About the Program

The Executive M.Tech. in Computer Science and Engineering (Specialization in Cyber Security) is designed for working professionals aiming to develop advanced expertise in securing modern computing systems and digital infrastructures. The program addresses the growing demand for skilled cybersecurity professionals capable of protecting critical information assets in an increasingly interconnected world.

The curriculum provides a strong foundation in core computer science areas such as programming, data structures, databases, operating systems, and computer networks, while integrating specialized knowledge in cryptography, network security, operating system security, and distributed systems. Advanced electives such as ethical hacking, digital forensics, malware analysis, and security auditing enable learners to gain hands-on exposure to real-world cyber threats and defence mechanisms.

It aims to prepare professionals for roles in cybersecurity engineering, threat analysis, digital forensics, and security consulting, while fostering research and innovation in secure computing systems.

Program Educational Objectives

PEO-1	Build a strong foundation in mathematical, computational, and algorithmic principles underlying cybersecurity.
PEO-2	Develop advanced technical skills in cybersecurity for digital forensics, malware analysis, information warfare, secure software engineering, and secure governance.
PEO-3	Design and implement security governance, regulatory compliance, and audit functions using diverse frameworks.
PEO-4	Practice ethical conduct, legal awareness, and societal responsibility in all aspects of cybersecurity.
PEO-5	Pursue lifelong learning to adapt to evolving threats, emerging technologies, and new regulatory requirements.
PEO-6	Exhibit leadership and teamwork skills to manage Security-based projects in multidisciplinary environments.

Program Outcomes

PO-1	Apply knowledge of mathematics, computing, and cybersecurity techniques to solve complex engineering problems.
PO-2	Analyze and design efficient algorithms and methods for data-driven decision-making.
PO-3	Develop, evaluate, and deploy cybersecurity and secure systems with consideration of scalability and performance.
PO 4	Utilize the latest cybersecurity tools and techniques, including various security standards and audit reports.
PO-5	Communicate technical concepts effectively to both technical and non-technical stakeholders.
PO-6	Demonstrate project management and collaborative skills in a professional environment.

Curriculum of Executive M.Tech.
in
Computer Science and Engineering (with Specialization in Cyber Security)

Semesters	Subject Code	Subject Name	Category	L	T	P	Credits
Semester-1	CS34111CS	Advance Programming with Python	DC	2	0	2	3
	CS34112CS	Mathematical foundation for Computer Science	DC	3	0	0	3
	CS34113CS	Advanced Data Structures & Algorithms	DC	2	0	2	3
	CS3412XCS	Elective-1	DE	3	0	0	3
Semester-2	CS34211CS	Digital Forensics and Incident Response	DC	2	0	2	3
	CS34212CS	Information System security	DC	2	0	2	3
	CS34213CS	Operating System Security	DC	2	0	2	3
	CS3422XCS	Elective-2	DE	3	0	0	3
Semester-3	CS3432XCS	Elective-3	DE	3	0	0	3
	CS3432XCS	Elective-4	DE	3	0	0	3
	CS34351CS	Project work / Dissertation-I	PW	-	-	16	8
Semester-4	CS34451CS	Project Work / Dissertation-II	PW	-	-	36	18
			Total Credits				56

Tentative List of Elective Subjects may be updated as and when required			
Elective-1		**Elective-2**	
CS34121CS	Advance Computer Networks	CS34221CS	Foundation of Modern Cryptography and Applications
CS34122CS	Blockchain Technology	CS34222CS	Quantum Cryptography

Tentative List of Elective Subjects may be updated as and when required			
Elective-3		**Elective-4**	
CS34321CS	Ethical Hacking and Penetration Testing	CS34324CS	Cloud Security
CS34322CS	Malware Analysis and Reverse Engineering	CS34325CS	Information Warfare
CS34323CS	Secure Software Engineering	CS34326CS	Security Standards and Audits