SAIRAM
COLLEGE OF ENGINEERING
Anekal, Bengaluru

Accredited by NAAC
ISO 9001:2015 Certified Institution
Approved by AICTE, New Delhi
Affiliated to Visvesvaraya Technological University
www.sairamce.edu.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Date: 29.07.2026

REPORT – KNOWLEDGE SHARING SESSION ON "CYBER SECURITY: THREATS, DEFENSE AND EMERGING TRENDS"

The Department of Electronics and Communication Engineering, Sri Sairam College of Engineering, Bangalore, conducted a knowledge-sharing session on "Cyber Security: Threats, Defense and Emerging Trends" on 28th July 2026. The session was conducted as an outcome of the knowledge and learning gained through the AICTE-QIP Course on Cyber Security attended at the Indian Institute of Information Technology Dharwad (IIIT Dharwad).

The AICTE-QIP course provided valuable exposure to the fundamentals of cybersecurity, cyber threats, vulnerabilities, preventive measures, and emerging security practices. Based on the knowledge acquired through the course, the concepts were further consolidated and presented as a knowledge-dissemination activity. The objective was to share the learning gained from the course and create awareness about cybersecurity and its growing importance in the present digital environment. The session introduced the fundamental concepts of Information Security, Physical Security, Digital Security, and Cybersecurity. Cybersecurity was explained as the practice of protecting internet-connected systems, networks, and data from unauthorized access, damage, and digital attacks. The importance of security in an institutional environment, particularly in protecting student records, personal information, digital systems, networks, and institutional resources, was also highlighted.

The session covered the evolution of cybersecurity and the Internet of Things (IoT), highlighting the increasing connectivity of devices and the security challenges associated with connected technologies. The growth of IoT and the emergence of vulnerabilities in connected devices emphasized the need for stronger cybersecurity practices. Major cybersecurity threats including viruses, hackers, malware, Trojan horses, and password attacks were discussed. Different categories of hackers, namely White Hat, Grey Hat, and Black Hat hackers, were explained along with their roles and objectives. Various types of malware, including viruses, worms, Trojans, spyware, adware, rootkits, and crimeware, were also discussed. Preventive measures such as strong passwords, firewalls, antivirus and anti-malware solutions, network threat protection, and regular backups were emphasized.

The session further focused on emerging trends in cybersecurity, including Artificial Intelligence and Machine Learning, threat detection and response, predictive analytics, automation, ransomware mitigation, cloud security, and the growing cybersecurity skills gap. The importance of training and upskilling in cybersecurity was also highlighted. A major component of the session was Cyber Threat Intelligence (CTI). CTI was explained as the process of collecting and analyzing

information about cyber threats to provide detailed, contextual, and actionable threat information. The session highlighted the role of CTI in proactive defense, informed decision-making, faster incident response, resource optimization, and enhanced situational awareness. The three major types of Cyber Threat Intelligence—Strategic, Operational, and Tactical Threat Intelligence—were also discussed.

The session also introduced emerging cybersecurity approaches such as AI-Based Cybersecurity, intelligent firewalls, AI automation, predictive analytics, Zero Trust Architecture, cloud security, behavioral analysis, threat intelligence platforms, and automated response systems. Zero Trust Architecture was highlighted as an approach involving verification of access attempts and continuous monitoring to minimize data-breach risks.

Following the presentation, an interactive quiz was conducted through Mentimeter to assess and reinforce the participants' understanding of the concepts discussed during the session. The quiz questions were prepared based on the contents of the presentation and covered areas such as the fundamentals of cybersecurity, types of security, major cyber threats, malware, hackers, password security, Cyber Threat Intelligence, AI-based cybersecurity, Zero Trust Architecture, cloud security, and emerging cybersecurity trends. The Mentimeter-based quiz provided an interactive and engaging assessment platform, enabling participants to respond to the questions in real time. The activity helped reinforce the concepts presented during the session and provided an opportunity to assess the participants' understanding and learning outcomes.

The session served as a knowledge-dissemination outcome of the AICTE-QIP Cyber Security course attended at IIIT Dharwad. The learning gained through the course was consolidated, structured, and presented in an academic environment. The subsequent Mentimeter quiz provided an opportunity to reinforce the acquired knowledge and assess the effectiveness of the knowledge-sharing activity.

The activity helped enhance awareness of cyber threats, cybersecurity practices, defensive mechanisms, Cyber Threat Intelligence, Artificial Intelligence in cybersecurity, Zero Trust Architecture, cloud security, and emerging security trends. It also demonstrated the effective application and dissemination of knowledge gained through professional development.

The knowledge-sharing session successfully combined professional learning, knowledge dissemination, presentation, and interactive assessment. The learning acquired through the AICTE-QIP Cyber Security course at IIIT Dharwad was effectively translated into a structured academic session, followed by a Mentimeter-based quiz to reinforce and assess the concepts presented. The activity contributed to creating greater awareness of cybersecurity and encouraged participants to develop a proactive approach towards protecting digital systems and information.







Dr.P.Hosanna Princye

HOD 28/8/26

29/08/2026