SSIPMT RAIPUR

Department of Information Technology

TECHNO TALKS

VOLUME - 5

JULY - DEC 2026

SHRI SHANKARACHARYA INSTITUTE OF PROFESSIONAL MANAGEMENT AND TECHNOLOGY, RAIPUR

DEPARTMENT OF INFORMATION TECHNOLOGY PRESENTS

TECHNO TALKS

MISSION

1. **To create and disseminate knowledge and learning, innovation, and research in order to enhance society in meaningful and sustainable ways.**
2. **To encourage students to acquire multidisciplinary skills-sets by providing innovative education and research opportunities.**
3. **To strengthen ethical IT professionals and entrepreneurs through problem-solving and lifelong learning skills.**

VISION

To empower the young minds as world-class engineering professionals equipped with value- based contemporary skills and tools in the field of Information Technology.

"There's always something going on on the SSIPMT campus, and it's developed into a fascinating destination for the world's best minds to come together and share their vast reservoirs of knowledge and skills, and it has become a popular destination for students. The Institute devotes a significant amount of time and resources to assist students with innovations and startups. In addition, the institution provides assistance with their communication skills, critical thinking capacity, sense of responsibility and ethical values and ultimately enhances the placements on the campus.

Shri Nishant Tripathi
Chairman (B.G), SSIPMT

At SSIPMT, we are committed to provide our students with the best possible start in life. As part of our goal, we wish to inculcate in our students a passion for learning that will enable them to make a positive contribution to the world in which they live. Students, parents, and the institution all contribute to the creation of a vibrant learning environment on our campus. The success of our students is a direct outcome of the quality of our collaborative effort."

"It gives me immense pleasure to pen a few words about our newsletter meant for churning out the latent writing talent which bears immense potentiality of sharpening student's communication skill as part of student's overall personality development. I congratulate all the contributors and the editorial board for bringing out such a beautiful magazine, in SSIPMT, it is believed and practiced that excellence is a continuous precess and in pursuit of which the institute has made deep forays into contributing world-renowned technocrats, successful entrepreneurs, competent & Innovative engineers.

Dr. Alok Kumar Jain
Principal, SSIPMT

My Best wishes to the Techno Talks to achieve all of its a objectives."

"It brings me great pleasure to congratulate the Information Technology department's students, faculty, and staff on the release of the department's inaugural newsletter. Published biannually, it serves as an important source of information on academics, achievements, and departmental innovations. The newsletter provides a platform for teachers and students to share their ideas and perspectives, supporting their academic growth. I strongly believe that one must find meaning in daily work, and knowing that your efforts positively impact others brings out your best. It is truly an honor to be part of such a motivated environment. I wish all team members the very best for the publication. "

Mr. Sunil Dewangan
Assistant Professor and Head, IT Dept.

FUTURE OF CYBERSECURITY IN THE AI ERA MEMORANDUMS

The future of cybersecurity in the AI era is best understood not simply as stronger protection, but as an intelligent digital defense system. Similar to how the human immune system detects harmful threats before they spread, AI-powered cybersecurity enables systems to identify suspicious activity and respond to threats in real time, without waiting for manual intervention.
Rather than relying only on predefined security rules, AI systems continuously analyze patterns, learn from emerging threats, and adapt their defenses accordingly. This shifts the traditional paradigm from reactive security with fixed defenses to proactive, intelligent protection. As a result, AI can accelerate threat detection, reduce response time, strengthen data privacy, and help organizations remain resilient against increasingly sophisticated cyberattacks. In essence, AI-powered security systems act as digital first responders, handling routine threats automatically while escalating critical incidents for deeper human analysis."

Mr. Sunil Dewangan
(Assistant Professor and Head, IT Dept.)

"Future of Cybersecurity in the AI Era refers to the growing use of artificial intelligence to detect, prevent, and respond to digital threats. AI-powered security systems can continuously monitor networks, devices, and user activity to identify suspicious patterns and potential attacks. By analyzing large amounts of data in real time, AI enables faster threat detection and reduces dependence on manual monitoring. It can strengthen data protection by identifying vulnerabilities, detecting unusual behavior, and responding to threats more efficiently. AI-driven cybersecurity is becoming increasingly important in areas such as network protection, fraud detection, cloud security, and privacy. This approach makes security systems more adaptive, proactive, and reliable in an increasingly connected digital environment."

Dr. Advin Manhar
(Assistant Professor, IT Dept.)

