The program enhanced your teaching, research, or administrative skills/knowledge

53 responses



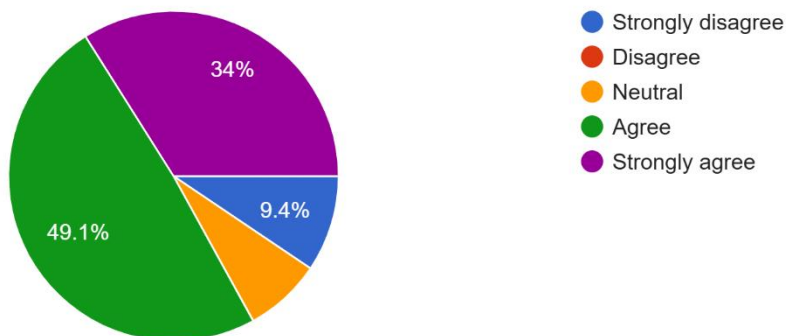
The program enhanced your teaching, research, or administrative skills/knowledge

53 responses



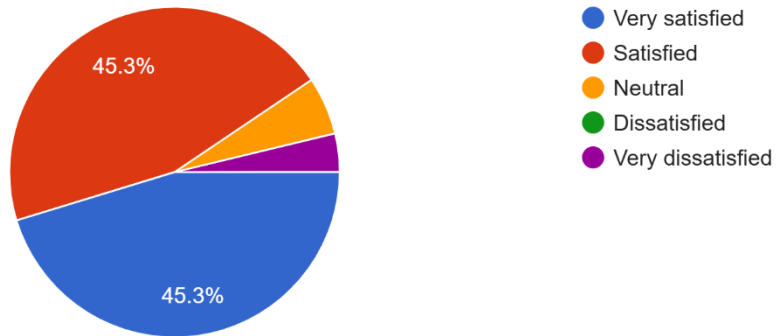
The program enhanced your teaching methodologies and pedagogical approaches

53 responses



Overall how satisfied are you with the Faculty Development Program?

53 responses



DAY3: 29-04-2026

**LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING(A)**

**Resource Person**

**Ramesh Vudata**  
Founder-KodeKnow  
Kuala Lumpur , Malaysia

**29-04-2026**

**Online FDP On**

**1:30 PM : 4:00 PM**

**AI-DRIVEN CYBERSECURITY FOR SECURE FINANCIAL TRANSACTIONS**

**Jointly Organized by Department of CSE(AI&ML), IT and MBA**

## AI in Financial Security

Artificial Intelligence (AI) plays an increasingly important role in improving security within the financial sector. Banks, insurance companies, digital payment platforms, and financial institutions use AI technologies to detect threats, prevent fraud, and protect sensitive customer information. As digital financial systems continue to grow, AI has become a powerful tool for strengthening cybersecurity and enhancing trust in financial services.

One of the most important applications of AI in financial security is **fraud detection**. Traditional fraud detection methods often rely on fixed rules and manual monitoring, which may fail to identify advanced cyber threats. AI systems can analyze large volumes of transaction data in real time and identify unusual patterns or suspicious behavior. For example, if a customer suddenly makes transactions from different countries within a short period, AI can immediately flag the activity and prevent possible fraud.

AI is also widely used in **risk management**. Financial institutions use machine learning algorithms to predict risks related to loans, investments, and cybersecurity attacks. These systems can study historical data, customer behavior, and market trends to identify potential threats before they cause damage. Predictive analysis helps organizations make faster and more accurate decisions.

Another important use of AI is in **cyber threat detection and prevention**. AI-powered security systems continuously monitor networks, applications, and devices for unusual activities. Unlike traditional systems, AI can learn from new attack patterns and adapt to evolving cyber threats such as malware, ransomware, and phishing attacks. This improves the ability of financial institutions to respond quickly to security incidents.

**Biometric authentication** is another AI-driven security solution. Many banks and financial applications now use facial recognition, fingerprint scanning, and voice recognition to verify customer identities. AI enhances the accuracy and speed of these authentication methods, reducing the risk of unauthorized access and identity theft.

AI also supports **anti-money laundering (AML)** and **compliance monitoring**. Financial institutions are required to follow strict regulations to prevent illegal activities such as money laundering and terrorist financing. AI systems can analyze transaction patterns, detect suspicious activities, and automatically generate alerts for further investigation. This reduces manual workload and improves regulatory compliance.

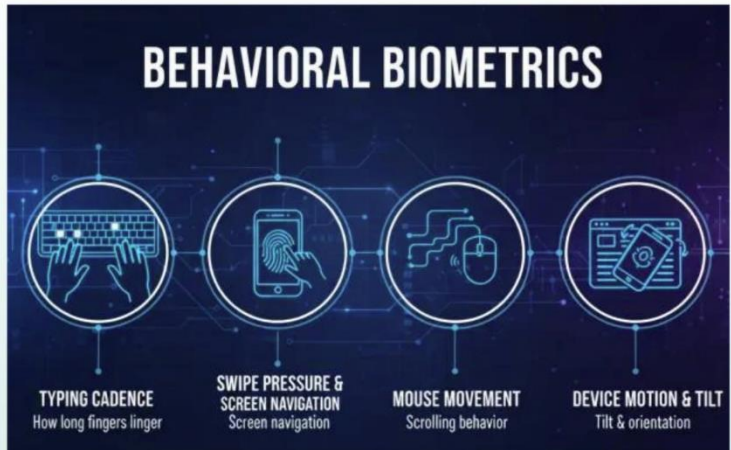
In addition, AI-powered **chatbots and virtual assistants** improve customer security by helping users report fraud, monitor account activities, and receive instant security support. These systems provide quick responses while maintaining secure communication channels.

Despite its advantages, AI in financial security also faces certain challenges. Cybercriminals can use AI to create more advanced attacks, such as AI-generated phishing messages or deepfake fraud. AI systems may also produce false positives or biased decisions if trained on poor-quality data. Furthermore, protecting customer privacy and ensuring ethical use of AI remain important concerns. To maximize the benefits of AI in financial security, organizations should:

- Use high-quality and secure data for AI training
- Regularly update AI models to detect new threats
- Combine AI systems with human expertise
- Implement strong data privacy and ethical standards
- Conduct continuous monitoring and testing of AI systems

In conclusion, AI has transformed financial security by providing faster, smarter, and more efficient methods for detecting fraud, managing risks, and protecting digital financial systems. As cyber threats continue to evolve, AI will remain a key technology in ensuring the safety, reliability, and stability of the global financial sector.

