भारतीय प्रौद्योगिकी संस्थान भुवनेश्वर
INDIAN INSTITUTE OF TECHNOLOGY BHUBANESWAR
शैक्षणिक अनुभाग /Academic Section

15-62/2025-Acad/Minutes-69th **दिनांक/dated. 31 July, 2026**

कार्यालय आदेश सं./Office Order No. 446 / 2026

Senate : 69th Meeting held on 13th April, 2026
Sub. : New course for Blended-Mode M.Tech "Cyber Security" in SECS –reg
Ref. : Agenda Item No. 69.A.C.3

1. The undersigned is directed to convey that the Senate has approved the introduction of a new course, **"Cyber Security,"** under the **Blended-Mode M.Tech. Programme**, as proposed by the **School of Electrical and Computer Sciences**.

2. The detailed course structure is enclosed as **Annexure-I**.

3. All other generic terms and conditions governing the programme shall be as prescribed in the **Blended-Mode M.Tech. Regulations**, as amended from time to time.

Jigyasha 31/07/2026
सहायक कुलसचिव (स्ना. और अ.का.) /
Assistant Registrar (PG & RP)

सेवा में /To
Committee Members

प्रतिलिपि/Copy to

1. Chairperson, Senate
2. All Members of the Senate
3. All Heads of the Schools/Departments
4. Respective Blended Mode Coordinator
5. Faculty Members
6. PS to Director
7. PS to Registrar
8. Office Order file
9. Senate File

Indian Institute of Technology Bhubaneshwar

Proposal Document

for

Blended Mode M.Tech in Cyber Security

Program
Offered by the

Department of Computer Science and Engineering

With Industry Partner

WhizHack Technologies Pvt. Ltd.

1. Objectives of the Programme

The primary objective of this programme is to provide students with advanced knowledge and skills in the field of cybersecurity and to prepare them for roles that require expertise in safeguarding digital assets and data. The key objectives of this programme are:

- Advanced Cybersecurity Knowledge: Develop an in-depth understanding of cybersecurity principles, including threat detection, risk assessment, incident response, and security policies.
- Technical Competence and Practical Skills: Build expertise in network security, cryptography, secure software development, ethical hacking, and hands-on use of modern cybersecurity tools.
- Secure Design and Risk Management: Enable students to design secure systems and architectures, assess organizational risks, and implement effective security and compliance strategies.
- Emerging Technologies and Research Orientation: Foster innovation and research capabilities, with emphasis on AI-driven security solutions and evolving cybersecurity techniques.
- Professional, Ethical, and Leadership Development: Prepare graduates for leadership roles with strong ethical grounding, effective communication skills, and the ability to manage security teams and respond to real-world challenges.

2. Learning Outcome

The learning outcomes of the M.Tech in Cyber Security programme are designed to demonstrate the knowledge, skills, and competencies students are expected to acquire upon completion of the programme. At the end of the programme, learners should be able to:

- Possess comprehensive knowledge of cybersecurity principles, threat landscapes, risk management, and compliance frameworks.
- Apply skills in cryptography, network security, secure development, ethical hacking, and cybersecurity tools to analyze and solve security challenges.
- Design secure architectures, assess organizational risks, and implement effective mitigation and incident response strategies.
- Leverage AI, blockchain, and advanced techniques while contributing to cybersecurity research and innovation.
- Communicate effectively, adhere to legal and ethical standards, lead security initiatives, and adapt to evolving threats through continuous learning.

These learning outcomes aim to prepare students for careers in cybersecurity and provide them with the knowledge and skills needed to protect organizations and individuals from cyber threats, manage security effectively, and contribute to the advancement of the field.

3. Eligibility Criteria

- Candidates should have bachelor's degree in Science and Engineering disciplines with minimum two years of relevant industry experience.
- Minimum eligibility criterion (in terms of marks/GCPA), shortlisting and selection process will be as per Blended-mode MTech regulations.