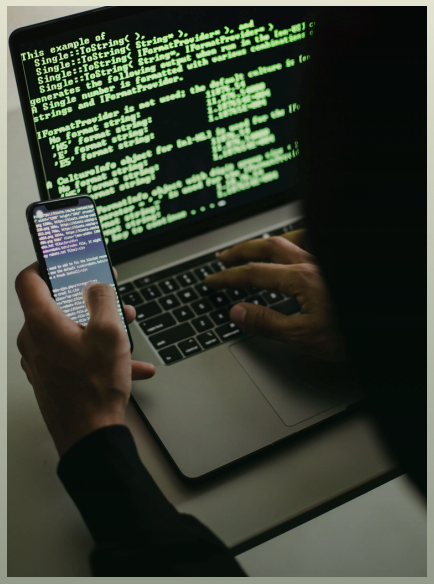
"The evolving field of cybersecurity has gained significant attention in recent times due to the growing need to protect digital systems from increasingly sophisticated threats. With the integration of artificial intelligence, modern cybersecurity systems can analyze large amounts of data, detect unusual patterns, and respond to potential attacks in real time with improved speed and efficiency. This approach strengthens data protection and security by enabling proactive threat detection and reducing the risk of breaches. AI-powered cybersecurity is widely applied in areas such as network protection, fraud detection, cloud security, and digital privacy, where continuous monitoring and rapid response are essential. Thus, the future of cybersecurity in the AI era is emerging as a powerful approach to strengthening digital protection and building more secure and resilient technological systems."

Mrs. Akanksha Mishra
(Assistant Professor, IT Dept.)

"Future of Cybersecurity in the AI Era is an exciting field where artificial intelligence helps protect systems, networks, and data from evolving threats. It is already used in real-life applications such as fraud detection, threat monitoring, and security systems. The biggest advantage is faster threat detection, quicker response, and stronger data protection. Learning AI-driven cybersecurity can boost your placement opportunities, as industries are actively looking for such skills. It is especially important as cyber threats become more advanced. I encourage you to explore this topic, as it can open doors to innovative projects and high-demand career paths."

Mr. Niraj Sahu
(Assistant Professor, IT Dept.)

THE FUTURE OF CYBERSECURITY IN THE AI ERA



- **INTRODUCTION**
- **ADVANTAGES & DISADVANTAGES**
- **FACTS & FIGURES**
- **EMERGING THREATS : THE DARK SIDE OF AI**
- **THE NEXT LINE OF DEFENSE**
- **WHAT LIES AHEAD : PREDICTIONS & TAKEAWAYS**

Context & Outlook

Artificial Intelligence is rewriting the rules of the digital world and cybersecurity is right at the center of this transformation. What used to be a battle between hackers and firewalls has evolved into a much more complex war between intelligent systems. On one side, AI is empowering defenders with tools that can detect threats in real time, predict attacks before they happen, and automate responses at a scale no human team could match. On the other side, the very same technology is arming attackers enabling hyper-realistic phishing scams, automated malware that adapts on the fly, and deepfakes that can fool even trained professionals.

As organizations race to adopt AI for efficiency and innovation, they're also opening new doors for exploitation. Cybersecurity is no longer just about protecting networks and data it's about securing the AI systems themselves, from the algorithms they run on to the massive datasets that train them. This newsletter dives into how AI is reshaping the cybersecurity landscape: the opportunities it creates, the risks it introduces, and what the future might look like as both attackers and defenders continue this AI-powered arms race.

