LAKIREDDY BALIREDDY COLLEGE OF ENGINEERING
(AUTONOMOUS)
L B Reddy Nagar, Mylavarm, Krishna District, Andhra Prade1sh-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.

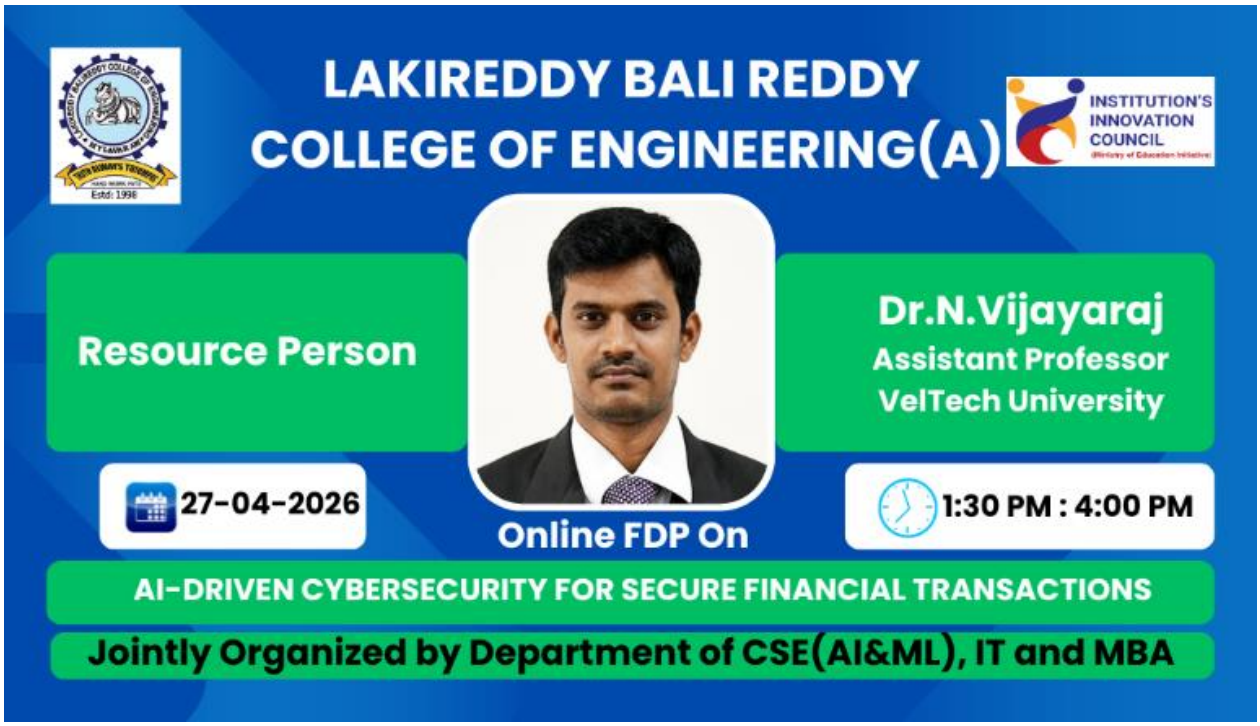
Outcomes of the FDP

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



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.

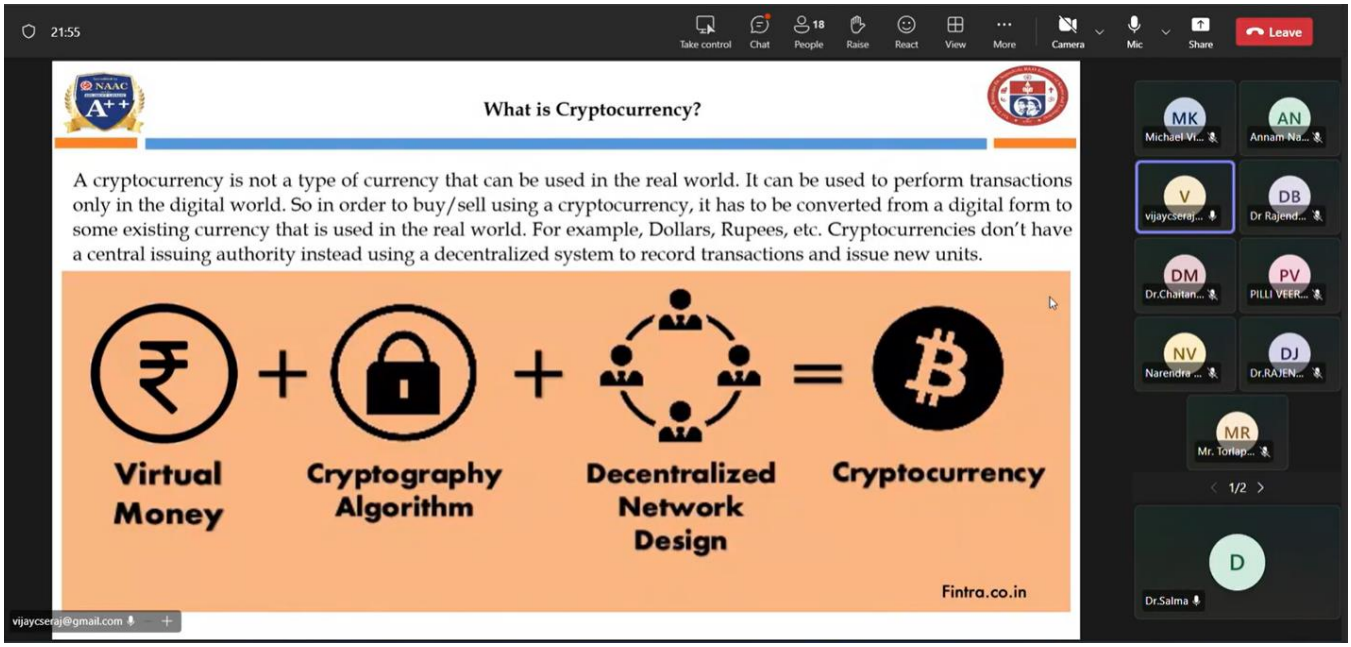
Another challenge is the increasing use of **cloud computing** in financial services. While cloud platforms improve scalability and efficiency, they also introduce concerns related to data privacy, access control, and third-party security. Financial institutions must ensure that cloud service providers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

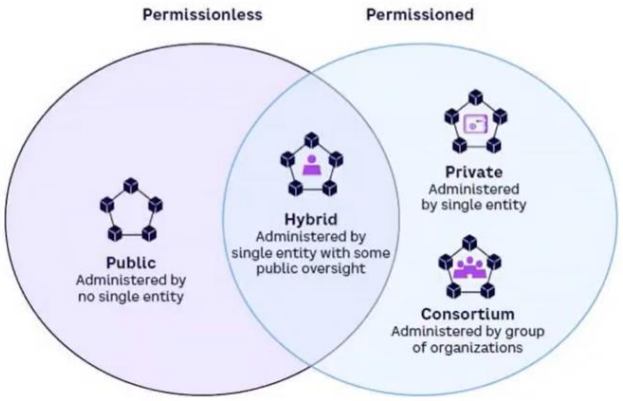
To address these cybersecurity challenges, financial institutions must adopt a comprehensive cybersecurity strategy. This includes implementing advanced technologies such as artificial intelligence for threat detection, conducting regular security audits, updating software systems, and ensuring compliance 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.



44:47

Types of Blockchain

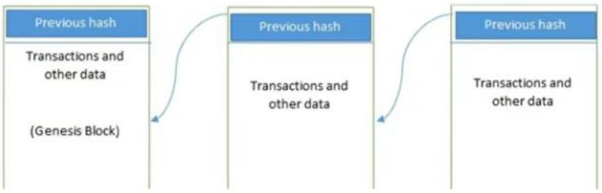


vijaycseraj@gmail.com

34:36

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).



vijaycseraj@gmail.com

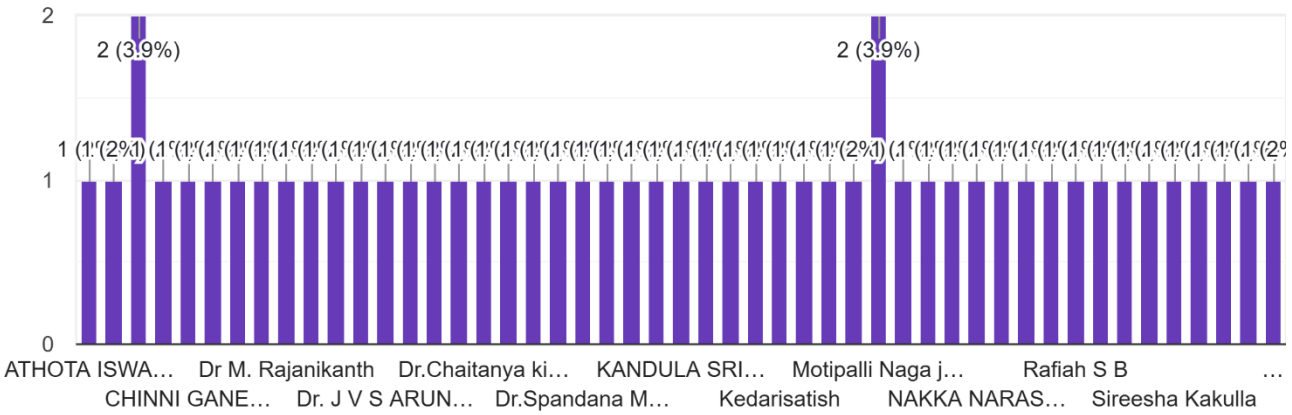
03:27

vijaycseraj@gmail.com 1/27/2026 13

Feedback

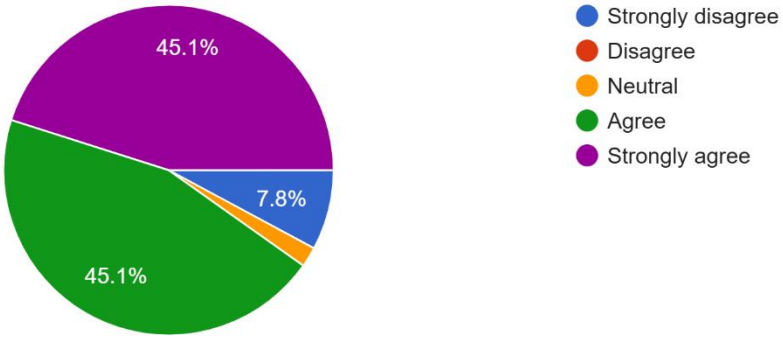
Name of the Faculty

51 responses



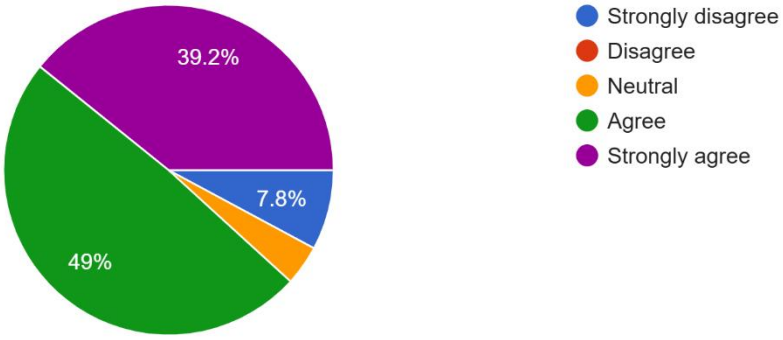
The course contents met with your expectations

