Centre for Excellence in Cyber Law and Data Protection

ICFAI Law School, IFHE, Hyderabad

One Day Workshop on "Role of Artificial Intelligence in Cyber Security and Data Privacy

Inaugural and Workshop Session 1

Date: 24-10-2025

Time: 10:30 AM to 1:00 PM

Rapporteur: Rishitha Bacchu

A one-day workshop on "Role of Artificial Intelligence in Cyber Security and Data Privacy" was organized under the guidance of Akbar Sir and Dr. Arun Kumar. The workshop aimed to spread awareness among students about the impact of Artificial Intelligence (AI) on data protection, cyber security, and privacy in today's digital era. The event featured distinguished speakers Mr. Abhishek Mitra, CEO and Founder of ICSS, and Adv. Bafna, Cyber Forensic Expert who shared their experiences and insights on the practical and legal aspects of cybercrimes and data protection.

The inaugural session began with a warm welcome by Akbar Sir, who addressed the gathering of dignitaries, faculty members, and students. He introduced the centre and discussed how modern society has become increasingly dependent on data and technology. Citing the Cambridge Analytica case, he explained how citizens' personal data had been misused for political manipulation. He also discussed the concept of social scoring and highlighted how technology influences public opinion. He concluded by stating that Artificial Intelligence is a double-edged sword its effects depend entirely on how responsibly it is used.

Following this, Dr. Arun Kumar delivered his address and introduced the theme of the workshop and the esteemed speakers. He spoke about the growing reliance on technology and explained how every online activity contributes to data collection managed by Artificial Intelligence. He pointed out that most users accept terms and conditions on various applications without reading them, unknowingly compromising their privacy. He also emphasized that while AI can be a powerful tool to enhance security, it can also become a source of cyber threats if misused. His address encouraged students to gain deeper awareness of AI's dual role in modern digital systems.

Advocate Pankaj Bafna then shared his insights, expressing his delight in interacting with students. As a cyber forensic expert, he emphasized the importance of understanding the intersection between law and technology. He spoke briefly about the processes of digital evidence collection, investigation, and the growing demand for techno-legal experts in the evolving field of cyber law. His address set a strong foundation for the sessions that followed.

The inaugural session also featured remarks from Mr. Abhishek Mitra, CEO and Founder of ICSS, who shared his real-world experiences in the field of cyber security. He spoke about his association with Interpol and elaborated on how Artificial Intelligence is used both to safeguard and to compromise data systems. He discussed emerging threats such as deepfakes, phishing attacks, and targeted advertising, cautioning students about the risks of digital manipulation. He concluded by encouraging students to explore the domain of cyber security and to develop technical awareness alongside their legal knowledge.

The session concluded with a vote of thanks proposed by Rakesh Sir, who extended gratitude to all dignitaries and participants. He expressed appreciation to the Director and Dean (in absentia) for their constant guidance and support, and to the guest speakers Mr. Abhishek Mitra and Adv. Bafna for sharing their expertise. He also thanked Akbar Sir and Dr. Arun Kumar for their efforts in organizing the workshop and ensuring its success. The inaugural ceremony ended on a positive note, followed by a short tea break.

After the inaugural session, the first technical session was conducted by Mr. Abhishek Mitra. His presentation focused on "Cyber Incidents that Shaped Digital India" and offered students a glimpse into real-world cases of cybercrime and security breaches. He narrated several major incidents, including the 2016 hacking of Indian airports by Pakistani hackers, explaining how his team identified vulnerabilities and responded ethically to prevent further damage. He also mentioned the 2019 hacking of the Coal India website, where his team helped the authorities patch the security flaws.

During the session, Mr. Mitra demonstrated live examples of ethical hacking and explained how hackers exploit system weaknesses. He categorized hackers into black hat, white hat, and grey hat hackers, explaining their motives and roles. He discussed the concept of digital arrest and the alarming increase in scams involving voice and video manipulation. He warned students about phishing attacks, fake links, and cloned websites that mimic legitimate ones. Through live demonstrations, he showed how slightly altered URLs could deceive users and expose their data.

Mr. Mitra also explained smishing and vishing techniques, ATM skimming, and SIM spoofing. He shared real-life examples of online fraud during CoWIN registration and the use of AI-generated voice cloning for extortion. He gave an overview of the dark web, TOR browser, and the hidden digital spaces often used for illegal trade. He further demonstrated practical tools like "Marg Darshak" for phishing detection and explained password protection techniques to enhance personal cyber hygiene.