### AI in Financial Security



RV VB

K MK

DJ PK

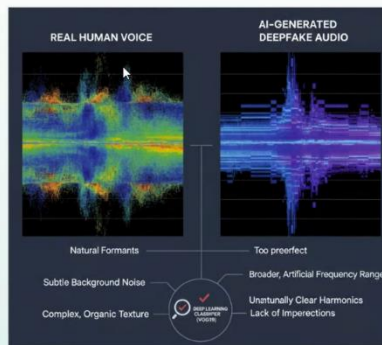
MP

DB

### 1. Voice Deepfake (Audio Cloning)

1. AI can clone a person's voice from just a few seconds of audio
2. Used in scams: "urgent money transfer" calls pretending to be boss/family
3. Hard to detect because tone, accent, emotion feel real

**Risk:** Real-time financial fraud (especially in banking/UPI scenarios)



RV VB

K MK

DJ PK

MP PV

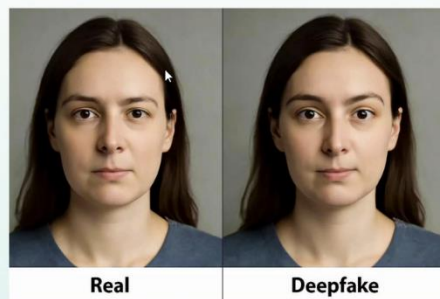
SR

DB

### 1. Voice Deepfake (Audio Cloning)

1. AI generates or alters faces to create fake identities
2. Used for:
3. Fake KYC verification
4. Social media impersonation
5. Can bypass basic facial recognition systems

**Risk:** Identity theft + account takeover



RV VB

K MK

DJ PK

MP PV

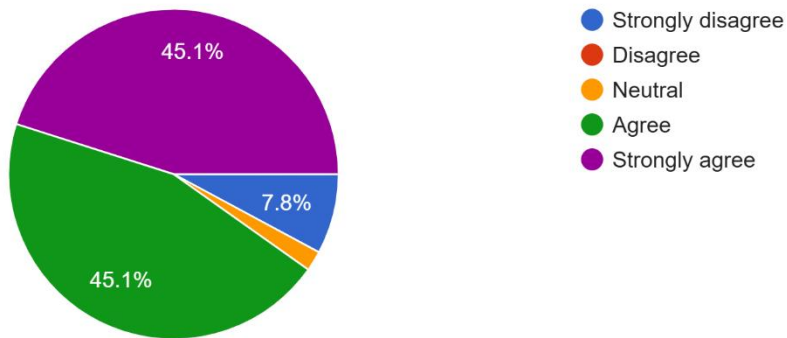
SR

DB



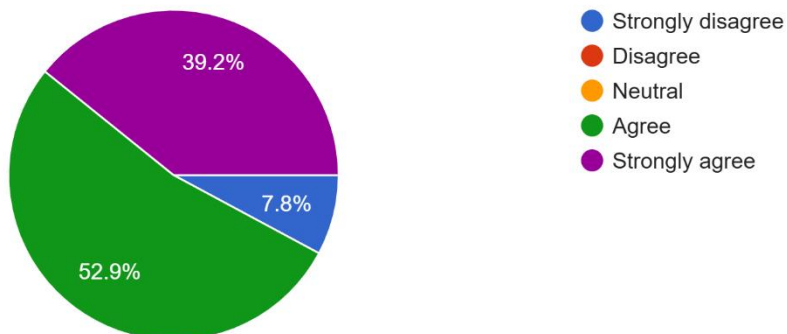
The course contents met with your expectations

51 responses



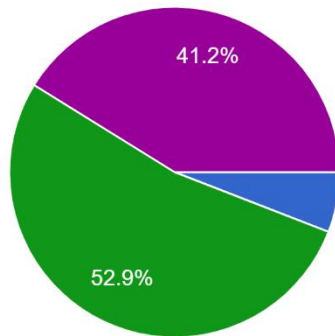
The course exposed you to new knowledge and practices

51 responses



The lectures were clear and easy to understand

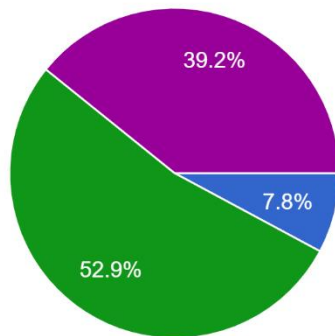
51 responses



- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

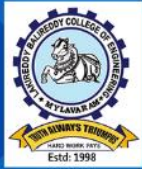
The course exposed you to new knowledge and practices

51 responses



- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

**DAY4: 30-04-2026**



# LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING(A)



**Resource Person**



**ANJA NARESH PADAVALA**  
Enterprise AI Architect



**30-04-2026**

**Online FDP On**



**1:30 PM : 4:00 PM**

**AI-DRIVEN CYBERSECURITY FOR SECURE FINANCIAL TRANSACTIONS**

**Jointly Organized by Department of CSE(AI&ML), IT and MBA**

## **Enterprise Security, Cybersecurity, and AI**

Enterprise security refers to the strategies, technologies, and practices used by organizations to protect their systems, networks, data, and digital assets from unauthorized access, cyberattacks, and other security threats. In today's digital world, businesses increasingly depend on technology and online services, making cybersecurity and Artificial Intelligence (AI) essential components of enterprise security.

### **Enterprise Security**

Enterprise security focuses on safeguarding an organization's entire infrastructure, including employees, devices, applications, databases, and cloud systems. Its main objective is to ensure confidentiality, integrity, and availability of information. Enterprise security includes:

- Access control systems

- Network security
- Data protection
- Endpoint security
- Identity and authentication management
- Security policies and compliance

Organizations use firewalls, encryption, intrusion detection systems, and multi-factor authentication to protect sensitive information and prevent unauthorized access.

