GANGA INSTITUTE OF TECHNOLOGY AND MANAGEMENT, KABLANA (JHAJJAR)

An Autonomous Institute

'A' GRADE ACCREDITED BY NAAC

Evaluation Scheme and Syllabus For

Master of Technology (Cyber Forensics and Information Security)

Effective from the Session: 2025-26

APPROVED BY AICTE, NEW DELHI AND AFFILIATED TO MDU, ROHTAK

1. DEFINITION OF CREDIT

1	1 Lecture (L) per week	1 Credit
2	2 Practical (P) per week	1 Credit
3	2 Seminar per Week	2 Credit
4	4 Project Per Week	2 Credit

2. RANGE OF CREDIT

A credit of 86 is required for a student to be eligible for a postgraduate degree in Cyber Forensics and Information Security.

3. STRUCTURE OF POSTGRADUATE ENGINEERING PROGRAM (M.TECH)

Sr. No.	**Category**	**Breakup of Credits**
1	Professional Core Courses	32
2	Professional Elective Courses (Relevant to chosen specialization/branch)	8
3	Mandatory Learning Course	3
4	Multidisciplinary Open Elective Courses	6
5	Foundation Elective Courses	3
6	Seminar	6
7	Lab Courses	4
8	Project	2
9	Dissertation	22
	Total Credits	**86**

4. COURSE CODE AND DEFINITIONS

Sr. No.	**Category**	**Course Code**
1	Professional Core Courses	PCC
2	Professional Elective Courses (Relevant to chosen specialization/branch)	PEC
3	Mandatory Learning Course	MLC
4	Multidisciplinary Open Elective Courses	OEC
5	Foundation Elective Courses	FEC
6	Seminar	SM
7	Lab Courses	LC
8	Project	PROJ
9	Dissertation	DISS

GANGA INSTITUTE OF TECHNOLOGY AND MANAGEMENT, KABLANA, JHAJJAR (HR.)

Scheme of Studies and Examination

M.Tech (Cyber Forensics and Information Security) – 3rd Semester

w.e.f. 2025-26

Sr. No.	Category	Course Code	Course Title	Hours per week			Total Load Per Week	Credits	Examination Scheme (Marks)				Exam Duration in H
				Lecture (L)	Tutorial (T)	Practical (P)			Assessment	End Semester Examination		Total	
										Theory	Practical		
1	Professional Core Courses	PCC-MTCFIS-201A	Preserving & Recovering Digital Evidence	4	0	0	4	4	40	60		100	3
2	Professional Elective Courses	Refer Table -IV	....	4	0	0	4	4	40	60		100	3
3	Multidisciplinary Open Elective Courses	Refer Table -V	....	3	0	0	3	3	40	60		100	3
4	Mandatory Learning Courses	MLC-01A	Research Methodology and IPR	3	0	0	3	3	40	60		100	3
5	Project Courses	PROJ-MTCFIS-213A	Project	0	0	4	4	2	50		50	100	3
6	Seminar	SM-MT-215A	Seminar-III	0	0	2	2	2	50			50	
7	Dissertation	DISS-MTCFIS-217A	Dissertation (Phase-1)	0	0	4	4	2	100			100	3
							Total Credits	**20**				**650**	

Table IV: Professional Elective Courses

Sr. No.	Course Code	Course Name
1	PEC- MTCFIS-203A	Security in 5G Technologies
2	PEC- MTCFIS-205A	Social Media Security
3	PEC- MTCFIS-207A	Wireless Security
4	PEC- MTCFIS-209A	Internet of Things and Security
5	PEC- MTCFIS-211A	Professional ethics and cyber security

GANGA INSTITUTE OF TECHNOLOGY AND MANAGEMENT, KABLANA, JHAJJAR (HR.)

Scheme of Studies and Examination

M.Tech (Cyber Forensics and Information Security) –4th Semester

w.e.f. 2025-26

Sr. No.	Category	Course Code	Course Title	Hours per week			Total Load Per Week	Credits	Examination Scheme (Marks)				Exam Duration in H
				Lecture (L)	Tutorial (T)	Practical (P)			Assessment	End Semester Examination		Total	
										Theory	Practical		
1	Dissertation	DISS-MTCFIS-202A	Dissertation and viva (Phase-2)	-	-	20	20	20	250		500	750	
Total Credits								**20**				**750**	

<table>
<tr><td>Course Code</td><td colspan="5"><b>PCC-MTCFIS-201A</b></td></tr>
<tr><td>Category</td><td colspan="5">Professional Core Courses</td></tr>
<tr><td>Course Title</td><td colspan="5"><b>Preserving and Recovering Digital Evidence</b></td></tr>
<tr><td rowspan="2">Scheme and Credits</td><td>L</td><td>T</td><td>P</td><td><b>Credits</b></td><td rowspan="2"><b>Semester-III</b></td></tr>
<tr><td>4</td><td>0</td><td>0</td><td><b>4</b></td></tr>
<tr><td>Course Objectives</td><td colspan="5">The objectives of this course are
• To understand digital evidence, computer crime, and investigation procedures.
• To learn forensic methods for computers and handheld devices.
• To explore network forensics and evidence collection across network layers.
• To investigate cybercrimes and follow digital evidence handling guidelines</td></tr>
<tr><td>Assessment</td><td colspan="5">40 Marks</td></tr>
<tr><td>End Semester Examination</td><td colspan="5">60 Marks</td></tr>
<tr><td>Total Marks</td><td colspan="5">100</td></tr>
<tr><td>Duration of Exam</td><td colspan="5">03 Hours</td></tr>
</table>

Course Outcomes: After studying this course, the students will be able to

COs	Skill Demonstrated	RBT Level
CO1	Define key concepts related to digital evidence, computer crime history, and the digital investigation process.	Level 1: Remember
CO2	Describe the role of forensic science in examining various computer systems and explain the structure of digital evidence across different operating environments.	Level 2: Understand
CO3	Apply appropriate forensic techniques and tools to investigate digital crimes involving computers, mobile devices, and networks.	Level 3: Apply
CO4	Analyze digital crime scenarios by reconstructing incidents, evaluating modus operandi and motives, and interpreting digital evidence for legal proceedings.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Digital Investigation: Digital evidence and computer crime – history and terminals of computer crime investigation – technology and law - the investigate process – investigate reconstruction-modus operandi, motive and technology –digital evidence in the court room.