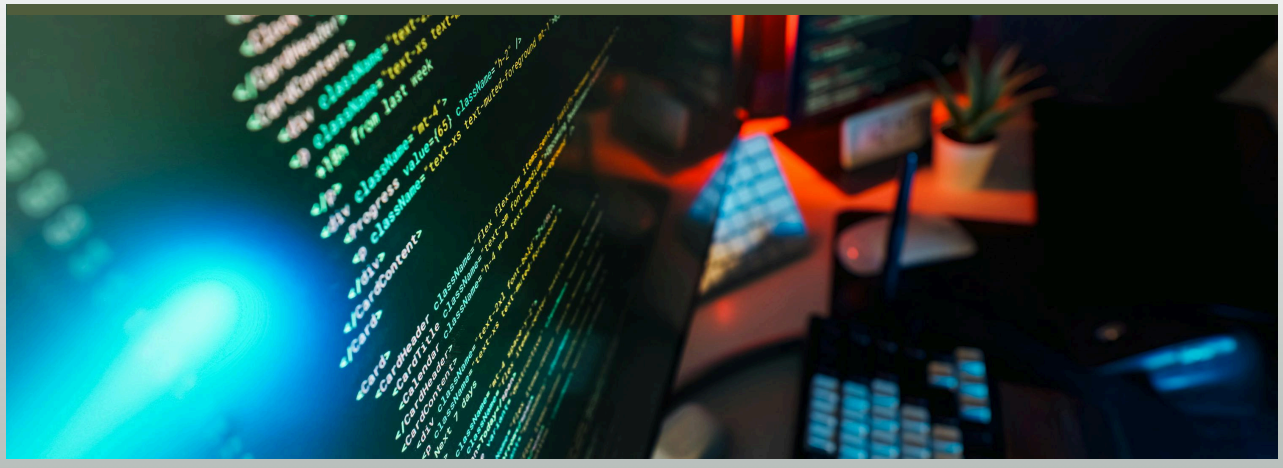
ADVANTAGES

- AI scans huge volumes of network traffic in real-time, identifying suspicious patterns and anomalies within seconds something that would take human analysts hours or even days to manually catch.
- By analyzing historical attack data, AI models can forecast likely vulnerabilities and attack vectors before they're exploited, shifting cybersecurity from a reactive approach to a proactive, prevention-first strategy.
- Unlike human teams that work in shifts and get fatigued, AI systems continuously monitor networks, servers, and endpoints around the clock catching attacks even during odd hours when human vigilance typically drops.
- A large percentage of breaches happen due to simple human mistakes like misconfigurations or delayed responses. Automating routine tasks such as log analysis and alert triaging significantly minimizes these errors.
- As organizations grow, their digital footprint expands rapidly. AI-driven security solutions can scale almost instantly across thousands of devices and massive cloud infrastructures without a proportional rise in cost or manpower.
- AI doesn't just detect threats it can automatically isolate infected systems, block malicious traffic, or shut down compromised accounts within seconds, drastically limiting the damage before a human even gets involved.
- While initial setup can be expensive, AI reduces long-term costs by cutting down on manual labor, minimizing breach-related financial losses, and preventing costly downtime from successful attacks.

DISADVANTAGES

- The same AI tools used for defense are being weaponized by hackers to craft hyper-realistic phishing emails, generate deepfakes for social engineering, and build adaptive malware that evades traditional detection.
- Deploying advanced AI security infrastructure requires significant investment in specialized hardware, quality training data, skilled professionals, and continuous system updates often out of reach for smaller organizations.
- AI models trained on incomplete or biased data can misjudge threats, leading to a flood of false alarms that waste analyst time, or worse, missing genuine attacks entirely.
- Excessive dependence on AI can cause human expertise to erode over time. If the system malfunctions or is compromised, organizations may be left dangerously unprepared to respond manually.
- Effective AI security requires access to massive datasets, often including sensitive user and organizational information, raising serious concerns about how this data is collected, stored, and protected.
- Many AI systems operate as a "black box," making decisions without clear explanations. This makes it difficult for security teams to understand why a threat was flagged or dangerously, why one was missed.
- Sophisticated hackers can deliberately feed AI systems misleading or manipulated data, tricking detection models into misclassifying malicious activity as safe a technique known as adversarial machine learning.

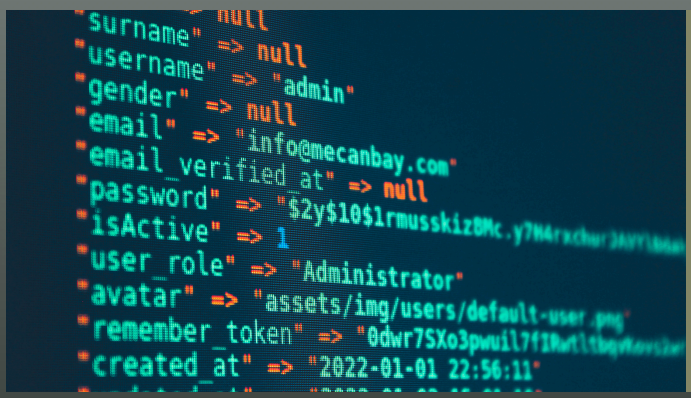
FACTS AND FIGURES



"Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks."