### Cybersecurity in Enterprises

Cybersecurity is a critical part of enterprise security. It involves protecting computer systems, networks, and digital data from cyber threats such as:

- Malware
- Ransomware
- Phishing attacks
- Data breaches
- Insider threats
- Denial-of-service (DoS) attacks

As businesses move toward cloud computing, remote work, and digital financial systems, cyber threats have become more advanced and frequent. Cybersecurity helps organizations identify vulnerabilities, monitor suspicious activities, and respond quickly to attacks.

Key cybersecurity practices in enterprises include:

- Regular software updates and patch management
- Employee cybersecurity awareness training
- Strong password and authentication policies
- Security audits and penetration testing
- Backup and disaster recovery planning

### Role of AI in Enterprise Cybersecurity

Artificial Intelligence (AI) is transforming enterprise cybersecurity by improving threat detection, automation, and decision-making. AI systems can analyze huge amounts of data much faster than humans and identify unusual patterns that may indicate cyberattacks.

### Applications of AI in Cybersecurity

1. **Threat Detection and Monitoring**  
AI continuously monitors networks and systems to detect suspicious behavior in real time. Machine learning algorithms can identify unknown threats and zero-day attacks.
2. **Fraud Prevention**  
AI helps organizations detect fraudulent transactions, account misuse, and unauthorized access by analyzing user behavior and transaction patterns.
3. **Automated Incident Response**  
AI-powered systems can automatically isolate infected devices, block malicious traffic, and respond to security incidents quickly, reducing damage.
4. **Phishing Detection**  
AI can identify fake emails, malicious websites, and suspicious messages that may trick employees into revealing sensitive information.
5. **Behavioral Analytics**  
AI studies user and device behavior to detect anomalies. For example, if an employee suddenly accesses confidential data at unusual hours, the system may generate a security alert.
6. **Predictive Security**  
AI helps predict potential vulnerabilities and future attacks by analyzing historical threat data and trends.

### Challenges of AI in Cybersecurity

Although AI improves enterprise security, it also introduces challenges:

- AI systems may generate false alarms
- Poor-quality data can reduce accuracy
- Cybercriminals can use AI for advanced attacks
- AI models may be vulnerable to manipulation
- Privacy and ethical concerns may arise

Organizations must combine AI technologies with human expertise and strong cybersecurity policies to ensure effective protection.

### Future of Enterprise Security with AI

The future of enterprise security will increasingly depend on AI-driven technologies. Advanced AI systems will provide faster threat detection, automated defense mechanisms, and improved risk management. Technologies such as Zero Trust Architecture, cloud security, and AI-powered analytics will become essential for protecting modern enterprises.

### Conclusion

Enterprise security, cybersecurity, and AI are closely connected in today’s digital environment. Cybersecurity protects organizations from evolving digital threats, while AI enhances the speed and efficiency of security operations. By combining strong security practices with intelligent AI systems, enterprises can improve protection, reduce risks, and maintain trust in the digital age.

The screenshot shows a Zoom meeting interface. The main content is a slide titled "Enterprise Security, Cybersecurity to AI: How Digital Systems (IT), Factory Floor Systems (OT) Stay Secure". The slide includes a "SESSION INTRODUCTION" header, a central graphic of a shield and a brain, and a "WHAT WE'LL COVER" section with six topics: Security, Cybersecurity; CIA Triad; Enterprise Security; Cybersecurity Architecture & Principles; Enterprise Security Use cases; and Cybersecurity AI & Gen AI. The presenter is identified as Anja Naresh Padavala, Enterprise Strategist & AI Architect. The Zoom toolbar at the top shows various controls like Take control, Chat, People (15), Raise, React, View, More, Camera, and Leave. A participant list on the right shows names like Anja Naresh, Nandini A., and others.

The screenshot shows a Zoom meeting interface. The main content is a slide titled "A Simple Situation..." which illustrates a social engineering attack scenario in four steps: 01. You receive a message; 02. You panic; 03. You click; 04. You enter details. The slide includes a Microsoft OneDrive advertisement and two questions: "Was the system insecure?" and "Or was the user tricked?". The Zoom toolbar at the top shows various controls like Take control, Chat, People (16), Raise, React, View, More, Camera, and Leave. A participant list on the right shows names like Anja Naresh, Nandini A., and others.

18:09

Take control Chat People 16 Raise React View More Camera Share Leave

### A Simple Situation...

**01** You receive a message  
"Click this link now and provide the details, otherwise your bank account will be blocked"

**02** You panic  
Fear kicks in. You think you must act immediately or lose everything.

**03** You click  
One tap on the link — it opens a convincing-looking fake page.

**04** You enter details  
Name, card number, OTP — all handed over willingly.

**QUESTION 1**  
Was the system insecure?  
The bank's servers were running fine. None of the security layers were breached.

**QUESTION 2**  
Or was the user tricked?  
The attacker exploited fear and urgency — not code.

Microsoft OneDrive  
062809  
Extra protection for your most important files  
Learn more  
Sponsored by Microsoft  
To remove ads, subscribe to Microsoft 365. See benefits.

Unmute mic (Ctrl+Shift+M)

AP Anja Nare... NA Nandini A...  
KN k.aswini n... DB Dr.Rajend...  
VB venkaiah c... VB V.Narendr...  
MK Michael Vi... MH M.HAVILA...  
HK HYMAVAT...  
D

31:24

Take control Chat People 20 Raise React View More Camera Share Leave

### Putting it all together.

**CYBER** + **SECURITY** = **CYBERSECURITY**

**CS**  
Protecting the digital domain from threats

**DEFINITION**  
Cybersecurity is the practice of defending computers, servers, mobile devices, networks, and data from malicious digital attacks - acting as a digital security system for your virtual life.