Unit-II

Computer basics for digital investigators: Applying forensic science to computers-forensic examination of Windows systems – forensic examination of Unix systems - forensic examination of Macintosh systems - forensic examination of handheld devices.

Unit-III

Networks: Networks basics for digital investigators – applying forensic science to networks-digital evidence on physical and data link layers - digital evidence on network and transport layers-digital evidence on the internet.

Unit-IV

Investigating Computer Crime: Investigating computer intrusions – investigating cyber stalking- digital evidence as alibi. Guidelines: Handling the digital crime scene – digital evidence examination guidelines.

Suggested Readings:

1. Eoghan Casey, Digital Evidence and Computer Crime Forensic science, Computers and Internet, Elsevier Academic Press –Second Edition, 2011.
2. Jack Wiles, Anthony Reyes, Jesse Varsalone The Best Damn Cybercrime and Digital Forensics Book Perio, Syngress Publishing, 2007.
3. Casey, Eoghan. Computer Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Cambridge: Cambridge University Press, 2000.
4. Vacca, John R. Computer Forensics Computer Crime Scene Investigation, Massachusetts: Charles River Media, 2002.

Useful Video links

Unit No.	Topics	Links
Unit-I	Handling, Collection and preservation of Digital evidence	https://www.youtube.com/watch?v=YglyYgmAeCw
	Digital Evidence-identification, etc in Court |	https://www.youtube.com/watch?v=SzxVK1zR_II
	Digital Investigation Procedure	https://www.youtube.com/watch?v=ZTZ_GnFR-GE
	Modus Operandi	https://www.youtube.com/watch?v=ZxmlTJ7WWLk
Unit-II	How to secure a Windows computer(forensic examination of windows systems)	https://www.youtube.com/watch?v=cENIGQdCvUk&list=PLJu2iQtpGvv-2LtysuTTka7dHt9GKUbxD&index=6
	Investigating Unix Systems in Digital Forensics	https://www.youtube.com/watch?v=eR4ROLnk5Sc
	Digital Investigations. Computer Forensics for Windows and Mac	https://www.youtube.com/watch?v=BW8pCe0wXtY
	Forensics of Hand-Held Devices	https://www.youtube.com/watch?v=j62svCbNf9I
Unit-III	Network Forensics	https://www.youtube.com/watch?v=OufDs4sI5P4
	Forensics - Basics of Networking	https://www.youtube.com/watch?v=DDHrTcMOGsE
	Cyber Forensics and Digital Evidence	https://www.youtube.com/watch?v=Qod9yrq0Ho0
Unit-IV	Computer Crime Investigations	https://www.youtube.com/watch?v=8uBU9n206b0
	Digital evidence	https://www.youtube.com/watch?v=taladDGFgKM
	Digital crime scene investigation	https://www.youtube.com/watch?v=NPgPE7WbJd4&t=179s

<table>
<tr><td>Course Code</td><td colspan="5"><b>PEC- MTCFIS-203A</b></td></tr>
<tr><td>Category</td><td colspan="5">Professional Elective Courses</td></tr>
<tr><td>Course Title</td><td colspan="5"><b>Security in 5G Technologies</b></td></tr>
<tr><td rowspan="2">Scheme and Credits</td><td>L</td><td>T</td><td>P</td><td><b>Credits</b></td><td rowspan="2"><b>Semester-III</b></td></tr>
<tr><td>4</td><td>0</td><td>0</td><td><b>4</b></td></tr>
<tr><td>Course Objectives</td><td colspan="5">The objectives of this course are
• To explain the evolution of cellular systems and 5G requirements.
• To enable students to apply security principles to 5G networks and assess privacy risks.
• To make student proficient in cryptographic techniques and security measures for 5G networks.
• To enable students to investigate security challenges in cloud and MEC environments for 5G.</td></tr>
<tr><td>Assessment</td><td colspan="5">40 Marks</td></tr>
<tr><td>End Semester Examination</td><td colspan="5">60 Marks</td></tr>
<tr><td>Total Marks</td><td colspan="5">100</td></tr>
<tr><td>Duration of Exam</td><td colspan="5">03 Hours</td></tr>
</table>

Course Outcomes: After studying this course, the students will be able to

COs	**Skill Demonstrated**	**RBT Level**
CO1	Define the evolution of cellular systems from 1G to 5G, understanding the features and requirements of each generation.	Level 1: Remember
CO2	Explain the enabling technologies of 5G and their role in meeting the requirements of next-generation mobile networks.	Level 2: Understand
CO3	Apply design principles for securing 5G networks, including strategies for physical layer security and IoT device protection.	Level 3: Apply
CO4	Analyze cyber security business models in 5G and assess the impact of security measures on user privacy, identity, and trust.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Evolution of Cellular Systems: Introduction, First Generation Cellular Systems, Second- Generation Cellular Systems, Third Generation Cellular Systems, Cellular Systems beyond 3G, Fourth Generation Cellular Systems, 5G Mobile Networks: Requirements, Enabling Technologies and Research Activities.

Unit-II

Design Principles for 5G Security: Cyber Security Business Models in 5G, Physical Layer Security, 5G WLAN Security, Safety of 5G Network Physical Infrastructures.

Software Defined Security Monitoring in 5G Networks: 5G Device and User Security, IoT Security, User Privacy, Identity and Trust in 5G.