51 responses



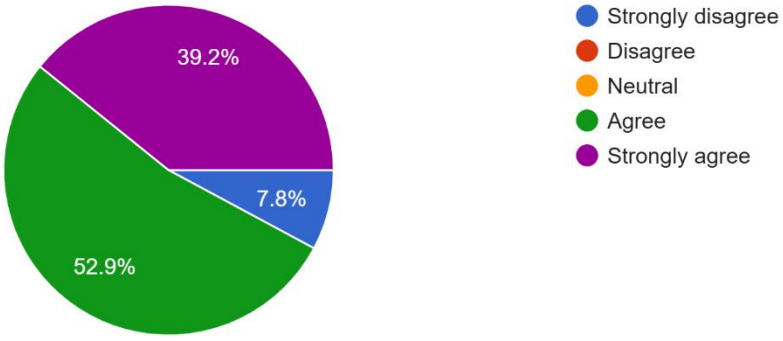
The lecture sequence was well planned

51 responses



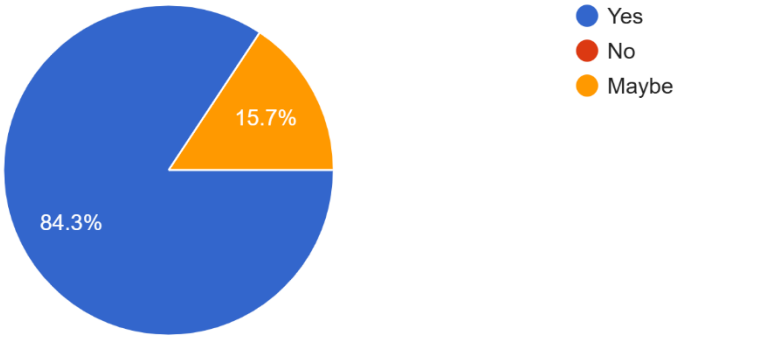
The course exposed you to new knowledge and practices

51 responses



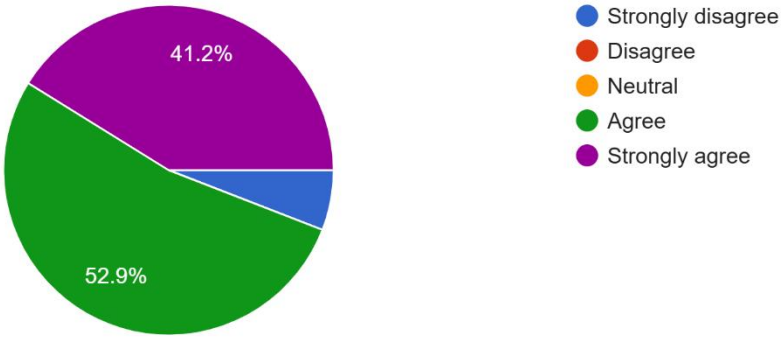
Will you recommend this course to your colleagues?

51 responses

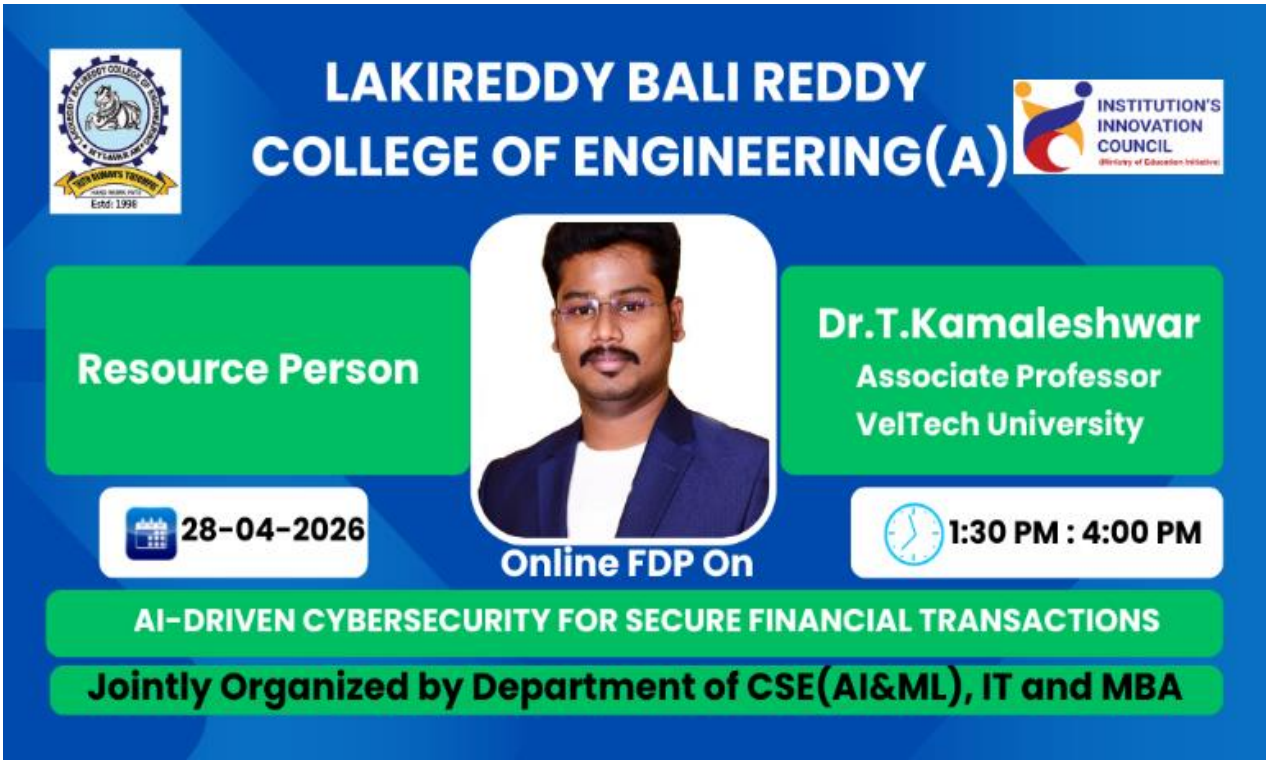


The lectures were clear and easy to understand

51 responses



DAY2: 28-04-2026



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

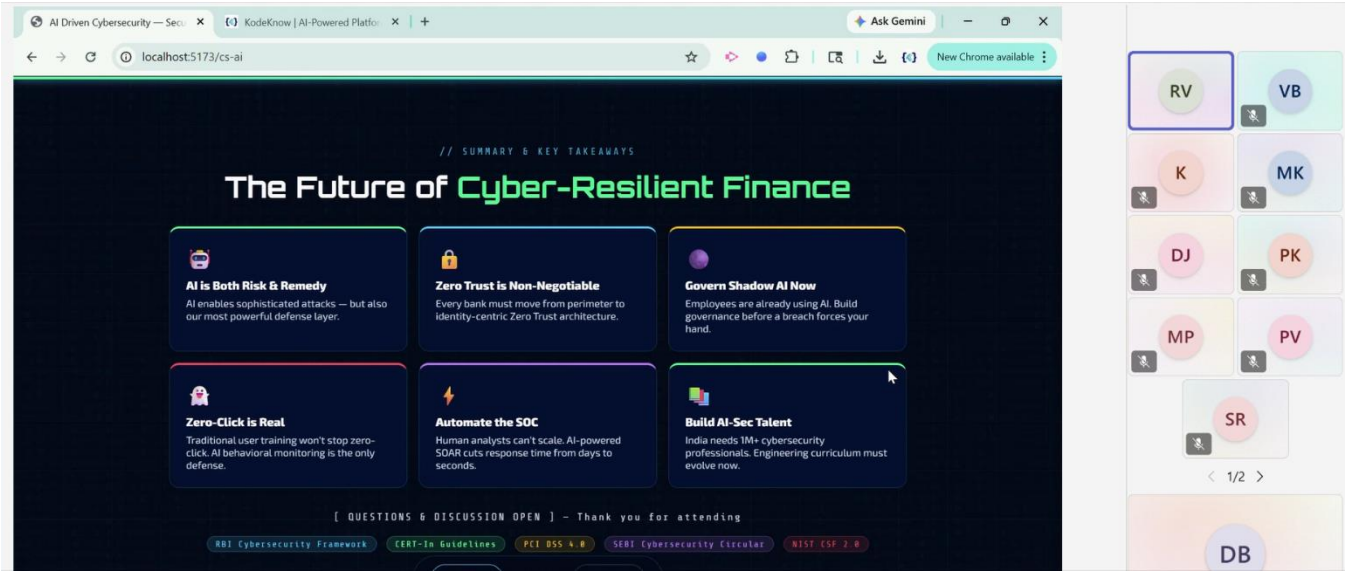
complexity and create delays in access or communication. Poor implementation may reduce productivity and encourage users to bypass security controls.