**THE KEY INSIGHT — IT'S ALWAYS LAYERED**

**Layer 1**  
Fence  
→ Firewall  
Keeps attackers away from the boundary

**Layer 2**  
Locked Door  
→ Password / Encryption  
Stops entry even if they reach the door

**Layer 3**  
Alarm System  
→ Antivirus / Monitoring  
Detects & alerts if something gets through

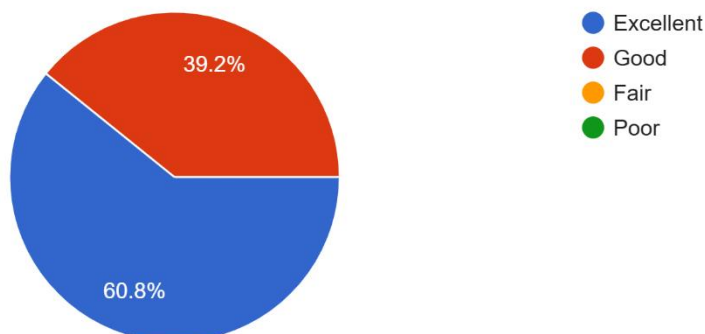
Cybersecurity is not just for experts. It's a layered defence - fence + locked door + alarm - making it harder for the wrong people to reach your information.

Unmute mic (Ctrl+Shift+M)

AP Anja Nare... NA Nandini A...  
DB Dr.Rajend... VB venkaiah c...  
VB V.Narendr... MK Michael Vi...  
HK HYMAVAT... SR SANKARA...  
GS Gunti Sur...  
D

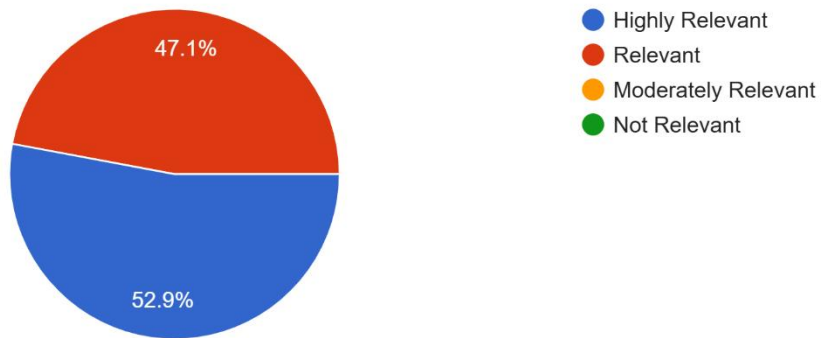
How would you rate the overall quality of the Session

51 responses



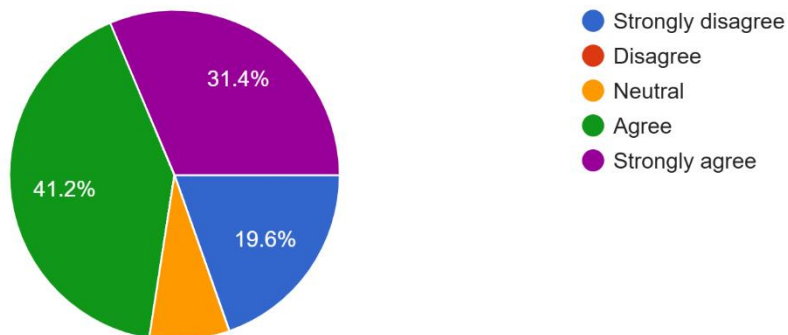
How relevant was the FDP content to your academic/research/industry needs?

51 responses



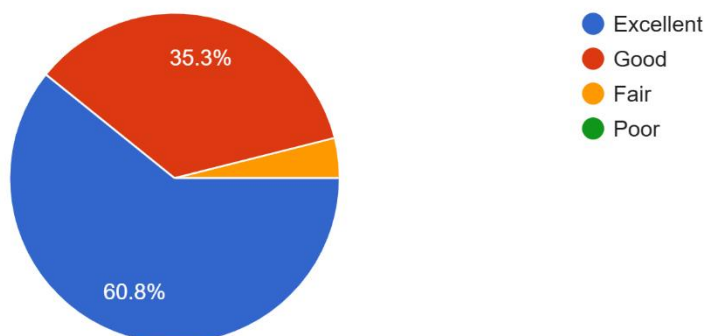
The topics covered (AI in Cybersecurity, Fraud Detection, Secure Transactions, etc.) were

51 responses



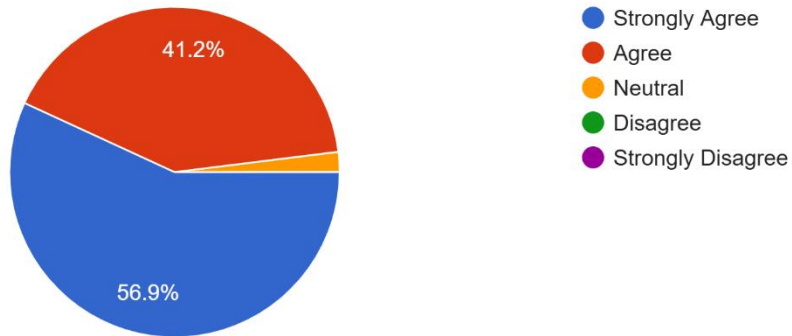
How do you rate the knowledge and expertise of the speakers?

51 responses



The FDP enhanced my understanding of AI in cybersecurity

51 responses



**DAY5: 01-05-2026**

A promotional banner for a Faculty Development Program (FDP) at Lakireddy Bali Reddy College of Engineering (A). The banner features the college's logo on the left and the Institution's Innovation Council logo on the right. The central text identifies the resource person as Mr. P. Chandra Tej, Technical Product Manager at PepsiCo India. The event is scheduled for 01-05-2026 from 1:30 PM to 4:00 PM. The topic is 'AI-DRIVEN CYBERSECURITY FOR SECURE FINANCIAL TRANSACTIONS', and it is jointly organized by the Department of CSE(AI&ML), IT, and MBA. A portrait of Mr. P. Chandra Tej is shown in a circular frame.

**LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING(A)**

**Resource Person**

**Mr. P. Chandra Tej**  
Technical Product Manager  
**PepsiCo India**

**01-05-2026**

**Online FDP On**

**1:30 PM : 4:00 PM**

**AI-DRIVEN CYBERSECURITY FOR SECURE FINANCIAL TRANSACTIONS**

**Jointly Organized by Department of CSE(AI&ML), IT and MBA**

## **NLP in Security**

Natural Language Processing (NLP) is a branch of Artificial Intelligence (AI) that enables computers to understand, analyze, interpret, and generate human language. In cybersecurity and enterprise security, NLP plays an important role in detecting threats, analyzing security data, improving communication, and automating security operations. As cyber threats become more advanced, NLP helps organizations process large amounts of text-based information quickly and efficiently.