5G Positioning: Security and Privacy Aspects, Outdoor Versus Indoor Positioning Technologies, Passive versus Active Positioning, Brief Overview of 5G Positioning Mechanisms.

Unit-III

Cryptographic Techniques for Security and Privacy of Positioning: Legislation on User Location Privacy in 5G. 5G Cloud and Virtual Network Security: Mobile Virtual Network Operators (MVNO) Security, NFV and NFV based Security Services.

Unit-IV

Cloud and MEC Security: Cloud Computing in 5G Networks, MEC in 5G Networks, Security Challenges in 5G Cloud, Security Challenges in 5G MEC. Security Architectures for 5G Cloud and MEC Regulatory Impact on 5G Security and Privacy: Regulatory Objectives for Security and Privacy. Legal Framework for Security and Privacy, Security and Privacy Issues in 5G Technologies

Suggested Readings

1. A Comprehensive Guide to 5G Security by Madhusanka Livanage ljaz Ahmad, Ahmed Bux Abro ,Andrei Gurtov, Mika Ylianttila.

Useful Video links

Unit No.	Topics	Links
Unit-I	Cellular Systems	https://www.youtube.com/watch?v=f2wlHL1Sok8
	5G Mobile Networks	https://www.youtube.com/watch?v=SbYltPawklg&list=PLFW6lRTa1g81SMpel8aIFBubvO0h1UOJV
Unit-II	Security Monitoring in 5G Networks,Security and Privacy Aspects	https://www.youtube.com/watch?v=6TGU9yy96Vk
	IoT Security	https://www.youtube.com/watch?v=o5ZsXCVZiiw
Unit-III	Mobile Virtual Network Operators (MVNO) Security	https://www.youtube.com/watch?v=a57B-9cSXZ4
	Cryptographic Techniques for Security	https://www.youtube.com/watch?v=Q-HugPvA7GQ&list=PL71FE85723FD414D7
Unit-IV	Security Challenges in 5G Cloud	https://www.youtube.com/watch?v=qCnPoZuo6oQ
	MEC in 5G Networks	https://www.youtube.com/watch?v=yoRUC0sFbJo

<table>
<tr><td>Course Code</td><td colspan="5"><b>PEC- MTCFIS-205A</b></td></tr>
<tr><td>Category</td><td colspan="5">Professional Elective Courses</td></tr>
<tr><td>Course Title</td><td colspan="5"><b>Social Media Security</b></td></tr>
<tr><td rowspan="2">Scheme and Credits</td><td>L</td><td>T</td><td>P</td><td><b>Credits</b></td><td rowspan="2"><b>Semester-III</b></td></tr>
<tr><td>4</td><td>0</td><td>0</td><td><b>4</b></td></tr>
<tr><td>Course Objectives</td><td colspan="5">The objectives of this course are
• To introduce the fundamental concepts, types, and significance of social media in modern communication.
• To create awareness about the ethical, privacy, and security challenges associated with social media use.
• To explore real-world social media practices to understand effective and ineffective campaign strategies.
• To highlight the long-term risks of digital presence, data sharing, and the importance of responsible online behavior.</td></tr>
<tr><td>Assessment</td><td colspan="5">40 Marks</td></tr>
<tr><td>End Semester Examination</td><td colspan="5">60 Marks</td></tr>
<tr><td>Total Marks</td><td colspan="5">100</td></tr>
<tr><td>Duration of Exam</td><td colspan="5">03 Hours</td></tr>
</table>

Course Outcomes: After studying this course, the students will be able to

COs	**Skill Demonstrated**	**RBT Level**
CO1	Identify key concepts, types, and issues related to social media, including its classifications, value, and potential problems.	Level 1: Remember
CO2	Explain the risks and ethical concerns of social media, including cybercrime, privacy issues, and the implications of content sharing and user behavior.	Level 2: Understand
CO3	Apply knowledge of social media strategies to evaluate good and bad campaigns and suggest improvements in content management and promotion.	Level 3: Apply
CO4	Analyze the security, privacy, and data-related risks associated with social media use, identifying potential vulnerabilities and their consequences.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Introduction to Social Media: Understanding Social Media, Different Types and Classifications, The Value of Social Media, Cutting Edge Versus Bleeding Edge, The Problems That Come With Social Media, Is Security Really an Issue? Taking the Good with the Bad.

Unit-II

Dark side: Cybercrime, Social Engineering, Hacked accounts, cyber stalking, cyber bullying, predators, phishing, hackers Policies and Privacy Blocking users controlling gap privacy, Location awareness, Security Fake accounts passwords, privacy and information sharing.

Unit-III

Being bold versus being overlooked: Good social media campaigns, Bad social media campaigns, Sometimes it’s better to be overlooked, Social media hoaxes, human factor, Content management, Promotion of social media.

Unit-IV

Risks of Social media: Introduction Public embarrassment, Once it’s out there, it’s out there False information, Information leakage, Retention and archiving, Loss of data and equipment Policies and Privacy Blocking users controlling app privacy, Location awareness, Security Fake accounts passwords, privacy and information sharing.

Suggested Readings

1. Inter disciplinary Impact Analysis of Privacy in Social Networks, Recognizing Your Digital Friends, Encryption for Peer-to-Peer Social Networks Crowd sourcing and Ethics , Authors: Altshuler Y, Elovici Y, Cremers A.B, Aharony N, Pentland A. (Eds.).
2. Social media security, https://www.sciencedirect.com/science/article/pii/B9781597499860000.
3. Social media security by Michael Cross, Syngress.