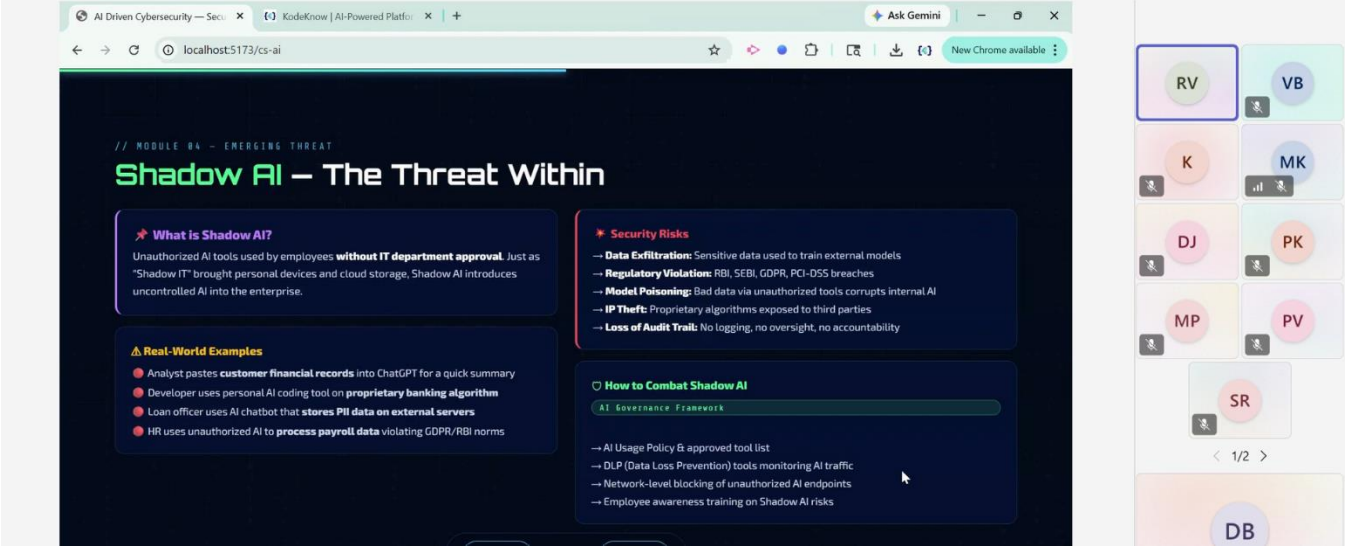
Additionally, **advanced persistent threats (APTs)** may still evade Zero Trust systems. Skilled attackers can move slowly within a network, using stolen credentials and legitimate tools to avoid detection. Without strong behavioral analytics and real-time monitoring, such attacks may remain unnoticed.

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

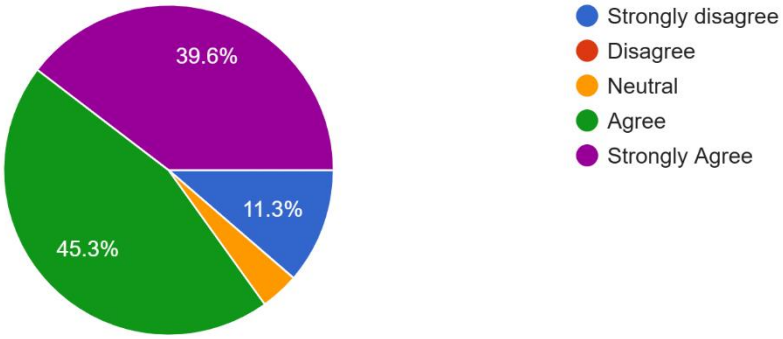
In conclusion, Zero Trust is an effective cybersecurity framework that enhances protection in modern digital environments. However, it is not completely immune to vulnerabilities. Proper implementation, continuous monitoring, and strong security practices are necessary to ensure the effectiveness of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





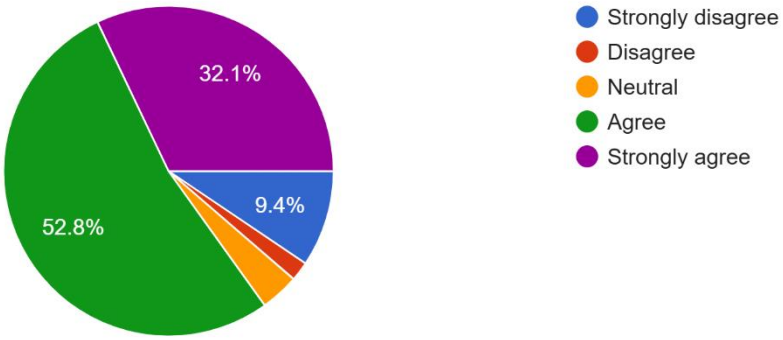
The content were relevant to the sessions within the program

53 responses



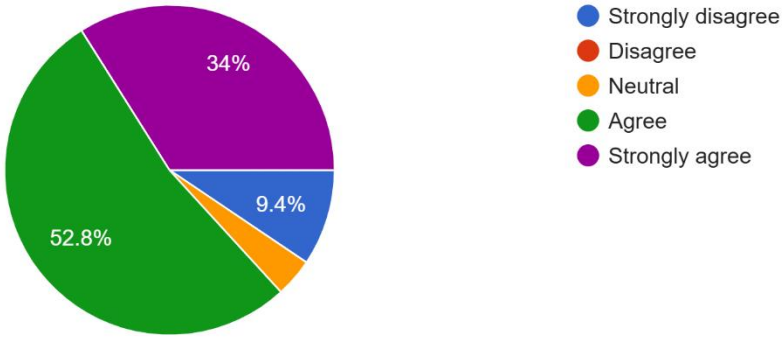
The presentations were effective

53 responses



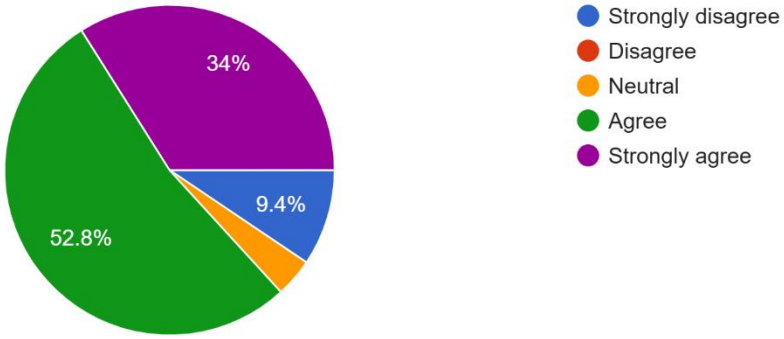
The program enhanced your teaching, research, or administrative skills/knowledge

53 responses



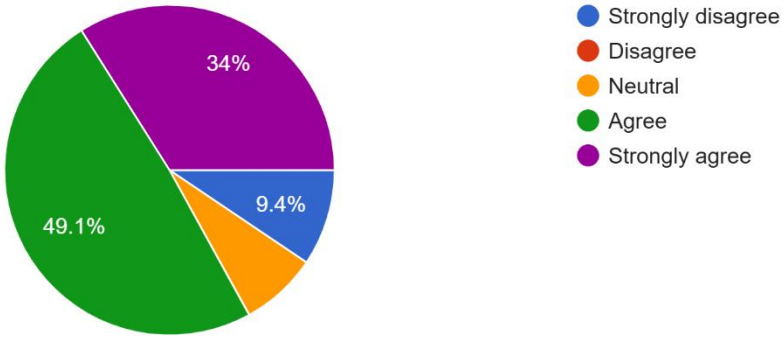
The program enhanced your teaching, research, or administrative skills/knowledge

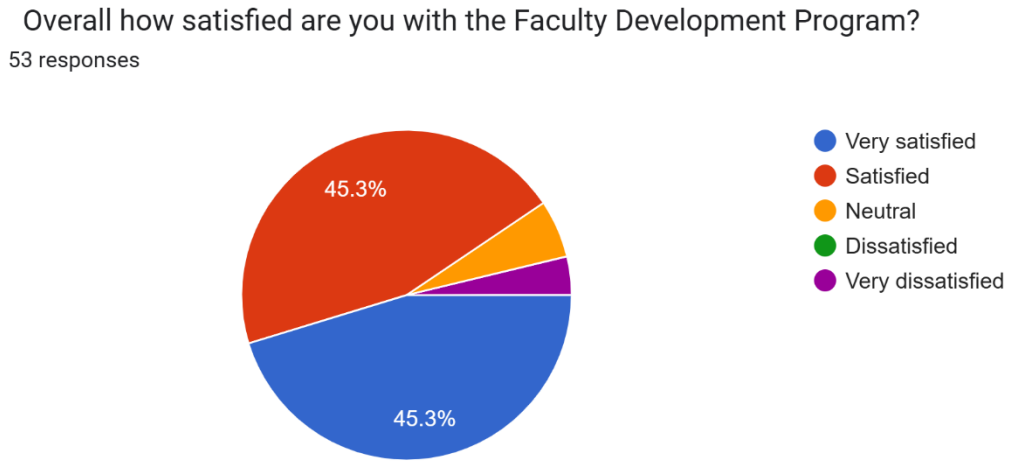
53 responses



The program enhanced your teaching methodologies and pedagogical approaches

53 responses





DAY3: 29-04-2026

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.

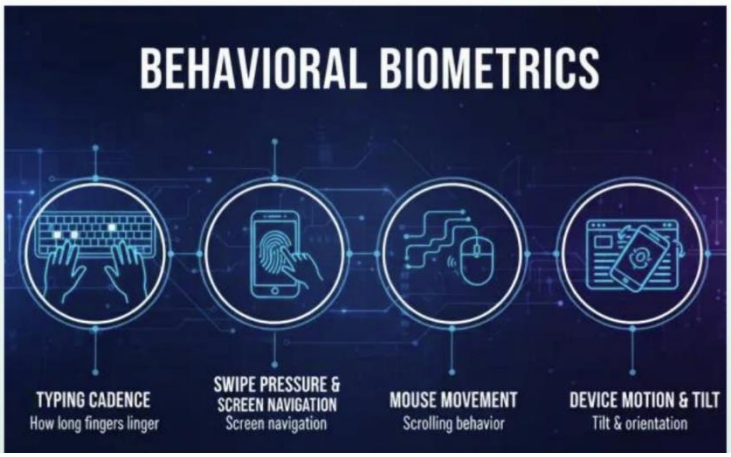
Despite its advantages, AI in financial security also faces certain challenges. Cybercriminals can use AI to create more advanced attacks, such as AI-generated phishing messages or deepfake fraud. AI systems may also produce false positives or biased decisions if trained on poor-quality data. Furthermore, 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



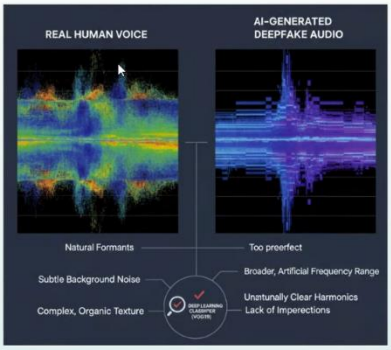
KodeKnow™

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)