~ Stephen Hawking, Theoretical Physicist

"Around 95% of cybersecurity breaches are still linked to human error misconfigurations, weak passwords, or falling for phishing scams. AI-driven automation is increasingly being deployed to close this gap by reducing dependency on manual processes."



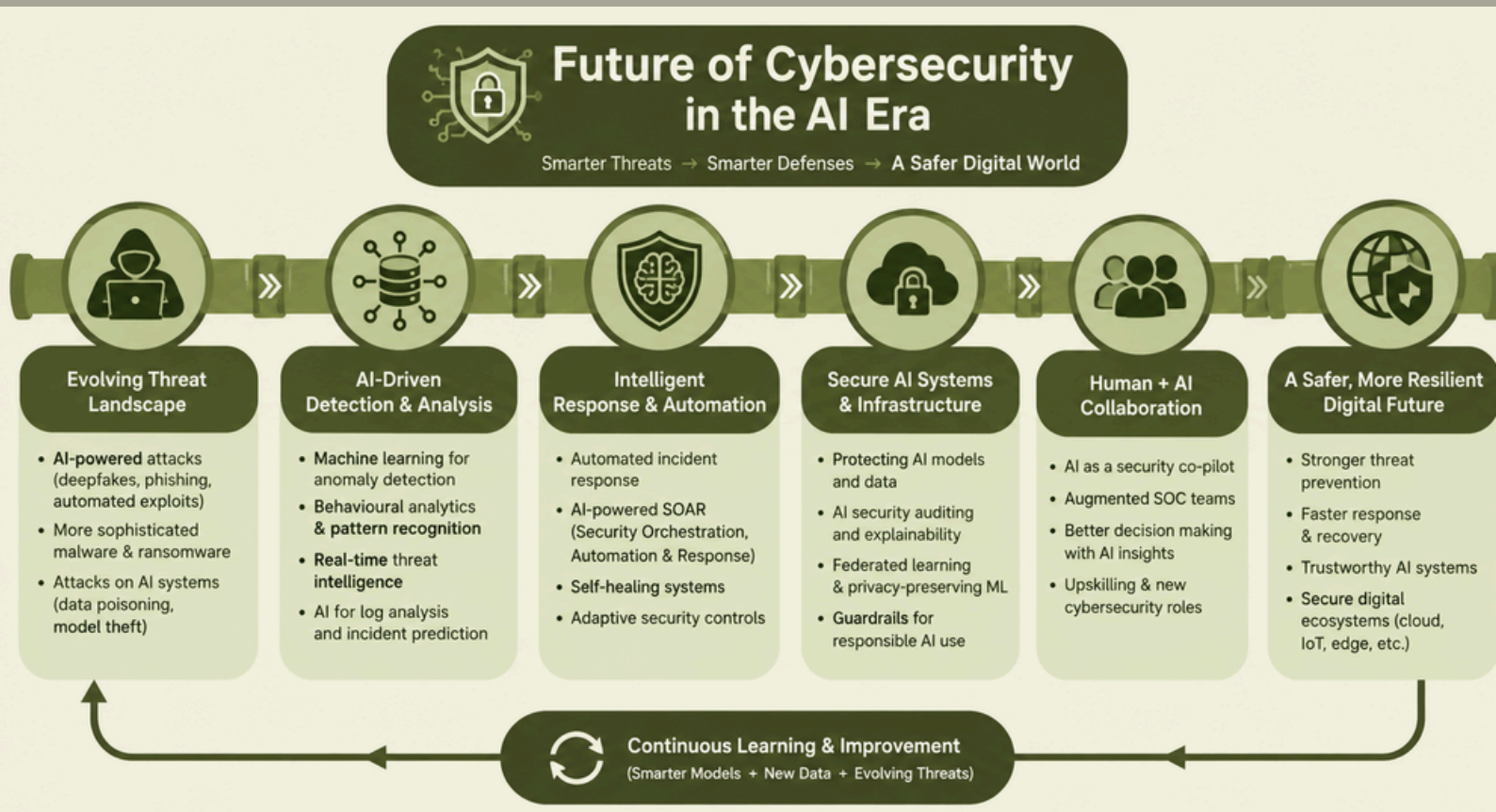
"Global investment in AI-powered cybersecurity solutions is projected to surpass $135 billion by 2030, as organizations worldwide race to integrate intelligent defense systems into their infrastructure."

"Traditional breach detection has historically taken an average of 207 days. With optimized AI-driven systems, this can now be reduced to under a minute, allowing for near-instant threat containment."