Useful Video links

Unit No.	Topics	Links
Unit-I	Introduction to Social Media	https://youtu.be/5Puxly9TnLk
	Privacy and Security in Online Social Media	https://youtu.be/wQYqsgNThKM
Unit-II	Dark sides of social media, Cyber security and Privacy	https://youtu.be/kZtw4L6LZS8?list=PLyqSpQzTE6M-jkJEzbS5oHJUp2GWPsq6e
	Privacy and Security in Online Social Media	https://youtu.be/AQClJAif5w8
Unit-III	Best Social Media Marketing Campaigns Ever	http3s://youtu.be/QKtf2IeR5rE
	Social media hoaxes	https://youtu.be/Ll5V4mFIXBE
Unit-IV	Risk Management	https://youtu.be/v7KtPLhSMkU?list=PLyqSpQzTE6M-jkJEzbS5oHJUp2GWPsq6e
	Privacy: Strategy and safety	https://youtu.be/All1JR-Avjw?list=PLyqSpQzTE6M-jkJEzbS5oHJUp2GWPsq6e

<table>
<tr><td>Course Code</td><td colspan="5"><b>PEC- MTCFIS-207A</b></td></tr>
<tr><td>Category</td><td colspan="5">Professional Elective Courses</td></tr>
<tr><td>Course Title</td><td colspan="5"><b>Wireless Security</b></td></tr>
<tr><td rowspan="2">Scheme and Credits</td><td>L</td><td>T</td><td>P</td><td><b>Credits</b></td><td rowspan="2"><b>Semester-III</b></td></tr>
<tr><td>4</td><td>0</td><td>0</td><td><b>4</b></td></tr>
<tr><td>Course Objectives</td><td colspan="5">The objectives of this course are
• To introduce the fundamentals of wireless communication and information warfare.
• To understand security protocols and threats in WLAN and mobile networks.
• To explore security challenges and solutions in ad hoc wireless networks.
• To study RFID system vulnerabilities and lightweight cryptographic techniques.</td></tr>
<tr><td>Assessment</td><td colspan="5">40 Marks</td></tr>
<tr><td>End Semester Examination</td><td colspan="5">60 Marks</td></tr>
<tr><td>Total Marks</td><td colspan="5">100</td></tr>
<tr><td>Duration of Exam</td><td colspan="5">03 Hours</td></tr>
</table>

Course Outcomes: After studying this course, the students will be able to

COs	**Skill Demonstrated**	**RBT Level**
CO1	Recall fundamental concepts of wireless communication, information warfare, and wireless network taxonomies	Level1: Remember
CO2	Explain security threats and standards in WLAN, cellular, and VoIP systems, including the roles of WAP, WTLS, and Bluetooth.	Level2:Understand
CO3	Apply routing protocols and security mechanisms to detect and mitigate attacks in ad hoc networks.	Level 3: Apply
CO4	Analyze vulnerabilities in RFID systems and evaluate lightweight cryptographic solutions for low-cost tags	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Communication Networks: Information Theory-Decision Theory-A Model for cost effective risk management-Performance measures. Uniqueness of Wireless-Wireless Information Warfare – Taxonomies of wireless.

Unit-II

Security in WLAN: Wireless Transmission Media, WLAN Products and standards- securing WLAN-counter measures-WAP-WTLS-Bluetooth-VoIP. Security in cellular Networks Threats, Hacking and Viruses in mobile communications- Access control and Authentication in mobile communications.

Unit-III

Security in Ad hoc Networks: Ad hoc Networking- Major Routing Protocol in Ad hoc Networks- Attacks against Ad Hoc Networks, Securing Ad hoc Networks- Authentication in Ad hoc Networks–key Management – Intrusion Detection in Ad hoc Networks.

Unit-IV

Security in RFID: Multi tag RFID systems-Attacking RFID systems- RFID Relay attacks- Physical privacy and security in RFID systems- Authentication Protocol in RFID systems- Lightweight Cryptography for Low-Cost RFID tags.

Suggested Readings:

1. Nichols, Randall K.; Lekkas, Panos, "Wireless Security : Models, Threats, And Solutions", Tata McGraw Hill Education, 2006.
2. Yan Zhang and Paris Kitsos, "Security in RFID and Sensor Networks", CRCPRESS, 2009.
3. Noureddine Boudriga, "Security of Mobile Communications", ISBN 9780849379413, 2010.

Useful Video links

Unit No.	Topics	Links
Unit-I	Wireless Communication Network	https://www.youtube.com/watch?v=Eu_mTZxPofI&list=PL1A4AFAC7AC1909C9&index=37
	Risk management	https://www.youtube.com/watch?v=zo_dLUoyqjc
Unit-II	Security in WLAN	https://www.youtube.com/watch?v=0mOrIOtw2_c
	VoIP	https://www.youtube.com/watch?v=zZoE7MQ8qO0
	Authentication in mobile communications	https://www.youtube.com/watch?v=VfFAYtmCaCY
Unit-III	Adhoc Networking	https://www.youtube.com/watch?v=ycaz99NogS4&list=PLJ5C_6qdAvBHroAfekCO7K4xphEF74UPc
	Routing Protocol in Adhoc Networks	https://www.youtube.com/watch?v=OaUE4otTsuc&list=PLJ5C_6qdAvBHroAfekCO7K4xphEF74UPc&index=29
	Intrusion Detection in Ad hoc Networks	https://www.youtube.com/watch?v=2YGUvopGkQc
Unit-IV	Security in RFID	https://www.youtube.com/watch?v=ssY2CpC0JAQ
	Light weight Cryptography	https://www.youtube.com/watch?v=8rtkOk-MUVc