4. Mode of Teaching

Component	Details
Live Classes	All lecture and lab courses are conducted through live interactive sessions (approx. 40 contact hours per 3-credit course)
Recorded Content	Recordings of live sessions are provided for revision and flexible learning
Project Work	Conducted through guided supervision meetings (live) with faculty
Lab Sessions	Hands-on sessions (live) with possible recorded demonstrations

5. Course Structure

	Subject Name	Subject Code	L-T-P	Credit	Contact Hours
Semester I	Networks and Systems Security	To be issued	2-0-2	3	3
	Advanced Algorithms	CS6L007	3-0-0	3	3
	Blockchain and Access Control	CS6L077	3-0-0	3	3
	Elective 1	-	3-0-0	3	3
	Elective 2	-	3-0-0	3	3
Semester II	Cryptography	CS6L005	3-0-0	3	3

	Advanced computer networks	CS6L048	3-0-0	3	3
	Advanced Algorithms Lab	CS6P010	0-0-3	2	3
	Elective 3	-	3-0-0	3	3
	Elective 4	-	3-0-0	3	3
	Thesis Part-1	CS6D008		2	
Semester III	Elective 5	-	3-0-0	3	3
	Thesis Part-2	CS6D009		14	
Semester IV	Thesis Part-3	CS6D010		14	
	Elective 6	-	3-0-0	3	3
Total Credit					65

List of Electives:

Subject Code	Subject Name	L-T-P-C	Hours
CS6L040	Machine Learning and Cyber Security	3-0-0-3	3
CS6L070	Cyber-Physical Systems	3-0-0-3	3
CS6L030	Data Intensive Computations	3-0-0-3	3
CS6L004	Machine Learning	3-0-0-3	3
CS6L047	Advanced Computer Architecture	3-0-0-3	3
CS6L045	Computer Vision	3-0-0-3	3
CS6L026	Wireless Sensor Networks	3-0-0-3	3
CS6L006	Fault Tolerant Systems	3-0-0-3	3
CS6L019	Artificial Intelligence	3-0-0-3	3
CS6L031	Game Theory	3-0-0-3	3
CS6L088	Ethical and Responsible Artificial Intelligence	3-0-0-3	3

CS6L024	Internet-of-Things	3-0-0-3	3
CS6L008	Cloud Computing	3-0-0-3	3
CS6L034	Software Engineering	3-0-0-3	3

6. Name of the Interested Faculties.

For Core Courses:

Subject Code	Subject Name	Faculty Name
CS6L002	Networks and Systems Security	Dr. Padmalochan Bera & Dr. Sumana Maiti
CS6L048	Advanced Computer Networks	Dr. Pragati Shrivastava & Dr. Sudipta Saha
CS6L007	Advanced Algorithms	Dr. Manas Jyothi Kashyap & Dr. Joy Chandra Mukherjee
CS6L005	Cryptography	Dr. Padmalochan Bera & Dr. Sumana Maiti
CS6L077	Blockchain and Access Control	Dr. Padmalochan Bera & Dr. Milan Patnaik (Whizhack Instructor)
CS6P010	Advanced Algorithms Lab	Dr. Manas Jyothi Kashyap & Dr. Joy Chandra Mukherjee

For Program Electives:

Subject Code	Subject Name	Faculty Name
CS6L040	Machine Learning and Cyber Security	Dr. Ram Prasad Padhy & Dr. Padmalochan Bera
CS6L070	Cyber-Physical Systems	Dr. Pragati Shrivastava & Prof. Manoranjan Satpathy
CS6L030	Data Intensive Computations	Dr. Padmalochan Bera & Dr. Devashree Tripathy
CS6L004	Machine Learning	Dr. Ram Prasad Padhy & Dr. Shreya Ghosh

CS6L047	Advanced Computer Architecture	Dr. Debiprasanna Sahoo & Dr. Devashree Tripathy
CS6L045	Computer Vision	Dr. Debi Prosad Dogra & Dr. Ram Prasad Padhy
CS6L026	Wireless Sensor Networks	Dr. Pragati Shrivastava & Sudipta Saha
CS6L006	Fault Tolerant Systems	Dr. Joy Chandra Mukherjee & Prof. Manoranjan Satpathy
CS6L019	Artificial Intelligence	Dr. Shreya Ghosh & Dr. Abhik Jana
CS6L031	Game Theory	Prof. Manoranjan Satpathy & Dr. Padmalochan Bera
CS6L088	Ethical and Responsible Artificial Intelligence	Dr. Shreya Ghosh & Dr. Debi Prosad Dogra
CS6L024	Internet-of-Things	Dr. Sudipta Saha & Dr. Pragati Shrivastava
CS6L008	Cloud Computing	Dr. Debiprasanna Sahoo and Dr. Padmalochan Bera
CS6L034	Software Engineering	Dr. Srinivas Pinisetty & Prof. Manoranjan Satpathy