KodeKnow™

RV VB K MK DJ PK MP PV SR DB

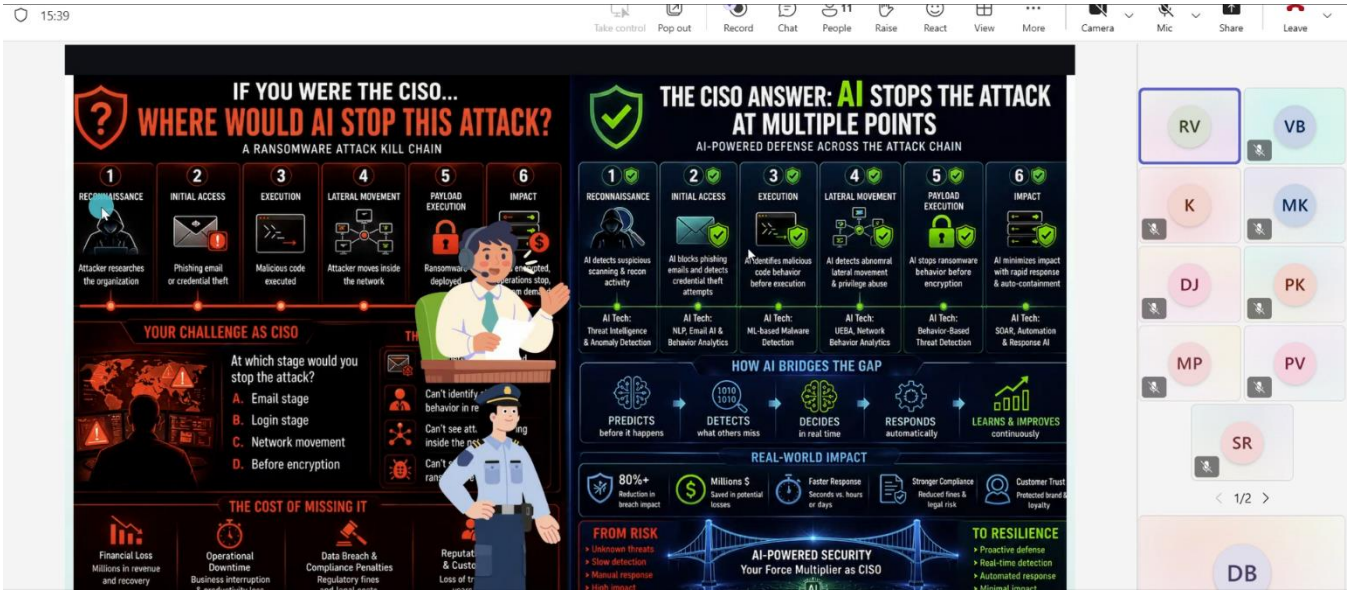
1. Voice Deepfake (Audio Cloning)

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

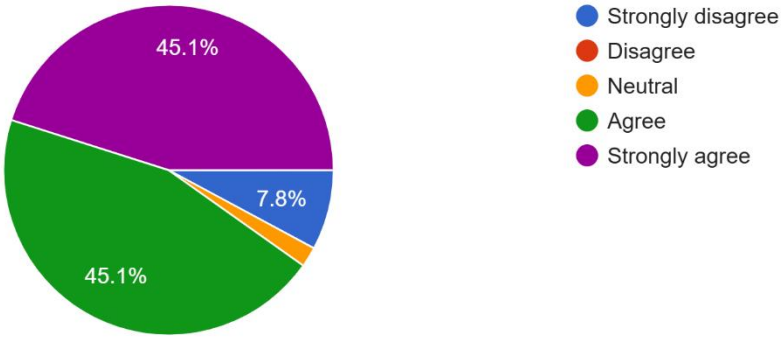
KodeKnow™

RV VB K MK DJ PK MP PV SR DB



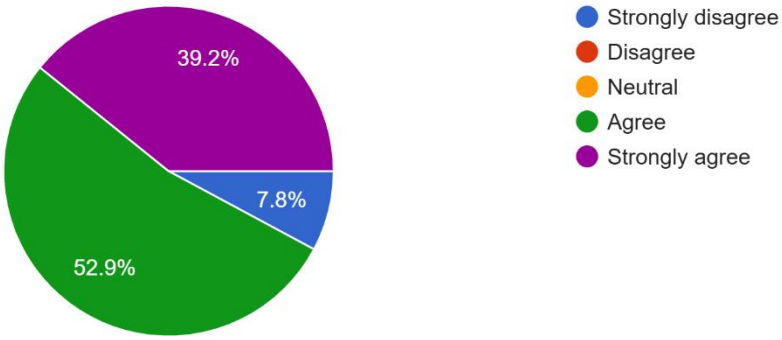
The course contents met with your expectations

51 responses



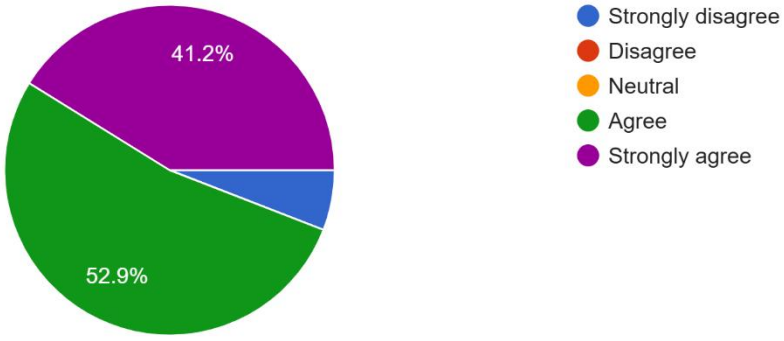
The course exposed you to new knowledge and practices

51 responses



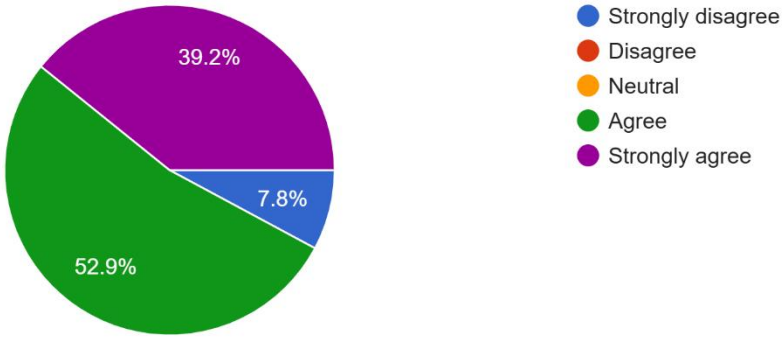
The lectures were clear and easy to understand

51 responses



The course exposed you to new knowledge and practices

51 responses



DAY4: 30-04-2026

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

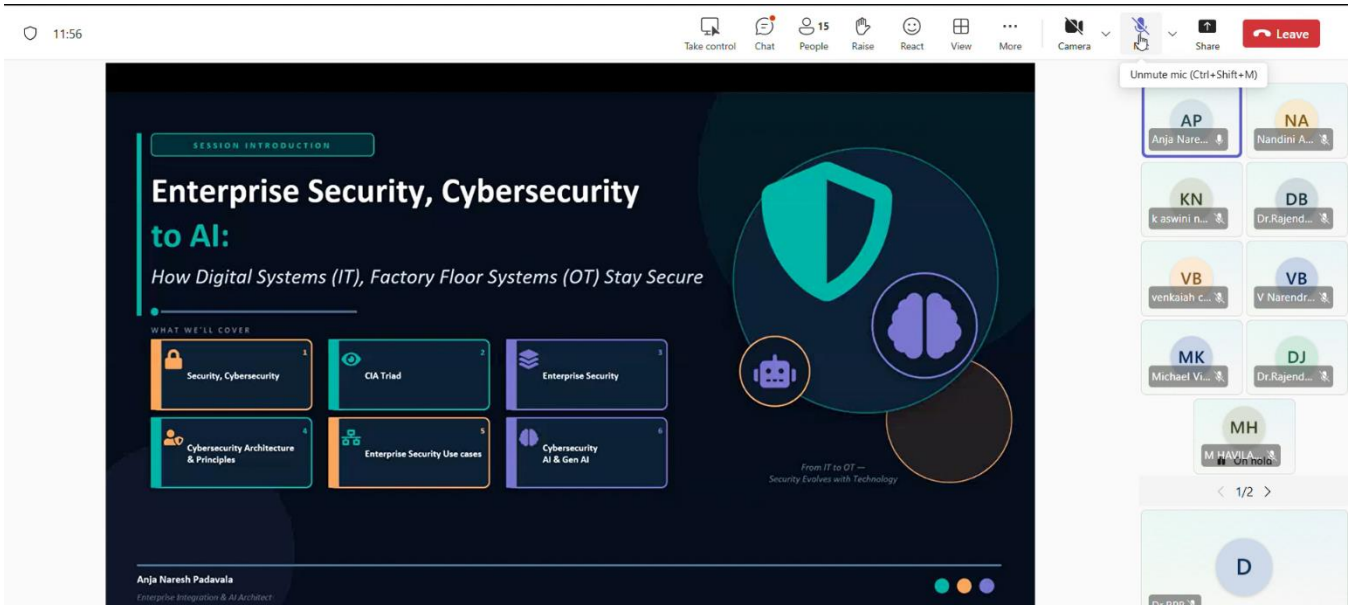
Organizations must combine AI technologies with human expertise and strong cybersecurity policies to ensure effective protection.