<table>
<tr><td>Course Code</td><td colspan="5"><b>PEC- MTCFIS-209A</b></td></tr>
<tr><td>Category</td><td colspan="5">Professional Elective Courses</td></tr>
<tr><td>Course Title</td><td colspan="5"><b>Internet of Things and Security</b></td></tr>
<tr><td rowspan="2">Scheme and Credits</td><td>L</td><td>T</td><td>P</td><td><b>Credits</b></td><td rowspan="2"><b>Semester-III</b></td></tr>
<tr><td>4</td><td>0</td><td>0</td><td><b>4</b></td></tr>
<tr><td>Course Objectives</td><td colspan="5">The objectives of this course are
• To introduce the fundamental concepts, technologies, and communication protocols of IoT.
• To explore embedded device prototyping using platforms like Arduino and Raspberry Pi.
• To develop skills in building physical and online IoT components using digital fabrication and APIs.</td></tr>
<tr><td>Assessment</td><td colspan="5">40 Marks</td></tr>
<tr><td>End Semester Examination</td><td colspan="5">60 Marks</td></tr>
<tr><td>Total Marks</td><td colspan="5">100</td></tr>
<tr><td>Duration of Exam</td><td colspan="5">03 Hours</td></tr>
</table>

Course Outcomes: After studying this course, the students will be able to

COs	Skill Demonstrated	RBT Level
CO1	**Describe** the fundamental concepts, technologies, protocols, and design principles involved in the Internet of Things (IoT).	Level1:Remember
CO2	**Explain** the components, platforms, and prototyping tools used in the development of embedded and connected devices.	Level2:Understand
CO3	**Develop** basic IoT prototypes using physical components and APIs, including digital fabrication techniques such as 3D printing and laser cutting.	Level 3: Apply
CO4	**Analyze** the transformation of IoT prototypes into scalable business models, considering ethical, environmental, and privacy challenges.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Fundamentals of IoT: The flavour of the Internet, Technology of IoT, Enchanted objects, Design principles for connected device, Privacy, Web thinking, Affordance.

Internet Principles: Internet Communications, IP, TCP, Protocol suite, UDP, IP Addresses, TCP and UDP ports, MAC Address – Application Layer Protocols.

Unit-II

Prototyping Embedded Devices: Prototypes and production, Open source versus closed source, Tapping into the community, Electronics Embedded computing basics, Arduino, Raspberry pi, electric imp, plug computing.

Unit-III

Prototyping Physical and Online Components: Preparation, sketch, iterate and explore, Non digital methods, Laser cutting, 3D printing Getting started with API, Writing a new API, Real time reactions, Memory Management.

Unit-IV

Prototype to Business Models: Business model canvas–Models, Funding an internet of things start-up, Scaling up Software, Ethics: Privacy, Control, Environment, Solutions.

Suggested Readings

1. Adrian McEwen, akim Cassimally, Designing the Internet of Things, 1/e, Wiley publication, 2013
2. Charalampos Doukas , Building Internet of Things with the Arduino, Create space, 2002.
3. Dieter Uckelmann(et.al), Architecting the Internet of Things, Springer, 2011

Useful Video links

Unit No.	Topics	Links
Unit-I	Fundamentals of IoT	https://www.youtube.com/watch?v=WUYAjxnwjU4&list=PLE7VH8RC_N3bpVne8QzOAHziEgmjQ2qE
	Internet Communications – IP, TCP	https://www.youtube.com/watch?v=nyUZn93Lro&list=PLE7VH8RC_N3bpVne8QzOAHziEgmjQ2qE&index=7
Unit-II	Open source versus closed source	https://www.youtube.com/watch?v=QQXcUODEKw
	Embedded computing basics	https://www.youtube.com/watch?v=y9RAhEfLfJs&list=PL90187D2B8F5AC28F
Unit-III	Laser cutting - 3D printing	https://www.youtube.com/watch?v=sFFcPPj4Ti8
	Getting started with API	https://www.youtube.com/watch?v=cRV4HQ39S2s
Unit-IV	Business model canvas–Models	https://www.youtube.com/watch?v=z6-Ly8Bl4Hc
	Ethics: Privacy – Control	https://www.youtube.com/watch?v=amGreeiv77M

<table>
<tr><td>Course Code</td><td colspan="5"><b>PEC- MTCFIS-211A</b></td></tr>
<tr><td>Category</td><td colspan="5">Professional Elective Courses</td></tr>
<tr><td>Course Title</td><td colspan="5"><b>Professional Ethics and Cyber Security</b></td></tr>
<tr><td rowspan="2">Scheme and Credits</td><td>L</td><td>T</td><td>P</td><td><b>Credits</b></td><td rowspan="2"><b>Semester-III</b></td></tr>
<tr><td>4</td><td>0</td><td>0</td><td><b>4</b></td></tr>
<tr><td>Course Objectives</td><td colspan="5">The objectives of this course are
• To introduce fundamental concepts of computer ethics, professional conduct, and privacy issues in computing.
• To provide understanding of intellectual property rights and ethical decision-making in cyberspace.
• To equip students with knowledge of cybercrime handling procedures and relevant legal frameworks
• To develop skills in cyber forensics, security policies, and understanding industry-standard information security certifications.</td></tr>
<tr><td>Assessment</td><td colspan="5">40 Marks</td></tr>
<tr><td>End Semester Examination</td><td colspan="5">60 Marks</td></tr>
<tr><td>Total Marks</td><td colspan="5">100</td></tr>
<tr><td>Duration of Exam</td><td colspan="5">03 Hours</td></tr>
</table>

Course Outcomes: After studying this course, the students will be able to

COs	**Skill Demonstrated**	**RBT Level**
CO1	Recall basic concepts of computer ethics, privacy, and professional codes of conduct relevant to computing and information technology.	Level1: Remember
CO2	Explain intellectual property rights, privacy laws, and ethical theories in the context of cyber technologies and professional responsibilities	Level2:Understand
CO3	Apply ethical frameworks and legal principles to resolve dilemmas related to cybercrime, intellectual property, and professional conduct.	Level 3: Apply
CO4	Analyze real-world case studies and cyber forensic scenarios to assess ethical decisions, incident responses, and information security policies.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Computer ethics and philosophical ethics: Vacuum of policies, conceptual muddles, social context, moral and legal issues, uniqueness of ethical issues, role of analogy, descriptive and normative claims, ethical relativism, utilitarianism, other theories. Professional Ethics: Characteristics, the system of professions, computing as a profession, professional relationships, responsibilities, code of ethics and professional conduct. Privacy: Computers and privacy issue, reframing this issue, legislative background, better privacy protection.