### **Role of NLP in Security**

Security systems generate huge volumes of text data every day, including emails, chat messages, security logs, reports, and threat intelligence feeds. NLP helps organizations analyze this information to identify risks, suspicious activities, and cyber threats in real time.

### **Applications of NLP in Security**

#### **1. Phishing Detection**

Phishing attacks often use fake emails and messages to trick users into revealing passwords or financial information. NLP can analyze the language, writing style, grammar, and suspicious keywords in emails to detect phishing attempts. AI-powered email filters use NLP to identify malicious messages before they reach users.

#### **2. Threat Intelligence Analysis**

Cybersecurity teams collect threat intelligence from websites, blogs, reports, forums, and social media. NLP helps process and summarize this large amount of text data, allowing analysts to quickly identify new malware, vulnerabilities, and attack techniques.

#### **3. Security Chatbots and Virtual Assistants**

Organizations use NLP-powered chatbots to provide automated security support. These chatbots can answer employee questions, guide users through security procedures, and help report suspicious activities. This improves response time and reduces workload for IT teams.

#### **4. Log and Incident Analysis**

Security systems produce logs and incident reports containing important information about network activities and attacks. NLP can automatically analyze these logs, identify patterns, and classify incidents based on severity. This helps security teams respond faster to threats.

#### **5. Insider Threat Detection**

NLP can analyze employee communications, emails, and behavioral patterns to identify possible insider threats. For example, unusual language or suspicious communication may indicate data theft or policy violations.

#### **6. Malware and Dark Web Monitoring**

Cybercriminals often communicate through forums, chat rooms, and dark web marketplaces. NLP helps monitor these platforms to detect discussions about hacking tools, stolen data, or planned cyberattacks.

#### **7. Compliance and Policy Management**

Organizations must follow cybersecurity regulations and policies. NLP can review legal documents, security policies, and compliance reports to ensure that organizations meet required standards and identify policy violations.

### **Benefits of NLP in Security**

- Faster analysis of large volumes of text data
- Improved threat detection and response

- Automated security monitoring
- Better phishing and fraud prevention
- Enhanced customer and employee support
- Reduced manual workload for security teams

### Challenges of NLP in Security

Despite its advantages, NLP also faces challenges in cybersecurity:

- Understanding complex or hidden language used by attackers
- Detecting sarcasm, slang, or coded communication
- False positives and inaccurate predictions
- Privacy concerns when analyzing communications
- High computational and data requirements

Cybercriminals may also use AI-generated text and advanced language techniques to bypass NLP-based security systems.

### Future of NLP in Cybersecurity

The future of NLP in security is expected to grow rapidly with advancements in AI and machine learning. NLP systems will become more accurate in understanding human language, detecting threats, and automating cybersecurity tasks. Combined with predictive analytics and real-time monitoring, NLP will help organizations strengthen their defense against evolving cyber threats.

### Conclusion

Natural Language Processing is becoming an essential technology in modern cybersecurity and enterprise security systems. By analyzing and understanding human language, NLP helps organizations detect phishing attacks, analyze threats, monitor suspicious activities, and improve security operations. Although challenges remain, NLP continues to enhance the efficiency, speed, and intelligence of cybersecurity solutions in the digital age.

31:24

Take control Chat People Raise React View More Camera Share Leave

Unmute mic (Ctrl+Shift+M)

AP Anja Nare... NA Nandini A... DB Dr.Rajend... VB venkatah c... VB V.Narendr... MK Michael Vi... HK HYMAVAT... SR SANKARA... GS Gunthi Sur... D

1/3

**Putting it all together.**

**THE DEFINITION**

**CYBER**  
The digital domain  
computers, networks, data

**SECURITY**  
Actions taken  
to protect

**CS**  
**CYBERSECURITY**  
Protecting the digital  
domain from threats

**DEFINITION**  
Cybersecurity is the practice of defending computers, servers, mobile devices, networks, and data from malicious digital attacks - acting as a digital security system for your virtual life.

**THE KEY INSIGHT — IT'S ALWAYS LAYERED!**

**Layer 1**  
Fence  
→ Firewall  
Keeps attackers away from the boundary

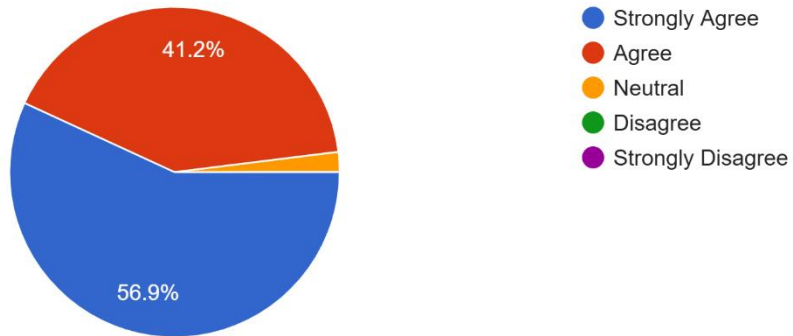
**Layer 2**  
Locked Door  
→ Password / Encryption  
Stops entry even if they reach the door

**Layer 3**  
Alarm System  
→ Antivirus / Monitoring  
Detects & alerts if something gets through

Cybersecurity is not just for experts. It's a layered defence - fence + locked door + alarm - making it harder for the wrong people to reach your information.