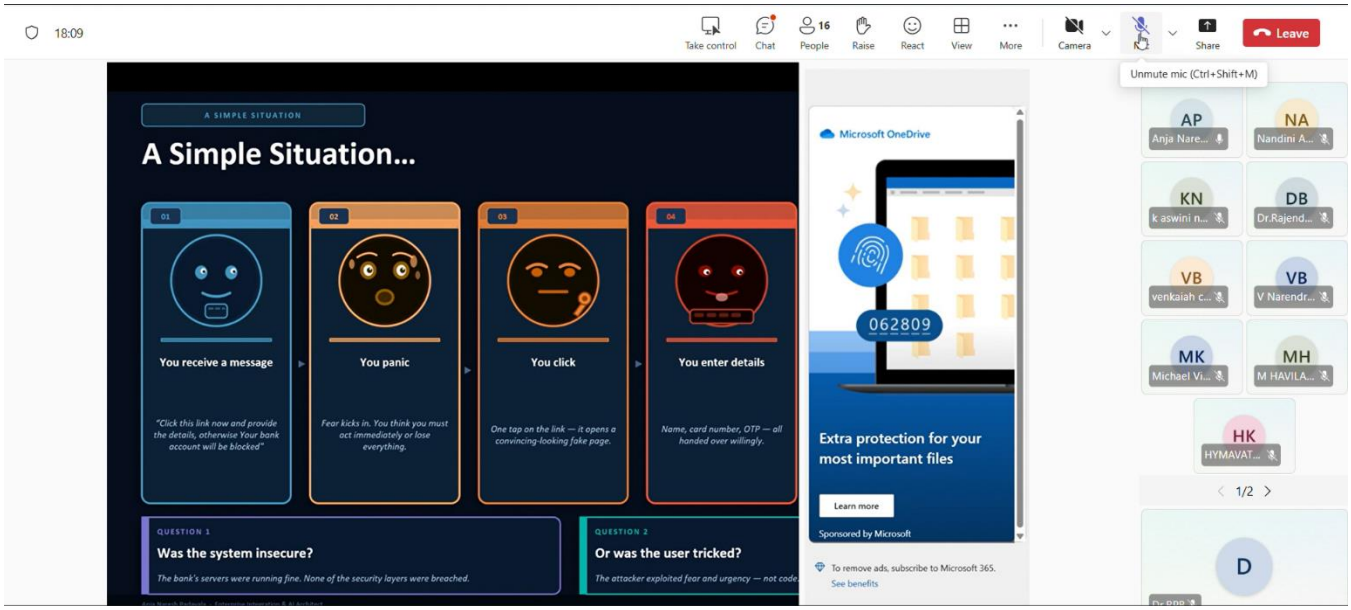
Future of Enterprise Security with AI

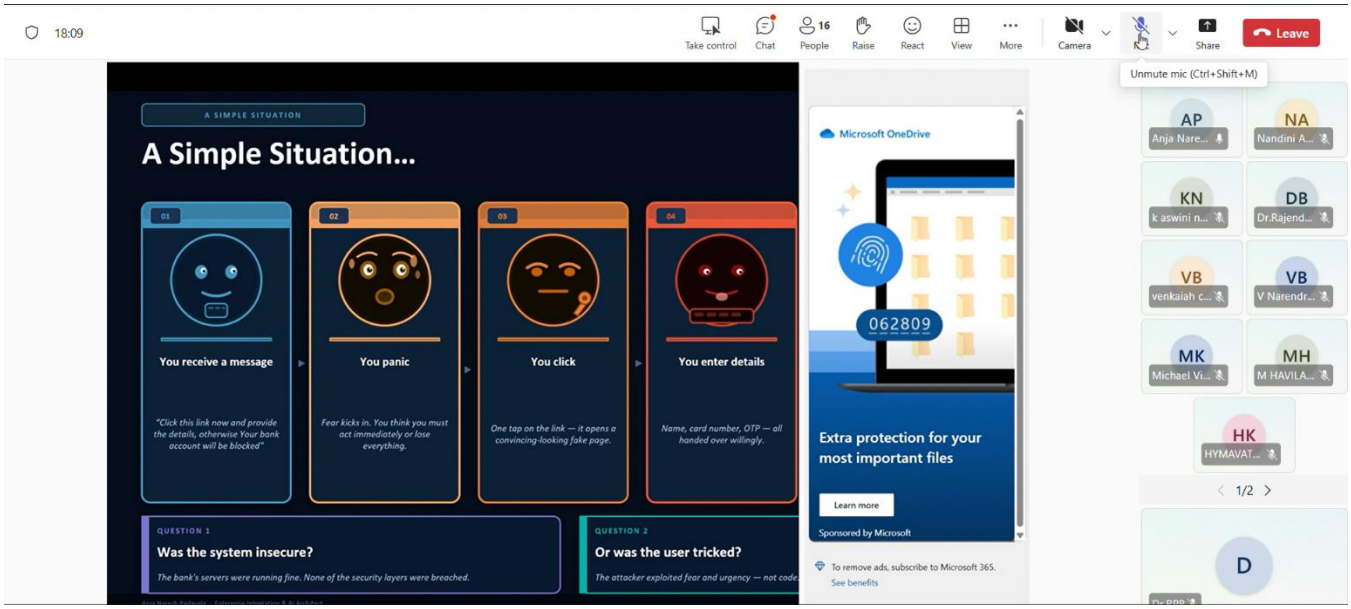
The future of enterprise security will increasingly depend on AI-driven technologies. Advanced AI systems will provide faster threat detection, automated defense mechanisms, and improved risk management. Technologies such as Zero Trust Architecture, cloud security, and AI-powered analytics will become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

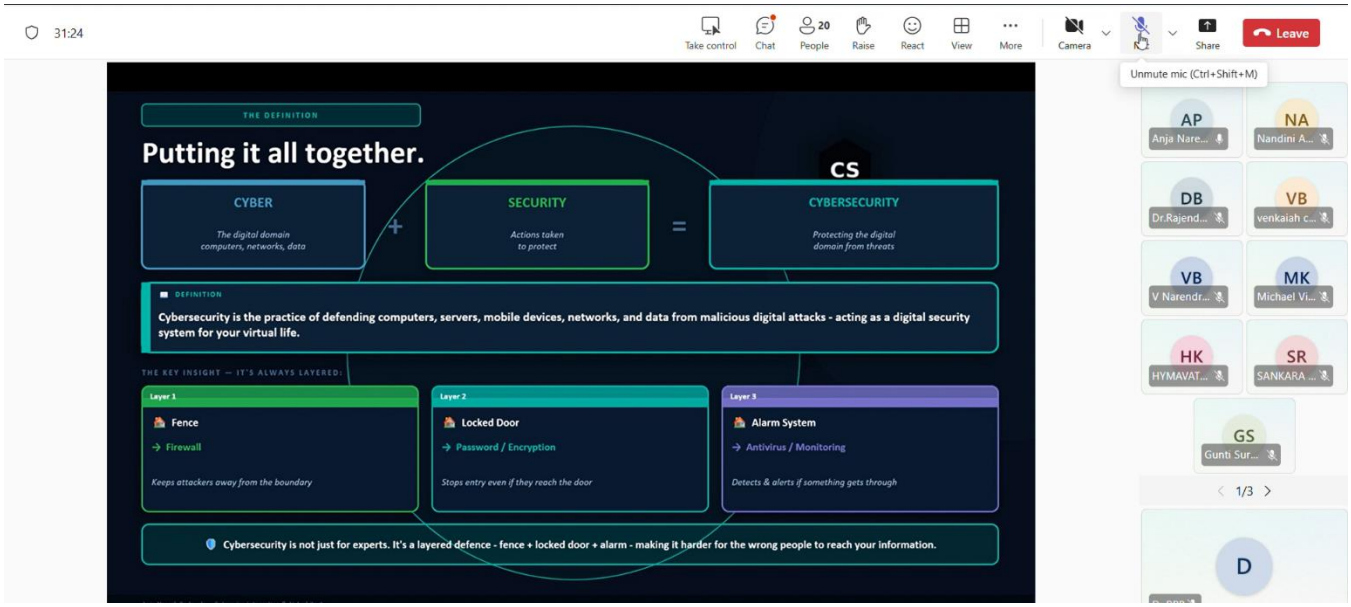
Conclusion

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.



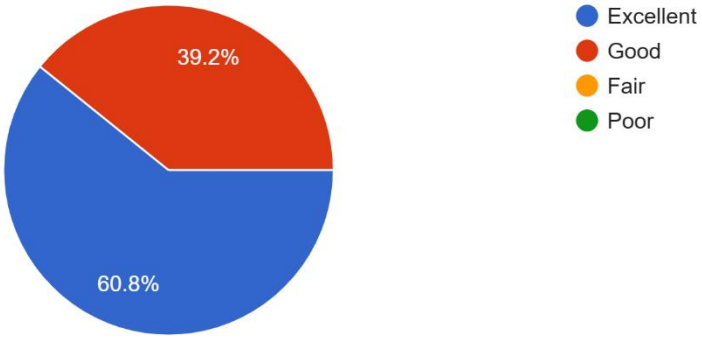






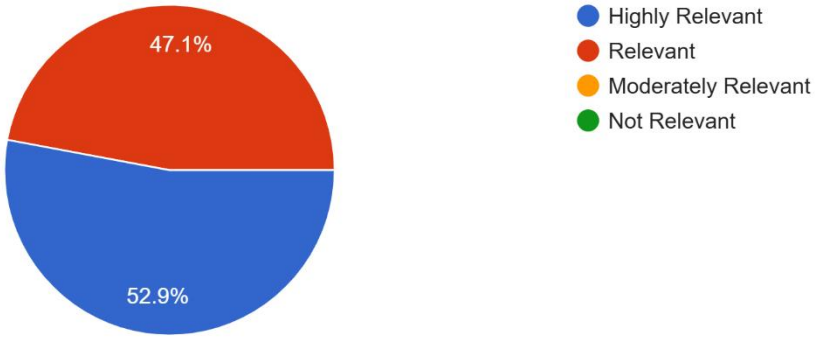
How would you rate the overall quality of the Session

51 responses



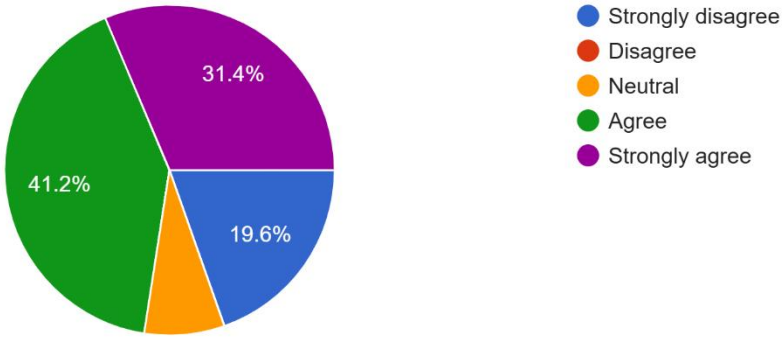
How relevant was the FDP content to your academic/research/industry needs?

51 responses



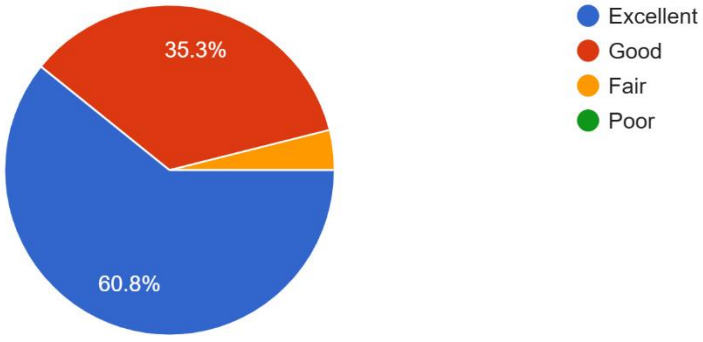
The topics covered (AI in Cybersecurity, Fraud Detection, Secure Transactions, etc.) were