Unit-II

Intellectual property issues in cyberspace: Introduction to intellectual property Protections via Copyright, Trade Secrets, Trademarks, Patents, Contracting to protect intellectual property, Protection options –Encryption, copyright on web-content, copyright on software. Ethical Decision Making: Types of ethical choices, Making defensible decisions, Ethical dilemmas, law and ethics, Guidelines for dilemma (Informal and Formal), Four-step analysis process of solving dilemma Case studies: i) A stolen password ii) Recovery of data leads to Discovery of confidential files iii) Do copyright ethics change overseas?

Unit-III

Crime incident Handling Basics: Hacking, cyber activism, Tracking hackers, clues to cybercrime, privacy act, search warrants, common terms, organizational roles, procedure for responding to incidents, reporting procedures, legal considerations, Information Technology Act 2000:Scope, jurisdiction, offense and contraventions, powers of police, adjudication.

Unit-IV

Cyber Forensics: Cyber forensics, cybercrime examples, forensics casework, investigative incident response actions, computer forensics tools, Threats in cyberspaces, Blended attacks Sample Policy Documents: Antivirus Guidelines Policy, Internal Lab Security Policy, Server Security Policy, Wireless Communications Policy. Information Security Certifications, CISS Pand SSCP, CISA and CISM, SCP, GIAC, certification weaknesses, Role of these certified professionals, Windows Server 2003 Security Fundamentals.

Suggested Readings:

1. Deborah G. Johnson, “ ComputerEthics”,4thEdition,PearsonEducationPublication, 2008.
2. EarnestA.Kallman,J.P. Grillo,“EthicalDecisionmakingandIT:AnIntroductionwithCases”,McGraw Hill Publication, 2008.
3. John W. Ritting house, William M. Hancock, “Cyber security Operations Handbook”, ElsevierPub., 2003.
4. MichaelE.Whitman,HerbertJ.Mattord,“PrinciplesofInformationSecurity”,2ndEdition, Cengage Learning Pub., 2012.
5. Randy Weaver, Dawn Weaver, “Network Infrastructure Security”, Cengage Learning Hub.,2006.

Useful Video links

Unit No.	Topics	Links
Unit-I	Utilitarianism	https://www.youtube.com/watch?v=IngDKG5Nw
	Professional Ethics	https://www.youtube.com/watch?v=9LSEBK03CiY&list=PLysZquKdjuWSv87TaE7pByn5TE_e46O2C
	Privacy: Computers and privacy issue	https://www.youtube.com/watch?v=_aGgZ9u6g3I
Unit-II	Intellectual property issues in cyberspace	https://www.youtube.com/watch?v=SbqtGOPgqIY
	Ethical Decision Making	https://www.youtube.com/watch?v=iiByedXbbso
Unit-III	Crime incident Handling Basics	https://www.youtube.com/watch?v=dm9xZIzDhwM&list=PLFW6lRTa1g80JCqzslAXGHMFIo2AJ_qyb
	Information Technology Act 2000	https://www.youtube.com/watch?v=DQmQYeb8M
Unit-IV	Types of cybercrime.	https://www.youtube.com/watch?v=gwDghhXamo
	Cyber security and privacy	https://www.youtube.com/watch?v=OYsY5B9pqYU&list=PLyqSpQzTE6MjkJEzbS5oHJUp2GWPsq6e

Course Code	**MLC-01A**				
Category	Mandatory Learning Course				
Course Title	**Research Methodology and IPR**				
Scheme and Credits	L	T	P	**Credits**	**Semester-III**
	3	0	0	**3**	
Course Objectives	The objectives of this course are: • To enable students to identify and define research problems, formulate objectives and apply appropriate investigative approaches in research methodology. • To impart knowledge of data sources, data collection methods, data processing and the application of statistical tools for research analysis. • To develop awareness of research ethics, plagiarism issues and effective practices in technical writing, report preparation, and research documentation. • To provide a comprehensive understanding of intellectual property rights, patent procedures, technology transfer and international frameworks for innovation protection.				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total Marks	100				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

COs	**Skill Demonstrated**	**RBT Level**
CO1	Identify research problems, objectives, and data sources based on fundamental research methodology principles.	Level 1: Remember
CO2	Explain intellectual property rights, patent procedures, and international frameworks for technology transfer and innovation protection.	Level 2: Understand
CO3	Apply research ethics to prepare plagiarism-free technical reports, research papers, and proposals using effective writing and presentation techniques.	Level 3: Apply
CO4	Analyze research data through classification and tabulation to extract meaningful patterns and conclusions using statistical tools and methods.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem, Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations

Unit-II

Effective literature studies approaches, analysis, Plagiarism, Research ethics, Effective technical writing, how to write the report, Paper, Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee.

Unit-III

Sampling Methods, Need, Meaning & Type of Sample, Sources of Data, Primary and Secondary, Classification and Tabulation of Data Processing, Analysis and Interpretation of Data, Chi Square Test, significance of statistics in Socio-legal Research, Use of Computer in the Research field work and report writing.

Unit-IV

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, and development. International Scenario: International cooperation on Intellectual Property, Procedure for grants of patents, Patenting under PCT. Patent Rights: Scope of Patent Rights, Licensing and transfer of technology.

Suggested Readings:

1. Research Methodology: Methods and Techniques (4th ed.) by Kothari, C. R., & Garg, G, New Age International Publishers.
2. Research Methodology: A Step-by-Step Guide for Beginners (4th ed.). by Kumar, R, SAGE Publications India. ISBN: 978-9351501337
3. Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets (6th ed.) by Bouchoux, D. E, Cengage Learning.
4. Intellectual Property Rights under WTO by T. Ramappa, S. Chand.