EMERGING THREATS : THE DARK SIDE OF AI

“As artificial intelligence becomes more powerful and accessible, it's not just cybersecurity teams who are benefiting cybercriminals are exploiting the same technology to launch faster, smarter, and far more convincing attacks. Phishing emails once riddled with typos are now hyper-personalized and nearly indistinguishable from genuine communication. Deepfake audio and video are being used to impersonate executives and trick employees into authorizing fraudulent transactions. Malware is no longer static AI-powered variants can adapt in real-time, rewriting themselves to slip past traditional security systems. What we're witnessing is the rise of an entirely new kind of digital warfare, one where attacking algorithms and defending algorithms clash at speeds far beyond human reaction time. As this arms race accelerates, the line between innovation and exploitation continues to blur, making the future of cybersecurity as much about outsmarting AI as it is about building it.

"AI IS GOING TO BE EXTREMELY BENEFICIAL AND ALREADY IS TO THE FIELD OF CYBERSECURITY. IT'S ALSO GOING TO BE BENEFICIAL TO CRIMINALS."
~ DMITRI ALPEROVITCH, CO-FOUNDER & FORMER CTO, CROWDSTRIKE

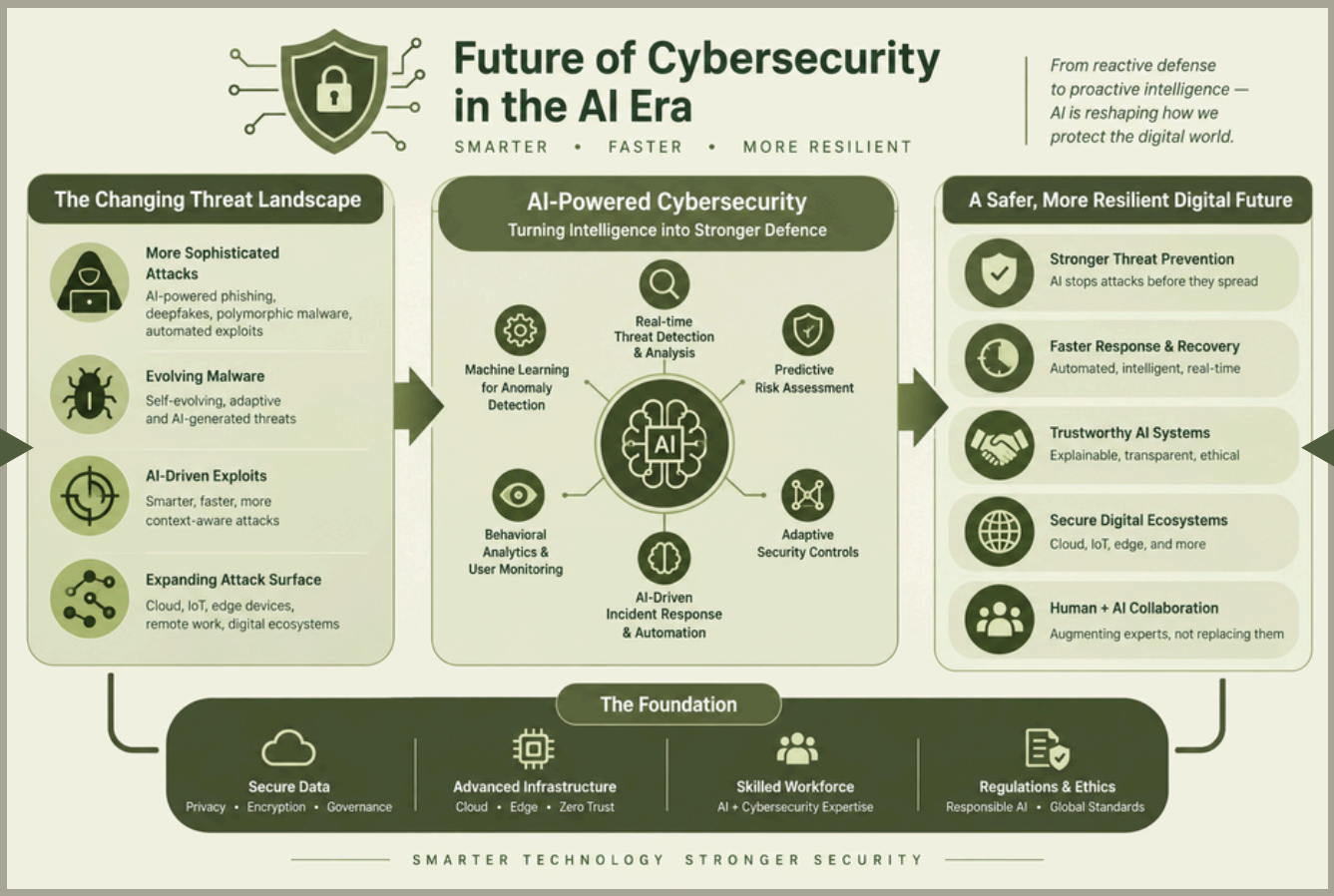


THE NEXT LINE OF DEFENSE

"WE ARE MOVING FROM AI AS AN EFFICIENCY TOOL TO AI MAKING AUTONOMOUS SECURITY DECISIONS. THAT SHIFT IS BOTH POWERFUL AND RISKY. THE FUTURE OF CYBER LEADERSHIP WILL BE ABOUT STRIKING THE RIGHT BALANCE TRUSTING AI WHILE MAINTAINING HUMAN OVERSIGHT."

~ TIMOTHY YOUNGBLOOD, CISO, ASTRIX SECURITY (FORMER CISO, MCDONALD'S)

"As AI-driven attacks grow more sophisticated, cybersecurity defense is shifting toward equally intelligent, autonomous systems. Tomorrow's security won't just react to threats it will predict them using AI models that flag vulnerabilities before they're exploited. Self-healing networks are leading this shift, capable of detecting a breach, isolating it, and patching the vulnerability within seconds, without human intervention. Platforms like Darktrace's Antigena and CrowdStrike's Falcon, powered by Charlotte AI, already showcase this today. Meanwhile, zero-trust architecture is being strengthened by AI's ability to continuously verify identity through behavioral biometrics like typing patterns and mouse movements. Looking ahead, quantum-AI security and AI-powered deception tech (honeypots) promise even stronger, self-healing defense systems for the future."



WHAT LIES AHEAD - PREDICTIONS & TAKEAWAYS

Predictions for the Future:

- By 2030, most large enterprises will run autonomous, self-healing security systems requiring minimal human intervention.