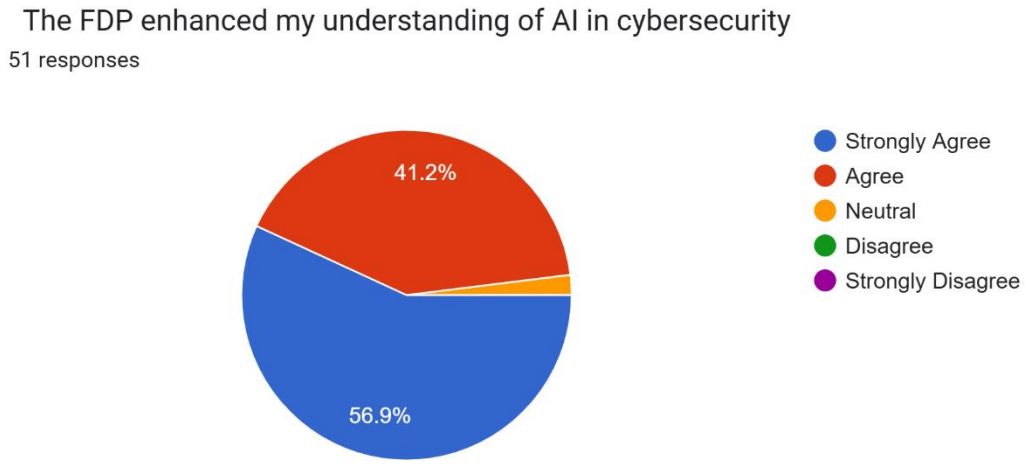
51 responses



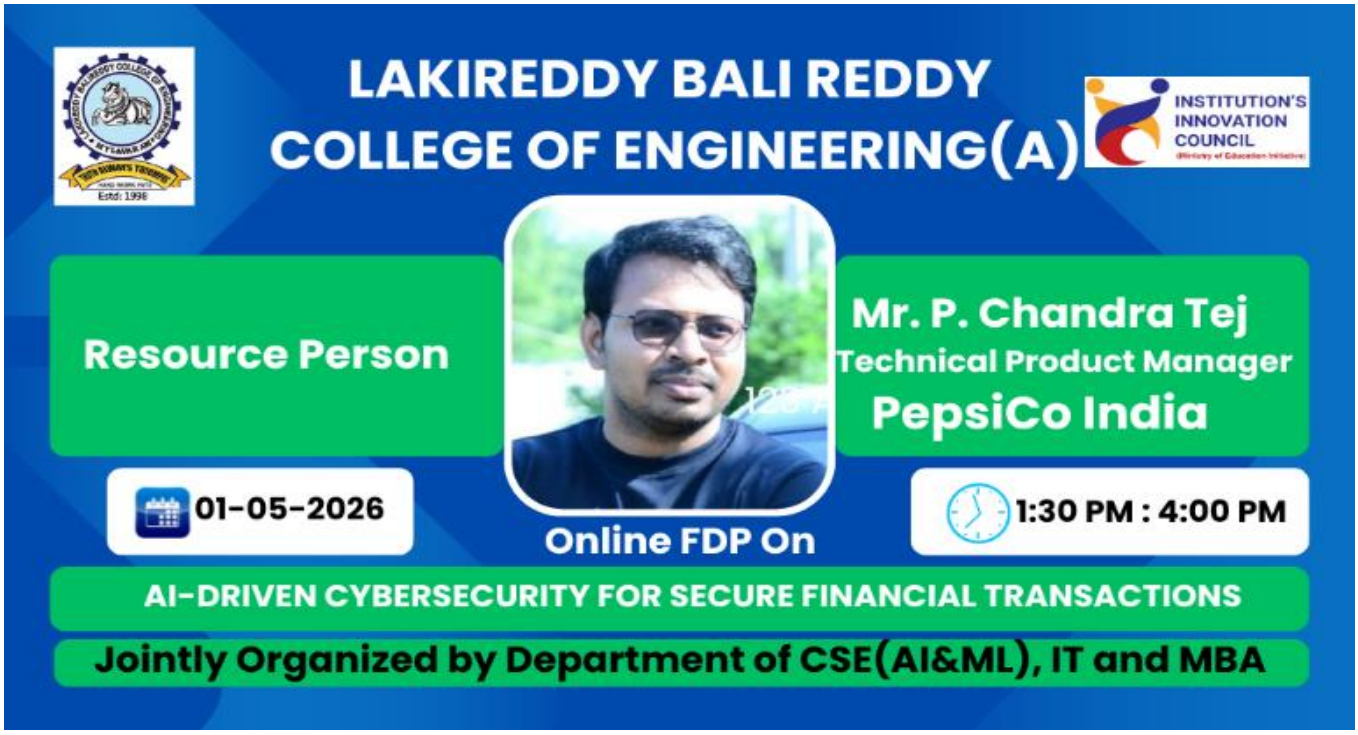
How do you rate the knowledge and expertise of the speakers?

51 responses





DAY5: 01-05-2026



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

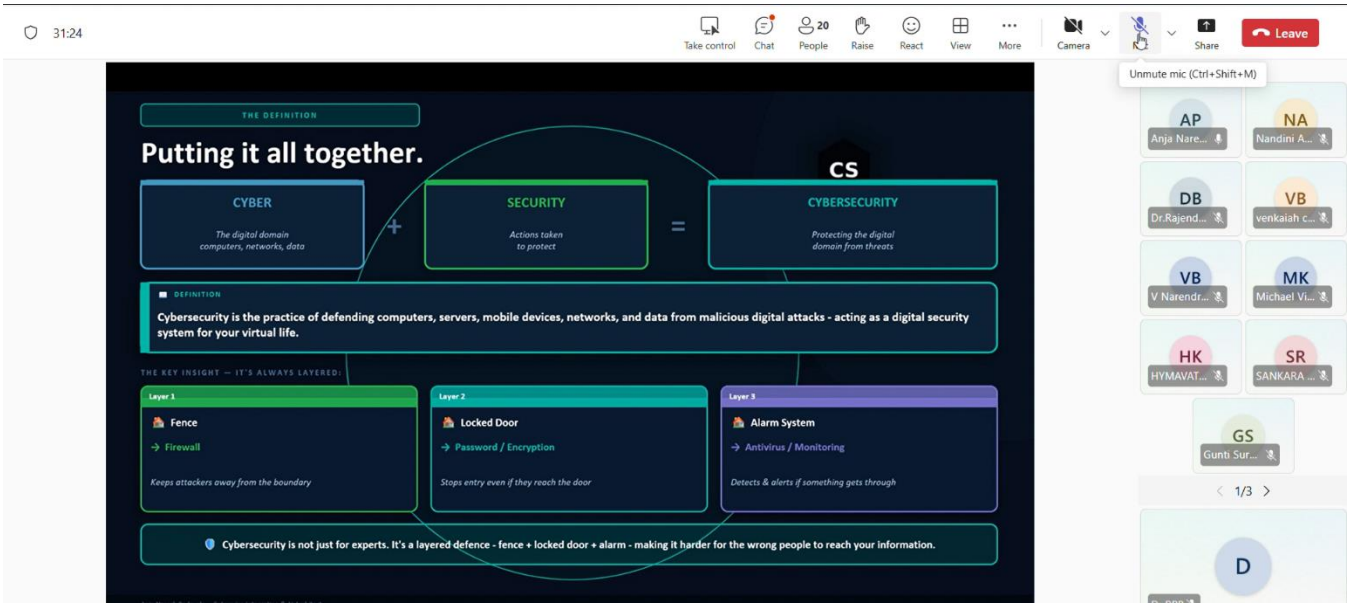
Cybercriminals may also use AI-generated text and advanced language techniques to bypass NLP-based security systems.

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.

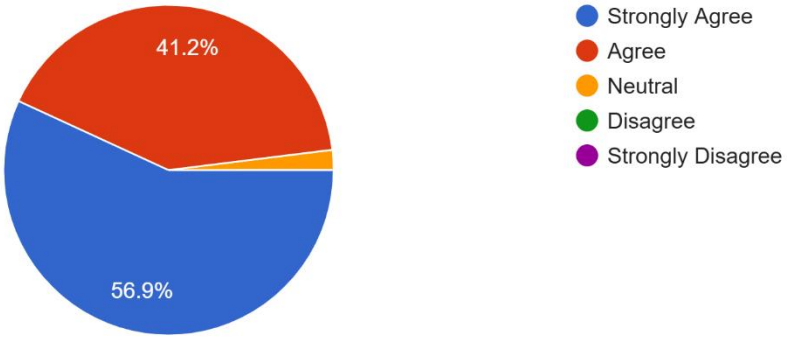
Conclusion

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.



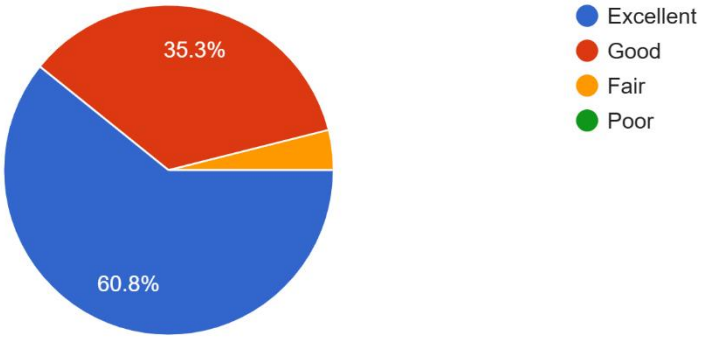
The FDP enhanced my understanding of AI in cybersecurity

51 responses



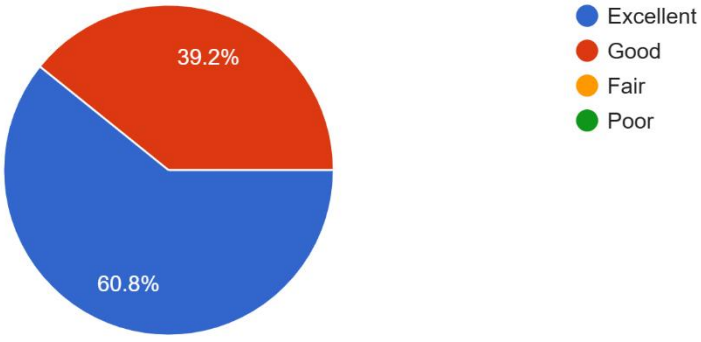
How do you rate the knowledge and expertise of the speakers?

