(M.TECH)

Course Duration

4 Semesters
(2 Years)

Eligibility Criteria

B E/B.Tech. in CSE/ISE/TE/ECE/EEE/IT/MCA/M.Sc in Computer Science or Mathematics or Information Science or Information Technology with a minimum of 50% (45% in case of SC/ST) marks in aggregate of any recognized University/Institution or AMIE or any other qualification recognized as equivalent thereto.

Overview

The M.Tech in Cybersecurity programme is designed to provide an outcome-driven and skill-based learning to make students become proficient cybersecurity professionals. Experiential learning with proprietary and open software programmes is the one of the best academic facilities of this programme. The School offers state-of-theart infrastructure to reproduce a real-time simulator-like environment to defend against cyberattack scenarios.

WHAT MAKES THE PROGRAMMEME UNIQUE?

Designed keeping in mind the exponential growth in the usage of information technology and the demand for huge number of cyber security professionals to counter measure online cyber-attacks.

Meet the demands of the future job market especially demand for cyber security professionals.

Designed with inputs from industry professionals and academic experts from various universities in India and abroad.

Some of the important courses of study include: cryptography, cloud security, block chain technology, cyber physical systems, Firewall and UTM architecture, digital forensics, ethical hacking, security architecture with solid theoretical foundation and project-based skills.

NASSCOM DSCI Certification

"Security Analyst" Certification from NASSCOM DSCI is integrated into the programme, which is a widely recognized industry certification. The certification will provide the participants the following skills:

- Coordinate responses to information security incidents.
- Contribute to managing information security.
- Install and configure information security devices.
- Contribute to information security audits etc.

Course Curriculum

- Sem - 1
- Sem - 2
- Sem - 3
- Sem - 4

01 Cyber Security and Programming
02 Mathematics for Cyber Security
03 Cyber Forensics (Entrepreneurship)
04 Security and investigation of the block chain
05 Ethical Hacking and Network Defense
06 Mini Project (Innovation and Intellectual Property)

Programme Educational Objectives (PEOs)

Graduates of M.Tech. (Cyber security) will be able to:

PEO-1

Demonstrate skills as a Cybersecurity professional and perform duties with ethical and moral values.

PEO-2

Engage in active research for professional development with an attribute of lifelong learning.

PEO-3

Be an active and useful members of the society contributing to the economic and technological development of the nation and the world.

PEO-4

Take up entrepreneurship.

Programme Outcomes (POs)

On successful completion of the programme, graduates of M.Tech (Cyber security) programme will be able to:

PO 1

Demonstrate in-depth knowledge of specific discipline or professional area, including wider and global perspective, with an ability to discriminate, evaluate, analyse and synthesise existing and new knowledge, and integration of the same for enhancement of knowledge.

PO 2

Analyse complex engineering problems critically, apply independent judgment for synthesizing information to make intellectual and/or creative advances for conducting research in a wider theoretical, practical and policy context.

PO 3

Think laterally and originally, conceptualize and solve engineering problems, evaluate a wide range of potential solutions for those problems and arrive at feasible, optimal solutions after considering public health and safety, cultural, societal and environmental factors in the core areas of expertise.

PO 4

Extract information pertinent to unfamiliar problems through literature survey and experiments, apply appropriate research methodologies, techniques and tools, design, conduct experiments, analyze and interpret data, demonstrate higher order skill and view things in a broader

perspective, contribute individually/in group(s) to the development of scientific/technological knowledge in one or more domains of engineering.

PO 5

Create, select, learn and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and modeling, to complex engineering activities with an understanding of the limitations.

PO 6

Possess knowledge and understanding of group dynamics, recognize opportunities and contribute positively to collaborative-multidisciplinary scientific research, demonstrate a capacity for self-management and teamwork, decision-making based on open-mindedness, objectivity and rational analysis in order to achieve common goals and further the learning of themselves as well as others.

PO 7

Demonstrate knowledge and understanding of engineering and management principles and apply the same to one’s own work, as a member and leader in a team, manage projects efficiently in respective disciplines and multidisciplinary environments after consideration of economic and financial factors.

PO 8

Communicate with the engineering community, and with society at large, regarding complex engineering activities confidently and effectively, such as, being able to comprehend and write effective reports and design documentation by adhering to appropriate standards, make effective presentations, and give and receive clear instructions.

PO 9

Recognize the need for, and have the preparation and ability to engage in life-long learning independently, with a high level of enthusiasm and commitment to improve knowledge and competence continuously.

PO 10

Acquire professional and intellectual integrity, professional code of conduct, ethics of research and scholarship, consideration of the impact of research outcomes on professional practices and an understanding of responsibility to contribute to the community for sustainable development of society.

Programme Specific Outcomes

On successful completion of the programme, graduates of M.Tech. (Cybersecurity) will be able to:

- **PSO-1:** Develop an in-depth knowledge and skill sets in Cybersecurity to monitor, prepare, predict, detect and respond and prevent cyber-attacks and ensure enterprise security.
- **PSO-2:** Identify, assess and protect the enterprise IT assets and risks, perform risk analysis and develop policies and procedures based on compliance and able to define the architecture, design, and management of the security of an organisation.
- **PSO-3:** Monitor, detect, respond, remediate cyber security threat using latest hardware and software tools and technologies, along with analytical and managerial skills to arrive at cost effective and optimum solutions either independently or as a team.
- **PSO-4:** Review scholarly work by referring journals, define a new problem, design, model, analyse and evaluate the solution and report as a project in the area of Cybersecurity.

Career Opportunities

- Cybersecurity Analyst
- Security Engineer
- Security Architect
- Security Administrator
- Security Software Developer
- Cryptanalyst
- Digital Forensic Analyst
- Vulnerability Assessor
- Cloud Security Architect
- Intrusion Detection Specialist

- Cybercrime Investigator
- Malware Analyst, Data Privacy Officer
- Computer Security Incident Responder
- Governance Compliance & Risk (GRC) Manager
- Security Consultant

Fee

- **Indian / SAARC Nationals₹ 1000**
- **NRI Fee₹ 2000**
- **Foreign NationalsUS$ 50**