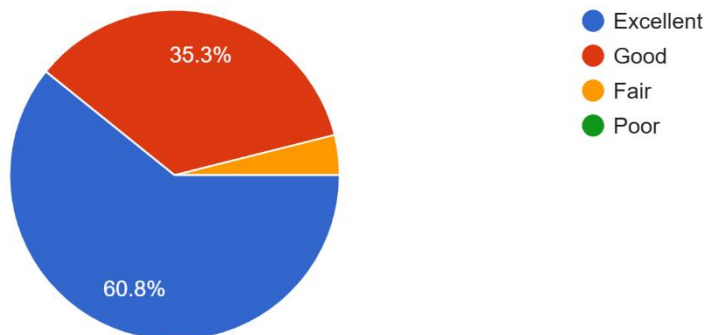
### The FDP enhanced my understanding of AI in cybersecurity

51 responses



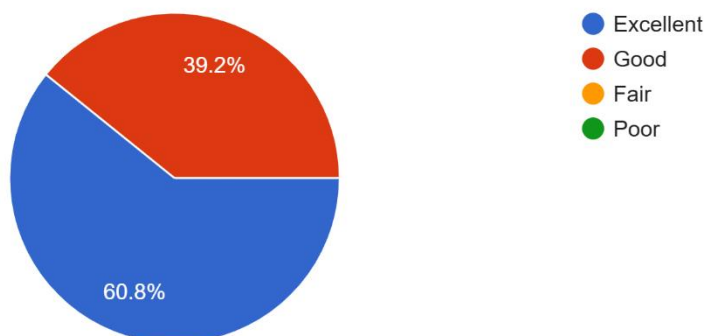
### How do you rate the knowledge and expertise of the speakers?

51 responses



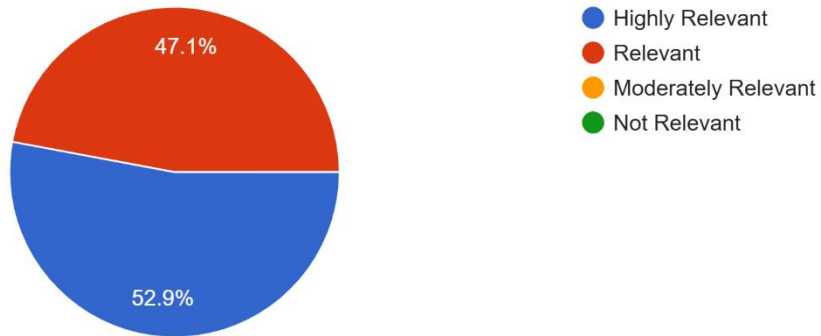
### How would you rate the overall quality of the Session

51 responses



How relevant was the FDP content to your academic/research/industry needs?

51 responses



**DAY6: 02-05-2026**

**LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING(A)**

**Resource Person**

**Mr. Shравan Kumar**  
Scientist-C  
Officer Cyber Advisory,  
DRDO, New Delhi

**02-05-2026**

**Online FDP On**

**1:30 PM : 4:00 PM**

**AI-DRIVEN CYBERSECURITY FOR SECURE FINANCIAL TRANSACTIONS**

**Jointly Organized by Department of CSE(AI&ML), IT and MBA**

## Zero-Day Buffer Overflow Exploitation

A Zero-Day Buffer Overflow Exploitation is a serious cybersecurity attack that takes advantage of a previously unknown software vulnerability involving buffer overflow errors. Because the vulnerability is unknown to the software developer or security community, there is no available patch or defense at the time of the attack. This makes zero-day exploits extremely dangerous and difficult to detect.

### Understanding Buffer Overflow

A buffer overflow occurs when a program writes more data into a memory buffer than it can hold. Buffers are temporary memory storage areas used by software applications. If excessive data is inserted into the buffer, the extra data can overwrite nearby memory locations.

Attackers exploit this weakness by inserting malicious code into the overflowed memory space. This may allow them to:

- Execute unauthorized commands
- Gain system access
- Crash applications
- Steal sensitive data
- Install malware or ransomware

### What is a Zero-Day Vulnerability?

A zero-day vulnerability is a software flaw that is unknown to the software vendor, developers, or users. Since no security patch exists, attackers can exploit the weakness before it is discovered and fixed. The term “zero-day” refers to the fact that defenders have had zero days to prepare or respond.

### How Zero-Day Buffer Overflow Exploitation Works

1. **Discovery** **of** **Vulnerability**  
Attackers identify a hidden flaw in software that improperly handles memory.
2. **Crafting** **Malicious** **Input**  
Specially designed input data is created to overflow the buffer and overwrite memory.
3. **Injection** **of** **Malicious** **Code**  
The attacker places executable code into memory or redirects the program’s execution flow.
4. **Execution** **of** **Exploit**  
Once the vulnerable program processes the malicious input, the attacker gains control over the system or application.
5. **System** **Compromise**  
The attacker may steal data, install malware, create backdoors, or disrupt operations.

### Types of Buffer Overflow Attacks

#### 1. Stack Buffer Overflow

Occurs when attackers overwrite memory in the stack area, often targeting return addresses to redirect program execution.

#### 2. Heap Buffer Overflow

Targets dynamically allocated memory in the heap, potentially corrupting application behavior.

### Risks of Zero-Day Buffer Overflow Exploits

- Unauthorized system access
- Data theft and privacy violations
- Remote code execution
- Financial losses
- Service disruption
- Malware installation
- Damage to organizational reputation

Zero-day exploits are commonly used against:

- Operating systems
- Web browsers
- Banking systems
- Enterprise applications
- IoT devices
- Mobile applications

### **Prevention and Protection Methods**

Organizations can reduce the risk of zero-day buffer overflow attacks through several security measures:

#### **1. Secure Coding Practices**

Developers should validate input, check memory boundaries, and avoid unsafe programming functions.

#### **2. Regular Software Updates**

Keeping systems updated reduces exposure to known vulnerabilities.

#### **3. Address Space Layout Randomization (ASLR)**

ASLR randomizes memory locations, making exploitation more difficult.

#### **4. Data Execution Prevention (DEP)**

DEP prevents malicious code from executing in protected memory areas.

#### **5. Intrusion Detection and Prevention Systems (IDS/IPS)**

These systems monitor suspicious activities and detect unusual exploit behavior.

#### **6. Antivirus and Endpoint Protection**

Modern security tools use behavioral analysis and AI to identify zero-day threats.

#### **7. Vulnerability Testing**

Penetration testing and code analysis help identify weaknesses before attackers exploit them.

### **Challenges in Detecting Zero-Day Exploits**

Zero-day attacks are difficult to detect because:

- No known signature exists
- Attack techniques constantly evolve
- Exploits may use encrypted or hidden payloads
- Traditional antivirus systems rely on known patterns

Advanced AI-based cybersecurity systems are increasingly used to detect abnormal behavior and unknown threats.