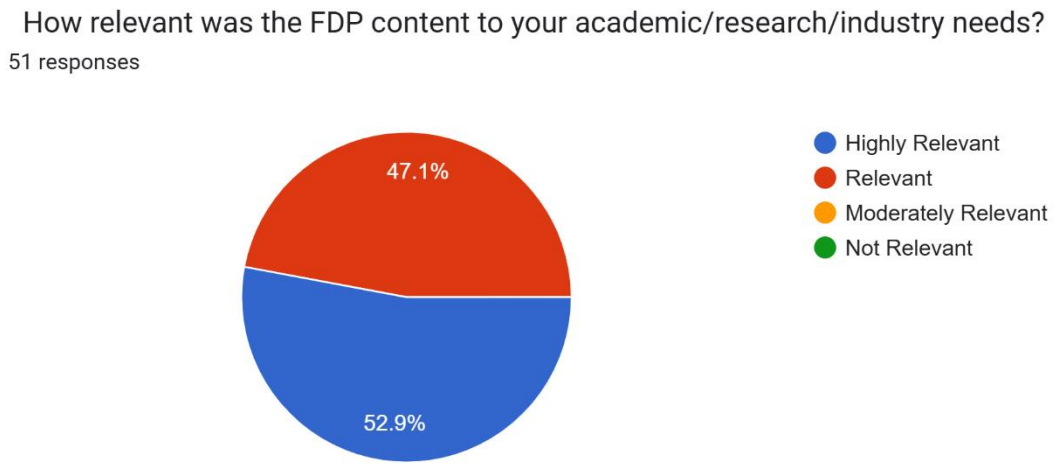
51 responses



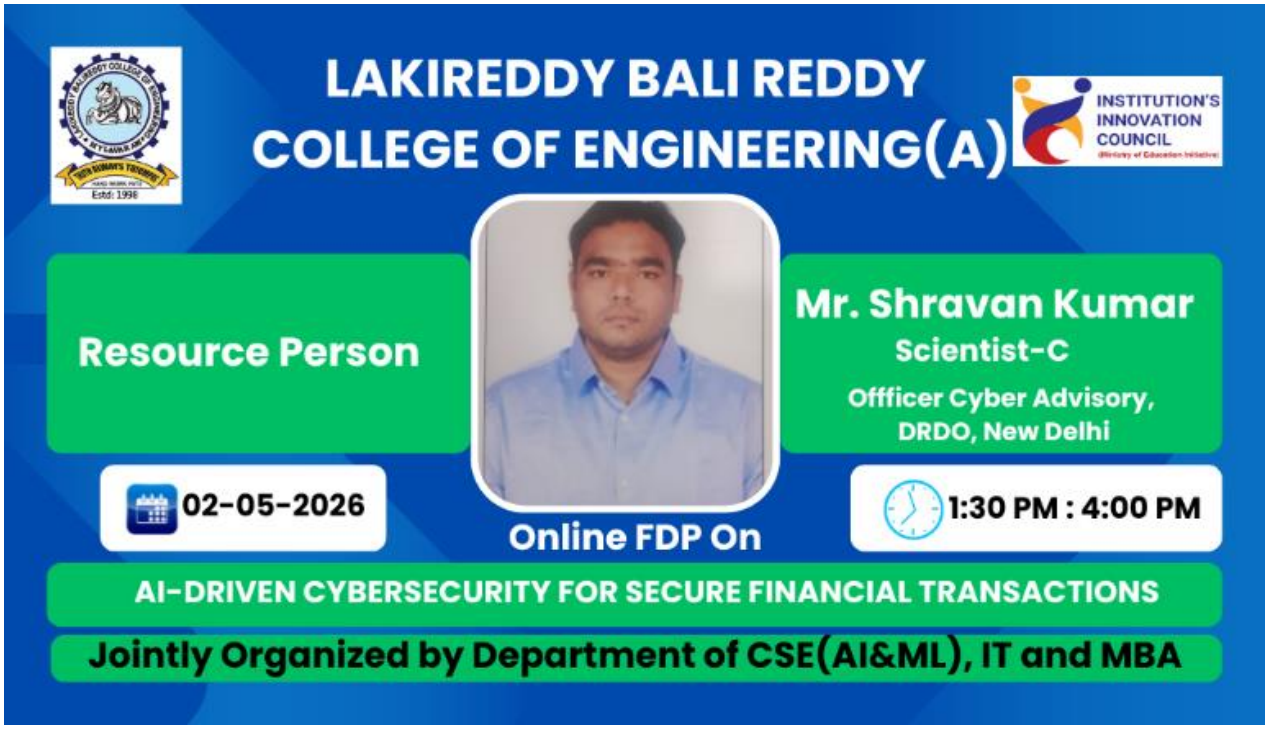
How would you rate the overall quality of the Session

51 responses





DAY6: 02-05-2026



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

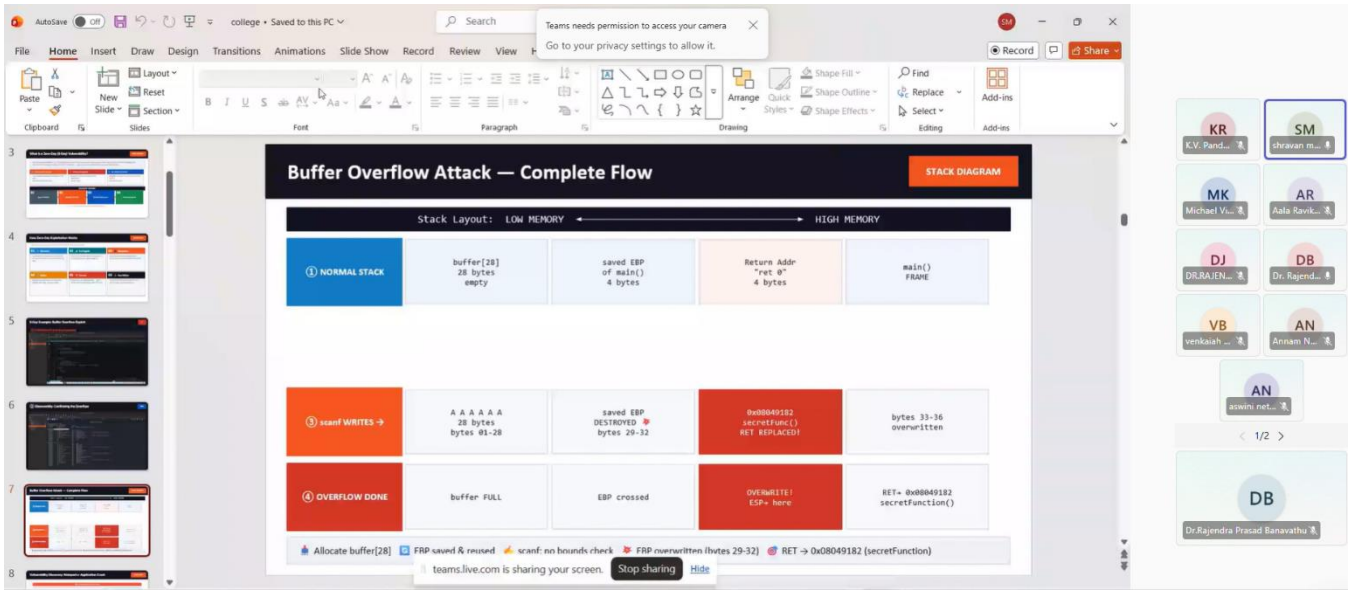
Zero-day attacks are difficult to detect because:

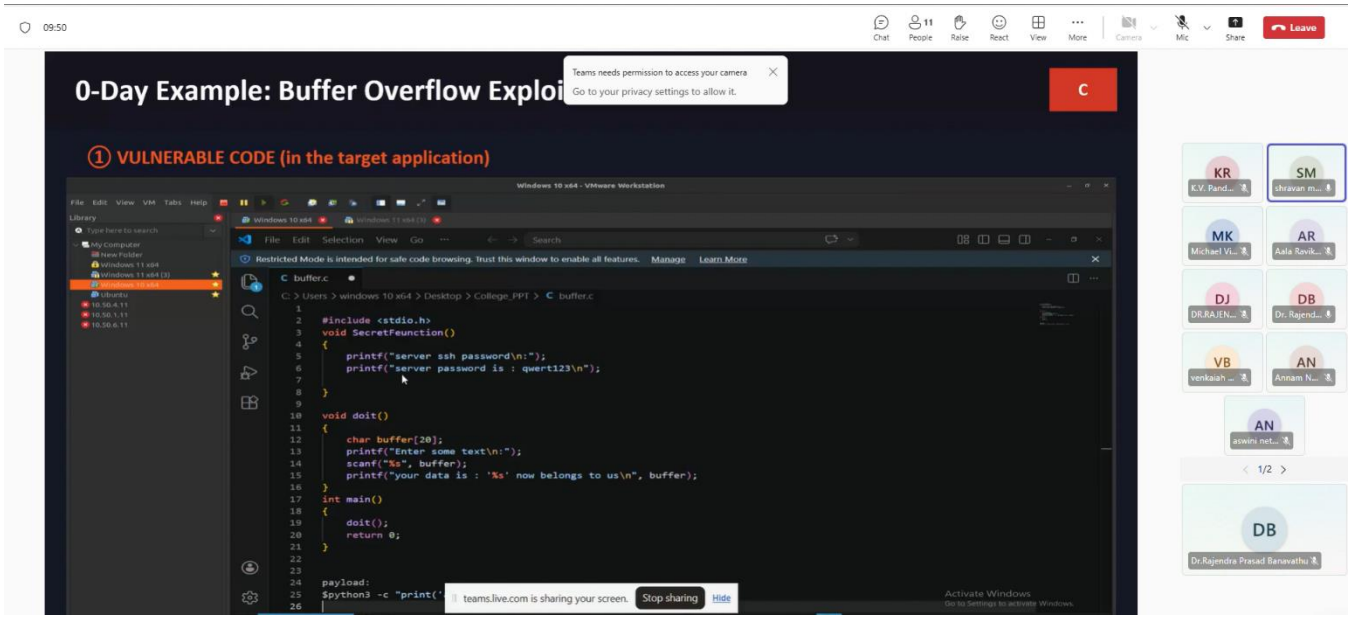
- No known signature exists
- Attack techniques constantly evolve
- Exploits may use encrypted or hidden payloads
- Traditional antivirus systems rely on known patterns

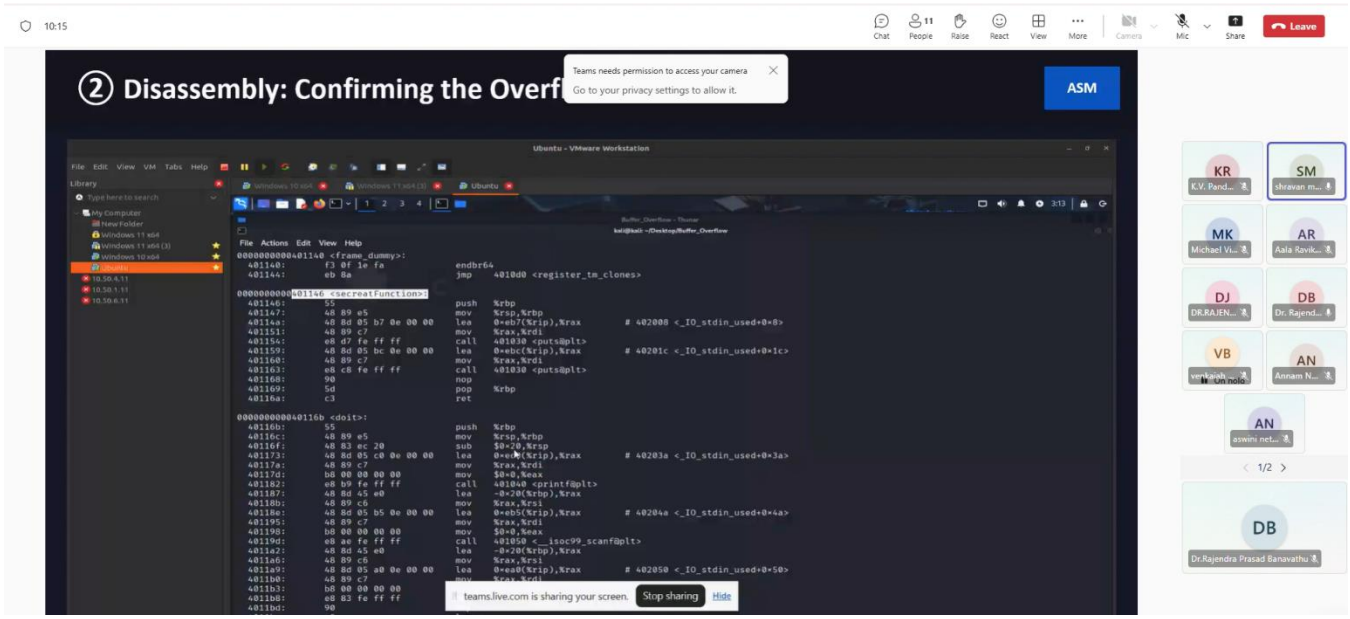
Advanced AI-based cybersecurity systems are increasingly used to detect abnormal behavior and unknown threats.