Useful Video links

Unit No.	Topics	Links
Unit-I	Defining/formulating research problem	https://www.youtube.com/watch?v=oTc4_zjmev0
	Research types, descriptive, analytical, action, empirical, research methodology	https://www.youtube.com/watch?v=tjDBPRoyDJA
Unit-II	Types of Plagiarism	https://www.youtube.com/watch?v=5--ssYqyWoE
	Research Ethics	https://www.youtube.com/watch?v=4tRCov8pVgQ
Unit-III	Primary data and Secondary Data	https://www.youtube.com/watch?v=caUiRsg5M6k
	Sampling techniques	https://www.youtube.com/watch?v=sKtoW5cXt14
Unit-IV	Patent Trademarks and Copyrights.	https://www.youtube.com/watch?v=XQ8tRdcr0xQ
	What is Patent? Patent Filing Procedure in India	https://www.youtube.com/watch?v=azMNhrkRzww

<table>
<tr><td>Course Code</td><td colspan="5">**PRO-MTCFIS-213A**</td></tr>
<tr><td>Category</td><td colspan="5">Project</td></tr>
<tr><td>Course Title</td><td colspan="5">**Project**</td></tr>
<tr><td>Scheme and Credits</td><td>L</td><td>T</td><td>P</td><td>**Credits**</td><td rowspan="2">**Semester-III**</td></tr>
<tr><td></td><td>0</td><td>0</td><td>4</td><td>2</td></tr>
<tr><td>Course Objectives</td><td colspan="5">The objectives of this course are to
• Identify suitable research topics in Computer Science and Engineering for independent investigation.
• Understand research methodologies, documentation, and referencing aligned with existing literature.
• Develop technical writing skills using appropriate tools, formats, and referencing techniques.
• Analyze, interpret, and synthesize research findings within a defined research scope or topic.</td></tr>
<tr><td>Assessment</td><td colspan="5">50 Marks</td></tr>
<tr><td>End Semester Examination</td><td colspan="5">50 Marks</td></tr>
<tr><td>Total Marks</td><td colspan="5">100 Marks</td></tr>
<tr><td>Duration of Exam</td><td colspan="5">03 Hours</td></tr>
</table>

Course Outcomes: After successful completion of this course, the students will be able to

COs	Skills Demonstrated
CO1	Identify complex engineering problems relevant to project work based on domain knowledge and real-world challenges.
CO2	Describe the workflow, technical background, and tools required for planning and executing engineering projects.
CO3	Apply appropriate methods, tools, and techniques to carry out project development and prepare technical documentation.
CO4	Analyze the key stages of project development to ensure systematic execution and identify performance issues.
CO5	Evaluate alternative approaches and select suitable methodologies to achieve optimal and feasible project outcomes.
CO6	Design innovative and practical engineering solutions to address societal and industrial needs.

Course Code	**SM-MT-215A**				
Category	Seminar				
Course Title	**Seminar-III**				
Scheme and Credits	L	T	P	**Credits**	**Semester-III**
	0	0	2	**2**	
Course Objectives	The objectives of this course are ● To develop students' ability to effectively present research topics and findings by effective communication. ● To improve problem-solving and critical thinking skills of the students. ● To expose students to the latest trends and advancements by reviewing and discussing contemporary research.				
Assessment	50 Marks				
End Semester Examination	-				
Total Marks	50				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

COs	Skill Demonstrated
CO1	Identify the trends and advancements in the related field.
CO2	Analyze and synthesize research literature with in-depth reviews of key studies and methodologies.
CO3	Undertake problem identification, formulation, proposing solution and analyze the impact on society, economy and environment.
CO4	Prepare a well-organized report employing elements of effective communication and critical thinking.
CO5	Demonstrate a sound technical knowledge of their research field.

Overview:

This is a course designed to help M.Tech students develop research presentation skills. The focus is on selecting a topic or research paper relevant to their specialization, conducting an in-depth review, and effectively presenting the research findings.

General Guidelines:

Topic Selection	Each student is required to choose the research topic based on published review paper(s) or literature related to their relevant field. The same topic cannot be selected by multiple students.
Approval Process	The selected paper or topic must be approved by the faculty members/committee appointed by the Head of Department.
Presentation Guidelines	Each student will have 30-40 minutes for their presentation, followed by 5 minutes for Q&A.
Evaluation	The presentation will be evaluated by a committee constituted by the Head of Department. The evaluation will be based on:

Parameters for the Evaluation of Seminar

Sr. No.	Parameters	Marks Allotted	Relevant COs
1	Clarity of the topic	10	CO1
2	Literature Survey	10	CO2
3	Content Relevancy	10	CO3
4	Presentation Skills	10	CO4
5	Q&A Response	10	CO5

<table>
<tr><td>Course Code</td><td colspan="5"><b>DISS-MTCFIS-217A</b></td></tr>
<tr><td>Category</td><td colspan="5">Dissertation</td></tr>
<tr><td>Course Title</td><td colspan="5"><b>Dissertation (Phase-1)</b></td></tr>
<tr><td rowspan="2">Scheme and Credits</td><td>L</td><td>T</td><td>P</td><td><b>Credits</b></td><td rowspan="2"><b>Semester-III</b></td></tr>
<tr><td>0</td><td>0</td><td>4</td><td>2</td></tr>
<tr><td>Course Objectives</td><td colspan="5">The objectives of this course are to
• Introduce students to identifying relevant research topics in Cyber Forensics and Information Security.
• Explain the research process, including literature review, documentation, and structured writing.
• Develop proficiency in using research tools, reference management, and academic writing techniques.
• Enhance ability to analyze, synthesize, and present research findings in a chosen domain.</td></tr>
<tr><td>Assessment</td><td colspan="5">100 Marks</td></tr>
<tr><td>End Semester Examination</td><td colspan="5">-</td></tr>
<tr><td>Total</td><td colspan="5">100 Marks</td></tr>
<tr><td>Duration of Exam</td><td colspan="5">03 Hours</td></tr>
</table>