7. Modified/newly added courses.

New Course Added: Networks and Systems Security (Core Course)

Subject Code: CS6L002	**Subject Name:** Networks and Systems Security	**L-T-P-C:** 2-0-2-3
Pre-requisite(s): None		
Learning Outcome(s): ● Analyze the security properties and vulnerabilities of Internet applications, network architectures, and protocols used in modern communication systems. ● Identify and evaluate common network and system attacks, including intrusion, malware, and denial-of-service attacks, and assess their impact on confidentiality, integrity, and availability. ● Explain and assess access control mechanisms and firewall technologies for enforcing security policies in networked systems.		

- Apply cryptographic principles to analyze the security of symmetric and public-key encryption schemes and key exchange protocols.

- **Module 1: Fundamental concepts:** Network applications – HTTP, FTP, Telnet, SMTP, DNS, web caching, proxies, client-server and peer-to-peer (P2P) architectures, chord protocol, and BitTorrent; review of data link and network layer protocols, basics of Internet Security – CIA principle, intrusions, vulnerability, risks, and controls
- **Module 2: Network and System Intrusions:** IP spoofing, Sniffing – passive vs active, sniffing tools, session hijacking, different types of DoS attacks with examples, DDoS attacks, ARP Poisoning, malware, virus, attack signatures and examples of advanced attacks
- **Module 3: Firewall and Access Control:** different types of access control – MAC, RBAC; ACLs, packet filter, and stateful firewall, working principle of stateful firewall, application, and circuit gateways
- **Module 4: Introduction to Cryptography:** CIA, perfect secrecy, one-time-pad, symmetric key cryptography – stream ciphers- LFSR, RC4; block ciphers - DES, 2DES, 3DES, AES; differential analysis and linear analysis; security analysis of symmetric key cryptography
- **Module 5: Public Key Cryptography:** one-way function, Markle-Hellman crypto, RSA, Elgamal, Diffie-Hellman; Elliptic Curve; Analysis of public key cryptography
- **Module 6: IP Security and Intrusion Detection System:** IPSec – Authentication, Encryption, AH, ESP; VPN using IPSec; Signature-based and Anomaly-based IDS; Host-based and Network-based IDS; Advanced IDS using AI techniques.
- **Laboratory:** Network and Transport layer protocol simulation (IP, TCP, RIP, OSPF, BGP), network device configuration and performance analysis (routers, switches, firewalls), network management and access control policies, network programming and secure communications. Cryptographic hashing, digital signatures, password cracking techniques, Man-in-the-Middle (MITM) attacks. IP spoofing, packet sniffing and traffic analysis (Wireshark, TCPDump), ARP poisoning, SYN flooding attacks, Smurf attacks, Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks, botnets, network-based malware detection. Stateful firewalls, network intrusion detection systems (signature-based and anomaly-based), honeypots. Peer-to-peer (P2P) networking, BitTorrent file sharing, torrent-based attacks, network forensics tools (Wireshark, TCPDump, Sleuthkit).

Text Books:

1. W. Stallings. Network Security Essentials, Prentice Hall
2. Saadat Malik. Network Security Principles and Practices, Pearson Education
3. Forouzan and Mukhopadhyay: Cryptography and Network Security

Reference Books:

1. R. Anderson. Security Engineering, 2nd edition, 2008.

8. Course Fee Structure

S.No	Tuition Fee Component	Rs.	Remarks
Part-A			
1.	Registration Fee (one-time)	25,000/-	One time (valid for 5 years). After 5 years, Rs. 5,000/- per semester
Part-B			
1.	Tuition fee for lecture/lab course	1,000/- per hour	40 hours for 3 credit course, 52 hours for 4 credit course
2.	Tuition fee for project work	30,000/-	For every 4 credits

Fee Component	Amount (INR)
Registration fee (One-time)	25,000
Tuition fee for lecture/lab course	4,50,000
Tuition fee for project work	2,25,000
Total	**INR 7,00,000**

8. Feedback from industry & academia on program & courses