- AI vs AI warfare will become the norm attacking algorithms and defending algorithms clashing in real-time at machine speed.
- Quantum-AI security will emerge as the next frontier, offering encryption that's virtually unbreakable by even the most advanced attackers.
- Deepfake detection tools will become as essential as antivirus software, integrated into everyday communication platforms.
- Cybersecurity roles will shift from manual monitoring to AI oversight and strategy professionals will manage and train AI systems rather than chase alerts manually.
- Regulatory frameworks around AI use in cybersecurity will tighten globally, addressing ethical concerns, bias, and data privacy.
- Smaller businesses will gain access to affordable, AI-driven security tools, narrowing the gap between enterprise-level and small-business protection.

Key Takeaways:

- **AI is a double-edged sword the same technology defending our systems is being used to attack them.**
- **The future belongs to organizations that strike the right balance: leveraging AI's speed while maintaining human oversight for critical decisions.**
- **Staying ahead in cybersecurity will require continuous adaptation, not one-time fixes as AI evolves, so must our defenses.**
- **Investing in AI literacy and skills today will be crucial for cybersecurity professionals to remain relevant tomorrow.**
- **Ultimately, trust, transparency, and ethical AI development will determine whether AI becomes cybersecurity's greatest ally or its biggest threat.**

NEWS LETTER TEAM

Mrs. Mahejabi Khan
Assistant Professor
(Incharge)Department of Information Technology

I feel that the future of cybersecurity in the AI era is bringing a real shift in how we protect digital systems today. Instead of relying only on traditional security methods, AI can help detect threats faster and make systems more secure and efficient.

What I find most important is how it can improve data protection while still enabling real time threat detection and response. Today, we can clearly see its growing impact in areas like network security, fraud detection, cloud systems, and privacy.

I always encourage my students to explore such emerging technologies. Cybersecurity in the AI era is not just a concept to study, but something they should try to understand practically. It opens up many opportunities for innovation and helps them prepare better for the future.

EXECUTIVES

Ayushi Chandrakar
-Executive Editor
(IT, 7th semester)

Palak Singh Rathour
-Documentation
(IT, 7th semester)

Gagan Rai
-Lens Man
(IT, 7th semester)

Shrejal Sharma
-Proof Reader
(IT, 7th semester)