### **Conclusion**

Zero-Day Buffer Overflow Exploitation is one of the most dangerous forms of cyberattack because it combines hidden software vulnerabilities with memory manipulation techniques. These attacks can cause severe damage to individuals, businesses, and critical infrastructure. Strong cybersecurity practices, secure software development, continuous monitoring, and advanced threat detection technologies are essential to reduce the risks associated with zero-day buffer overflow exploits.

college - Saved to this PC

Teams needs permission to access your camera  
Go to your privacy settings to allow it.

Record Share

## Buffer Overflow Attack — Complete Flow

Stack Layout: LOW MEMORY ← → HIGH MEMORY

1 NORMAL STACK

buffer[28] 28 bytes empty	saved EBP of main() 4 bytes	Return Addr "ret 0" 4 bytes	main() FRAME
---------------------------------	--------------------------------	-----------------------------------	-----------------

2 scanf WRITES →

A A A A A 28 bytes bytes 01-28	saved EBP DESTROYED bytes 29-32	0x00049182 secretFunc() RET REPLACED!	bytes 33-36 overwritten
--------------------------------------	---------------------------------------	---	----------------------------

3 OVERFLOW DONE

buffer FULL	EBP crossed	OVERWRITE! ESP → here	RET= 0x00049182 secretFunction()
-------------	-------------	--------------------------	-------------------------------------

Allocate buffer[28] FRP saved & reused scanf: on bounds check FRP overwritten (bytes 29-32) RET → 0x00049182 (secretFunction)

teams.live.com is sharing your screen. Stop sharing Hide

Participants:

- K.V. Pand...
- shrayan m...
- MK Michael V...
- AR Aala Ravik...
- DJ DR.RAJEN...
- Dr. Rajend...
- VB venkaiah ...
- AN Annam N...
- AN anwini net...
- DB Dr.Rajendra Prasad Banavathu

< 1/2 >

09:50

Teams needs permission to access your camera  
Go to your privacy settings to allow it.

## 0-Day Example: Buffer Overflow Exploit

1 VULNERABLE CODE (in the target application)

```

1 #include <stdio.h>
2 void secretFunction()
3 {
4     printf("server ssh password:\n");
5     printf("server password is : quert123\n");
6 }
7
8
9
10 void doit()
11 {
12     char buffer[20];
13     printf("Enter some text:\n");
14     scanf("%s", buffer);
15     printf("your data is : '%s' now belongs to us\n", buffer);
16 }
17
18 int main()
19 {
20     doit();
21     return 0;
22 }
23
24 payload:
25 Spython3 -c "print('
26

```

teams.live.com is sharing your screen. Stop sharing Hide

Participants:

- K.V. Pand...
- shrayan m...
- MK Michael V...
- AR Aala Ravik...
- DJ DR.RAJEN...
- Dr. Rajend...
- VB venkaiah ...
- AN Annam N...
- AN anwini net...
- DB Dr.Rajendra Prasad Banavathu

< 1/2 >

10:15

Teams needs permission to access your camera  
Go to your privacy settings to allow it.

## 2 Disassembly: Confirming the Overflow

ASSEMBLY

```

00000000401140 <frame_dummy>:
401140: f3 1e fa          jmp     401144 <register_to_clones>
401144: 4b 0a             jmp     401000 <register_to_clones>

0000000040114c <secretFunction>:
40114c: 55               push   %rbp
40114d: 48 89 e5         mov    %rsp,%rbp
40114e: 48 8d 05 b7 0e 00 00 lea   0xb7(rip),%rax # 402008 <_IO_stdin_used+0x8>
401151: 48 89 c7         mov    %rax,%rdi
401152: 48 07 fe ff ff   call  401030 <puts@plt>
401157: 48 8d 05 bc 0e 00 00 lea   0xbc(rip),%rax # 40201c <_IO_stdin_used+0x1c>
40115b: 48 89 c7         mov    %rax,%rdi
40115c: e8 c8 fe ff ff   call  401030 <puts@plt>
401160: 90               nop
401161: 5d               pop    %rbp
401162: c3               ret

0000000040116b <doit>:
40116b: 55               push   %rbp
40116c: 48 89 e5         mov    %rsp,%rbp
40116d: 48 83 ec 20      sub   $0x20,%rsp
401170: 48 8d 05 c8 0e 00 00 lea   0xc8(rip),%rax # 40203a <_IO_stdin_used+0x3a>
401174: 48 89 c7         mov    %rax,%rdi
401175: 48 00 00 00     mov    $0x0,%eax
401178: 48 09 ff ff     call  401040 <printf@plt>
40117d: 48 8d 05 e0      lea   0xe0(rip),%rax
401180: 48 89 c7         mov    %rax,%rdi
401181: 48 8d 05 b5 0e 00 00 lea   0xb5(rip),%rax # 40204a <_IO_stdin_used+0x4a>
401185: 48 89 c7         mov    %rax,%rdi
401186: b8 00 00 00     mov    $0x0,%eax
401189: 48 ae fe ff ff   call  401050 <_isoc99_scanf@plt>
40118d: 48 8d 05 e8      lea   0xe8(rip),%rax
401190: 48 89 c7         mov    %rax,%rdi
401191: 48 89 c7         mov    %rax,%rdi
401192: 48 89 c7         mov    %rax,%rdi
401193: 48 83 fe ff     jmp   402050 <_IO_stdin_used+0x50>
401196: 90               nop
401197: 90               nop
401198: 90               nop

```

teams.live.com is sharing your screen. Stop sharing Hide

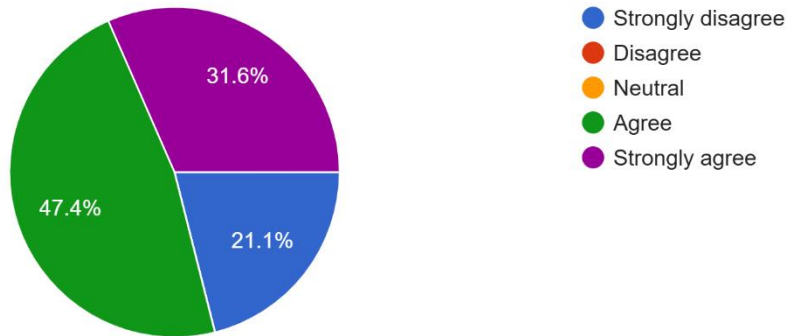
Participants:

- K.V. Pand...
- shrayan m...
- MK Michael V...
- AR Aala Ravik...
- DJ DR.RAJEN...
- Dr. Rajend...
- VB venkaiah ...
- AN Annam N...
- AN anwini net...
- DB Dr.Rajendra Prasad Banavathu

< 1/2 >

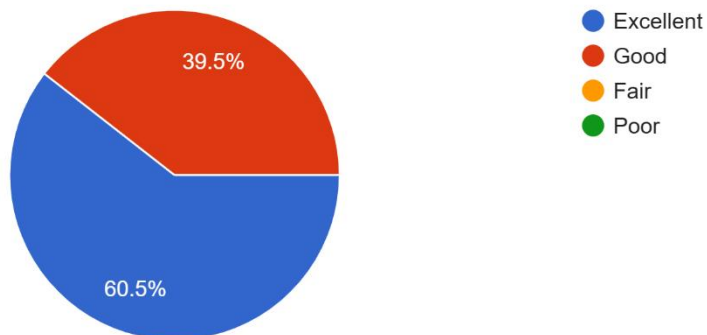
The topics covered in the FDP were well-structured and organized.

38 responses



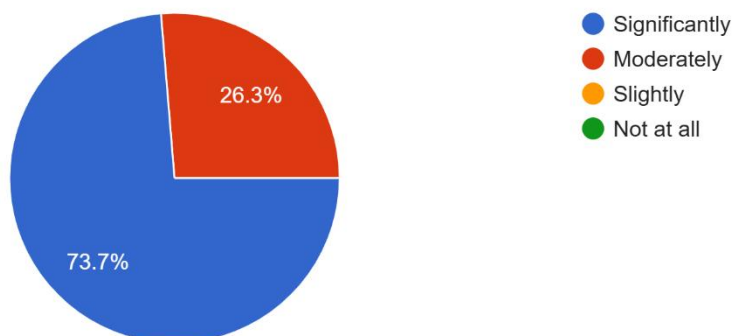
How effective were the resource persons in delivering the sessions?

38 responses



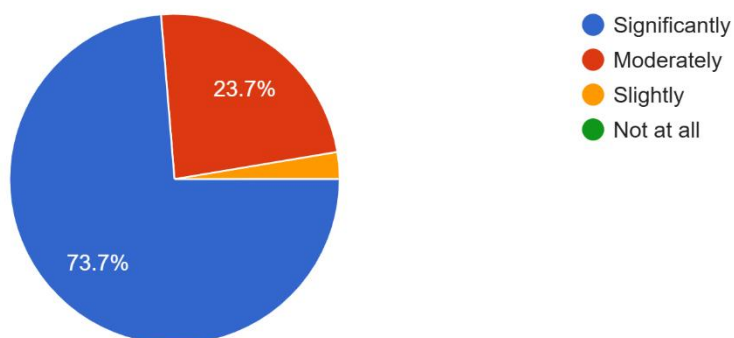
Learning Outcomes

38 responses



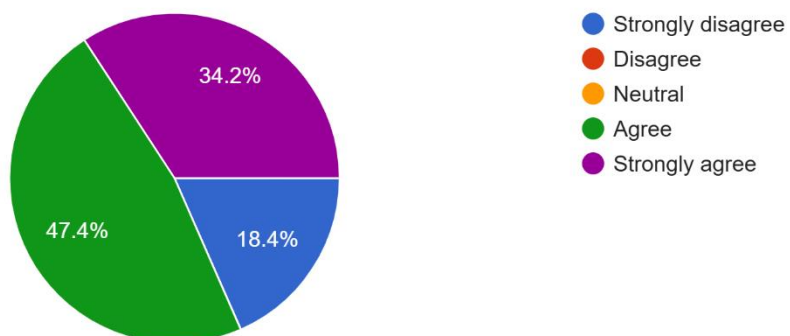
The FDP enhanced my knowledge/skills in the subject area.

38 responses



Overall, I am satisfied with this FDP.

38 responses



# LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING (A)

Accredited by NAAC 'A'  
ISO 9001:2015 Certified Institution  
Approved by AICTE, New Delhi and Affiliated to JNTUK, Kakinada  
L.B. REDDY NAGAR, MYLAVARAM, NTR DIST., A.P.-521 230.



## CERTIFICATE OF PARTICIPATION

This certificate is present to:

**Mrs. Sandireddy Ramadevi**  
**Associate Professor**

**Dr RVR NRI INSTITUTE OF TECHNOLOGY**  
**(DEEMED TO BE UNIVERSITY)**

has successfully participated in the Online Faculty  
Development Programme on “**AI-Driven  
Cybersecurity for Secure Financial Transaction**”  
organized by the Department of CSE(AI&ML), IT,  
MBA from 27/04/2026 to 02/05/2026.

CONVENOR

PRINCIPAL



# LAKIREDDY BALI REDDY COLLEGE OF ENGINEERING (A)

Accredited by NAAC 'A'  
ISO 9001:2015 Certified Institution  
Approved by AICTE, New Delhi and Affiliated to JNTUK, Kakinada  
L.B. REDDY NAGAR, MYLAVARAM, NTR DIST., A.P.-521 230.



## CERTIFICATE OF PARTICIPATION

This certificate is present to:

**Mrs. KAVALI RAJESWARI**

**Assistant Professor**

**ANDHRA LOYOLA INSTITUTE OF ENGINEERING AND TECHNOLOGY**

has successfully participated in the Online Faculty  
Development Programme on “**AI-Driven  
Cybersecurity for Secure Financial Transaction**”  
organized by the Department of CSE(AI&ML), IT,  
MBA from 27/04/2026 to 02/05/2026.

CONVENOR

PRINCIPAL



Participants gained knowledge of cloud-based AI services, generative AI workflows, MLOps, security best practices, and version control using Git & GitHub.

**Co-Ordinator**

**HoD**