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.

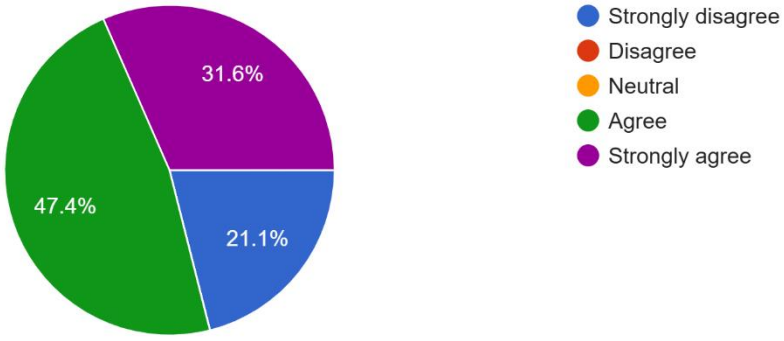

Buffer Overflow Attack — Complete Flow
STACK DIAGRAM
Stack Layout: LOW MEMORY → HIGH MEMORY
① NORMAL STACK
buffer[28] 28 bytes empty
saved EBP of main() 4 bytes
Return Addr "ret 0" 4 bytes
main() FRAME
③ scanf WRITES →
A A A A A A 28 bytes bytes 01-28
saved EBP DESTROYED bytes 29-32
0x08049182 secretFunc() RET REPLACED!
bytes 33-36 overwritten
④ OVERFLOW DONE
buffer FULL
EBP crossed
OVERWRITE! ESP+ here
RET+ 0x08049182 secretFunction()
Allocate buffer[28]
FRP saved & reused
scanf: no bounds check
FRP overwritten (bytes 29-32)
RET → 0x08049182 (secretFunction)
teams.live.com is sharing your screen.
Stop sharing
Hide


09:50
Chat
People
Raise
React
View
More
Camera
Mic
Share
Leave
0-Day Example: Buffer Overflow Exploi
Teams needs permission to access your camera
Go to your privacy settings to allow it.
C
① VULNERABLE CODE (in the target application)
Windows 10 x64 - VMware Workstation
buffer.c
#include <stdio.h>
void SecretFeunction()
{
printf("server ssh password\n:");
printf("server password is : qwert123\n");
}
void doit()
{
char buffer[20];
printf("Enter some text\n:");
scanf("%s", buffer);
printf("your data is : '%s' now belongs to us\n", buffer);
}
int main()
{
doit();
return 0;
}
payload:
$python3 -c "print('
teams.live.com is sharing your screen.
Stop sharing
Hide
Activate Windows


10:15
Chat
People
Raise
React
View
More
Camera
Mic
Share
Leave
② Disassembly: Confirming the Overf
Teams needs permission to access your camera
Go to your privacy settings to allow it.
ASM
Ubuntu - VMware Workstation
0000000000401140 <frame_dummy>:
401140: f3 0f 1e fa endbr64
401144: eb 8a jmp 4010d0 <register_tm_clones>
0000000000401146 <secreatFunction>:
401146: 55 push %rbp
401147: 48 89 e5 mov %rsp,%rbp
40114a: 48 8d 05 b7 0e 00 00 lea 0xeb7(%rip),%rax # 402008 <_IO_stdin_used+0x8>
401151: 48 89 c7 mov %rax,%rdi
401154: e8 d7 fe ff ff call 401030 <puts@plt>
401159: 48 8d 05 bc 0e 00 00 lea 0xebc(%rip),%rax # 40201c <_IO_stdin_used+0x1c>
401160: 48 89 c7 mov %rax,%rdi
401163: e8 c8 fe ff ff call 401030 <puts@plt>
401168: 90 nop
401169: 5d pop %rbp
40116a: c3 ret
000000000040116b <doit>:
40116b: 55 push %rbp
40116c: 48 89 e5 mov %rsp,%rbp
40116f: 48 83 ec 20 sub $0x20,%rsp
401173: 48 8d 05 c0 0e 00 00 lea 0xec0(%rip),%rax # 40203a <_IO_stdin_used+0x3a>
40117a: 48 89 c7 mov %rax,%rdi
40117d: b8 00 00 00 00 mov $0x0,%eax
401182: e8 b9 fe ff ff call 401040 <printf@plt>
401187: 48 8d 45 e0 lea -0x20(%rbp),%rax
40118b: 48 89 c6 mov %rax,%rsi
40118e: 48 8d 05 b5 0e 00 00 lea 0xeb5(%rip),%rax # 40204a <_IO_stdin_used+0x4a>
401195: 48 89 c7 mov %rax,%rdi
401198: b8 00 00 00 00 mov $0x0,%eax
40119d: e8 ae fe ff ff call 401050 <__isoc99_scanf@plt>
4011a2: 48 8d 45 e0 lea -0x20(%rbp),%rax
4011a6: 48 89 c6 mov %rax,%rsi
4011a9: 48 8d 05 a0 0e 00 00 lea 0xea0(%rip),%rax # 402050 <_IO_stdin_used+0x50>
4011b0: 48 89 c7 mov %rax,%rdi
4011b3: b8 00 00 00 00 mov $0x0,%eax
4011b8: e8 83 fe ff ff call 401040 <printf@plt>
4011bd: 90 nop
teams.live.com is sharing your screen.
Stop sharing
Hide

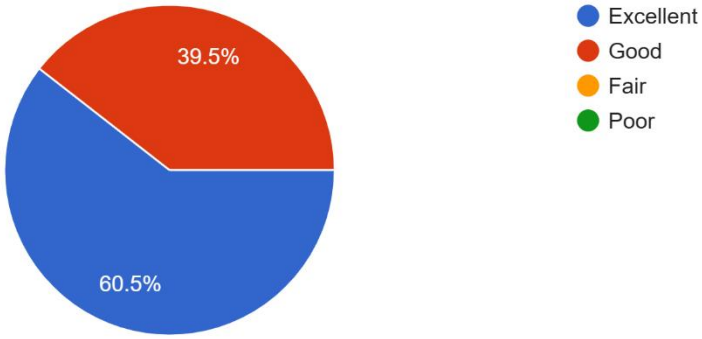
The topics covered in the FDP were well-structured and organized.

38 responses



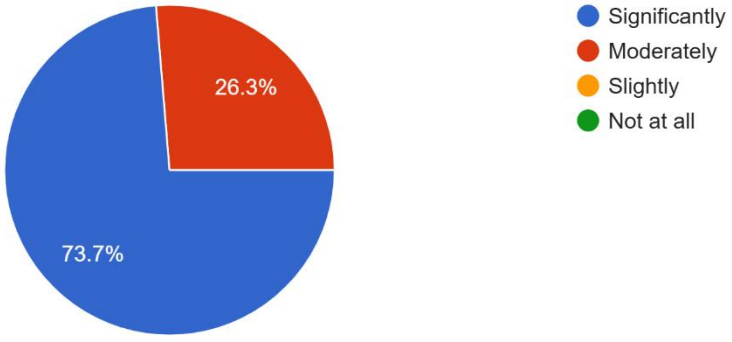
How effective were the resource persons in delivering the sessions?

38 responses



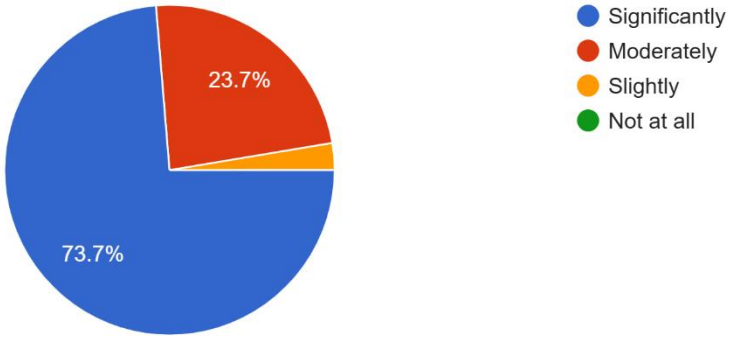
Learning Outcomes

38 responses



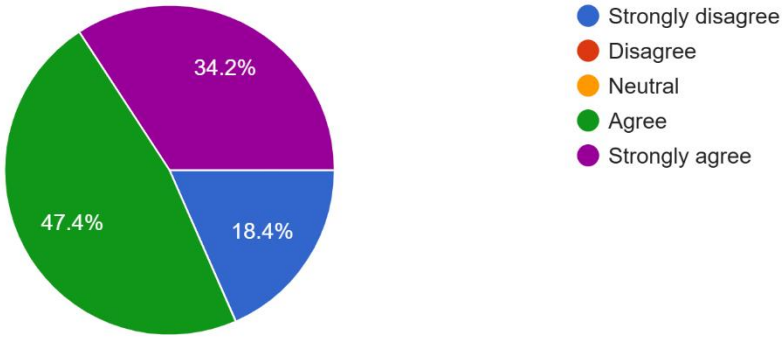
The FDP enhanced my knowledge/skills in the subject area.

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.

Estd: 1998

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**

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

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**

INSTITUTION'S INNOVATION COUNCIL (Ministry of Education Initiative)

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

Co-Ordinator **HoD**