The session was highly interactive, and students actively participated in discussions and live demonstrations. Mr. Mitra concluded by emphasizing the importance of staying alert in the digital world and adopting safe online practices. His talk provided an excellent blend of technical and legal perspectives, leaving students inspired to explore the intersection of Artificial Intelligence, cyber security, and law. The session concluded with enthusiastic applause from the audience, followed by a lunch break before the commencement of the afternoon sessions.

Workshop Session 2

Date: 24-10-2025

Time: 2:00 PM to 3:00 PM

Rapporteur: Srinidhi

The session began with an interactive introduction, where the speaker initiated a discussion by asking how many students were familiar with Artificial Intelligence and how many were genuinely interested in pursuing cyber law. To everyone's surprise, very few students raised their hands, indicating that cyber law still remains an unexplored and less-preferred field among many. He then questioned the audience about their awareness of different cyber-related legislations such as the Information Technology (IT) Act, the Digital Personal Data Protection (DPDP) Act, and the Consumer Protection Act, emphasizing how each of these laws plays a vital role in the current digital age. Moving forward, the speaker spoke about the evolution of Artificial Intelligence, pointing out that although AI marketing has gained prominence recently, the concept itself has existed since 2010 and has now become deeply integrated into every aspect of our daily lives be it education, communication, or business.

He also discussed the important role that advocates play in the cyber domain, particularly in filing complaints before competent authorities in cases of cybercrime. To clarify a common misconception among students, he explained that cybercrime cases do not fall under the jurisdiction of civil courts. Instead, such matters are taken before the IT Tribunal, followed by the IT Appellate Tribunal, and finally, the Supreme Court completely bypassing the High Court. This insight gave the students a clearer understanding of the legal hierarchy in handling cyber-related disputes.

The speaker further highlighted the ongoing transition from the existing IT Act to the upcoming Digital India Act, which aims to modernize and strengthen India's legal framework in the digital sphere. He emphasized that with the implementation of the DPDP Act and related rules, practising in cyber law will become increasingly important and in-demand. He also shared real-life examples of how deepfake technology is creating serious problems, narrating incidents involving his own juniors at work who have faced the negative consequences of manipulated online content. These examples served as a stark reminder of the real-world impact of emerging digital threats.

Concluding the session, he encouraged students to view cyber law as a promising and evolving field, noting that it will soon become a major source of professional growth and financial opportunity for advocates. He explained that as companies continue to depend heavily on technology and data, the demand for legal professionals specializing in cyber compliance, data protection, and digital governance will rise sharply making cyber law an essential and rewarding career path for the future.

Workshop Session 3

Date: 24-10-2025

Time: 3:15 PM to 4:15 PM

Rapporteur: Srinidhi

This session revolved around the theme “Tackling Cyber Threats Using Generative AI.” Sir began by drawing a distinction between Artificial Intelligence and Generative AI, explaining that while AI performs data driven tasks, Generative AI has the capability to create new content, simulate human thinking, and generate outputs such as text, images, and code through intelligent prompts. Using a well prepared and engaging presentation, he explained how prompt engineering plays a critical role in cybersecurity as the right prompts can be used to train AI systems to identify malicious patterns, detect vulnerabilities, and strengthen online defences.

He further explained how AI has become an indispensable tool in today’s digital world, not only in cybersecurity but also in research, app development, business innovation, and automation. Encouraging students to adapt to this transformation, he stressed the importance of learning how to build and utilize AI responsibly rather than merely relying on it. Various graphs and statistical visuals were shown, demonstrating how Generative AI assists in analyzing vast amounts of data, predicting potential breaches, and providing real time solutions to cyber threats.

Sir then delved into the different types of cybercrimes and digital threats such as data theft, phishing, malware attacks, and ransomware, and elaborated on several cybersecurity tools used for detection and prevention including firewalls, intrusion detection systems, and vulnerability scanners. He also introduced the concept of Red Teams and Blue Teams in cybersecurity operations. The Red Team, he explained, comprises ethical hackers who simulate real world cyberattacks to test the robustness of an organization’s defences, while the Blue Team is responsible for monitoring, responding, and reinforcing systems against such simulated or actual threats. This collaborative strategy between both teams helps organizations develop stronger, more resilient security systems.

Throughout the session, he used short, informative videos to demonstrate how Generative AI can both aid and challenge cybersecurity efforts. He emphasized that while AI can automate protection mechanisms, it can also be exploited by cybercriminals to create advanced attacks making responsible usage and awareness essential. Concluding the session, he urged students to explore the immense career potential in the field of AI and cybersecurity, underscoring that understanding these technologies is no longer optional but a necessity in the rapidly evolving digital era.