Course Outcomes: After successful completion of this course, the students will be able to

COs	Skills Demonstrated
CO1	Identify the research topic/area relevant to the field of Cyber Forensics and Information Security Computer Science and Engineering to carry out independent research.
CO2	Understand the research process, literature review, result formulation and writing conclusions with reference to existing literature.
CO3	Apply appropriate tools, references and writing skills for effective report writing related to research work.
CO4	Analyze and synthesize research findings to the agreed area of research carried out.
CO5	Evaluate the research methods and available knowledge to propose appropriate solutions to the specific research problem.
CO6	Design engineering solutions by developing improved results, properly documenting them in a thesis or report, and publishing them in journals or conferences.

Each student will undertake their dissertation under the supervision of one or more supervisors. The dissertation topic must be approved by a committee constituted by the Head of the concerned Department.

Students are required to deliver two seminar presentations: the first, at the beginning of Dissertation Phase-I, to outline the scope of the work and finalize the topic; the second, towards the end of the semester, to present the progress and work completed during the semester.

The committee will evaluate both presentations and award sessional marks out of 100. Students who fail to secure the minimum passing marks must improve their grade before proceeding to the 4th semester. Failure to do so will require the student to repeat Dissertation Phase-I in the next regular 3rd semester.

GANGA INSTITUTE OF TECHNOLOGY AND MANAGEMENT, KABLANA, JHAJJAR (HR.)

Scheme of Studies and Examination

M.Tech (Cyber Forensics and Information Security) –4th Semester

w.e.f. 2025-26

Sr. No.	Category	Course Code	Course Title	Hours per week			Total Load Per Week	Credits	Examination Scheme (Marks)				Exam Duration in H
				Lecture (L)	Tutorial (T)	Practical (P)			Assessment	End Semester Examination		Total	
										Theory	Practical		
1	Dissertation	DISS-MTCFIS-202A	Dissertation (Phase-2)	-	-	20	20	20	250		500	750	
Total Credits								**20**				**750**	

<table>
<tr><td>Course Code</td><td colspan="5"><b>DISS-MTCFIS-202A</b></td></tr>
<tr><td>Category</td><td colspan="5">Lab Courses</td></tr>
<tr><td>Course Title</td><td colspan="5"><b>Dissertation (Phase-2)</b></td></tr>
<tr><td rowspan="2">Scheme and Credits</td><td>L</td><td>T</td><td>P</td><td><b>Credits</b></td><td rowspan="2"><b>Semester-IV</b></td></tr>
<tr><td>0</td><td>0</td><td>20</td><td>20</td></tr>
<tr><td>Course Objectives</td><td colspan="5">The objectives of this course are to
• Introduce research fundamentals and help identify relevant topics in Cyber Forensics and Information Security.
• Understand literature review, structured research methodology and documentation of results and conclusions.
• Develop skills in using research tools, technical writing, referencing, and report formatting.
• Analyze, evaluate, and present research findings through effective report or thesis preparation.</td></tr>
<tr><td>Assessment</td><td colspan="5">250 Marks</td></tr>
<tr><td>End Semester Examination</td><td colspan="5">500 Marks</td></tr>
<tr><td>Total</td><td colspan="5">750 Marks</td></tr>
<tr><td>Duration of Exam</td><td colspan="5">03 Hours</td></tr>
</table>

Course Outcomes: After successful completion of this course, the students will be able to:

COs	Skills Demonstrated
CO1	Identify the research topic/area relevant to the field of Cyber Forensics and Information Security to carry out independent research.
CO2	Understand the research process, literature review, result formulation and writing conclusions with reference to existing literature.
CO3	Apply appropriate tools, references and writing skills for effective report writing related to research work.
CO4	Analyze and synthesize research findings to the agreed area of research carried out.
CO5	Evaluate the research methods and available knowledge to propose appropriate solutions to the specific research problem.
CO6	Design engineering solutions by developing improved results, properly documenting them in a thesis or report, and publishing them in journals or conferences.

Dissertation Phase-1 will continue as the final dissertation in the 4th semester. Sessional marks, out of 250, will be awarded by an internal committee constituted by the Head of the Department. The assessment will be based on presentations, reports, and related materials submitted to the committee. Failure to appear before the committee will result in disqualification from submitting the dissertation.

If a student scores less than 40% in the sessional assessment, they must revise and resubmit the dissertation after incorporating all required corrections and improvements. The revised dissertation will be evaluated in the next academic session.

At the end of the semester, each student is required to submit three soft-bound copies of their Master's dissertation to the office of the Head of the Department. One copy will be retained for departmental records, one will be provided to the supervisor, and one will be sent by mail to the external examiner, following their appointment and notification from the university.

The dissertation will be evaluated by a committee consisting of the Head of the Department, the dissertation supervisor(s), and one external examiner. The external examiner will be appointed by the Chairman of the Board of Studies. If the appointed examiner is unable to attend, the Director of the Institute, upon the recommendation of the Head of the Department, is authorized to appoint a substitute examiner from another institution or the parent institute.

Students must defend their dissertation through a presentation before the evaluation committee, which will assign marks accordingly.

Note:

- The scheme for awarding grades will be provided by the department to the examiner(s).
- The plagiarism of the dissertation report must be below 10%; otherwise, the report will not be accepted.
- Each student must publish at least one research paper related to their dissertation work in a peer-reviewed journal, IEEE conference, or SCOPUS/SCI-indexed journal before the final submission of Dissertation Phase-2.
- The student must follow the guidelines for the Dissertation report format as per Annexure-I.