S5 & S6 SYLLABUS

B. TECH.

COMPUTER SCIENCE AND ENGINEERING

(Cyber Security)

2024 SCHEME

FIFTH SEMESTER (July-December)														
Sl. No:	**Slot**	**Course Code**	**Course Type**	**Course Category**	**Course Title (Course Name)**	**Credit Structure**				**SS**	**Total Marks**		**Credits**	**Hrs./ Week**
						L	**T**	**P**	**R**		**CIE**	**ESE**		
1	A	24SJPCCCT501	PC	PC	Applied Cryptography	3	1	0	0	5	40	60	4	4
2	B	24SJPCCCT502	PC	PC	Network and System Security	3	1	0	0	5	40	60	4	4
3	C	24SJPCCST503	PC	PC	Machine Learning	3	0	0	0	4.5	40	60	3	3
4	D	24SJPBCST504	PC-PBL	PB	Microcontrollers	3	0	0	1	5.5	60	40	4	4
5	E	24SJPECCT52N	PE	PE	PE-2	3	0	0	0	4.5	40	60	3	3
6	I*	24SJICHUM506	HMC	IC	Constitution of India (MOOC)	-	-	-	-	2	-	-	1	-
7	L	24SJPCCCL507	PCL	PC	Cryptography Lab	0	0	3	0	1.5	50	50	2	3
8	Q	24SJPCCCL508	PCL	PC	Network and System Security Lab	0	0	3	0	1.5	50	50	2	3
9	R/M/H		VAC		Remedial/Minor/Honours Course	3	1	0	0	5			4*	4*
	S5/S6	Industrial Visit: Maximum 6 days (not exceeding 4 working days) / Industrial Training												
Total										**30 / 35**			**23/27***	**24/28***

No Grade Points will be awarded for the MOOC course and I slot course.

Industrial Training:

Students who are not participating in the industrial visit must attend industrial training during that period.

PROGRAM ELECTIVE 2: 24SJPECCT52N

SLOT	COURSE CODE	COURSES	L-T-P-R	HOURS	CREDIT
E	24SJPECCT521	Network fundamentals for cloud	3-0-0-0	**3**	**3**
	24SJPECCT522	Block chain and crypto currency	3-0-0-0		**3**
	24SJPECCT523	AI in Cyber Security	3-0-0-0		**3**
	24SJPECCT524	Advanced Industrial cyber security	3-0-0-0		**3**
	24SJPECST521	Software project management	3-0-0-0		**3**
	24SJ**PECST525**	**Data Mining**	**3-0-0-1**		**5/3**

SIXTH SEMESTER (January - June)														
Sl. No:	**Slot**	**Course Code**	**Course Type**	**Course Category**	**Course Title (Course Name)**	**Credit Structure**				**SS**	**Total Marks**		**Credits**	**Hrs./ Week**
						L	**T**	**P**	**R**		**CIE**	**ESE**		
1	A	24SJPCCST601	PC	PC	Compiler Design	3	1	0	0	5	40	60	4	4
2	B	24SJPCCCT602	PC	PC	Cyber Forensics	3	0	0	0	4.5	40	60	3	3
3	C	24SJPECCT63N	PE	PE	PE-3	3	0	0	0	4.5	40	60	3	3
4	D	24SJPBCCT604	PC-PBL	PB	Ethical Hacking and IoT Security	3	0	0	1	5.5	60	40	4	4
5	F	24SJGAEST605	ESC	GC	Design Thinking and Product Development (Group Specific Syllabus)	2	0	0	0	3	40	60	2	2
6	O	24SJOE--T61N /24SJIE--T61N	OE/ILE	OE/IE	OE/ILE-1	3	0	0	0	4.5	40	60	3	3
7	L	24SJPCCCL607	PCL	PC	Cyber Forensic Lab	0	0	3	0	1.5	50	50	2	3
8	P	24SJPCCSP608	PWS	PC	Mini Project: Socially Relevant Project	0	0	0	3	3	50	50	2	3
9	R/ M/ H		VAC		Remedial/Minor/Honours Course	3	0	0	0	4.5			3*	3*
	S5 / S6	Industrial Visit: Maximum 6 days (not exceeding 4 working days) / Industrial Training												
Total										**32/ 36**			**23/26***	**25/28***

Note: Open Electives are such courses which will be offered by other departments. Like CC department students have to opt open electives from ECE/ME/EEE etc. departments.

Industrial Training:

Students who are not participating in the industrial visit must attend industrial training during that period.

PROGRAM ELECTIVE 3: 24SJPECCT63N

SLOT	COURSE CODE	COURSES	L-T-P-R	HOURS	CREDIT
A	24SJPECCT631	Cloud Infrastructure and Systems	3-0-0-0	**3**	**3**
	24SJPECCT632	Cryptographic algorithms in blockchain	3-0-0-0		**3**
	24SJPECCT633	AI and ML in Cyber Security Defense	3-0-0-0		**3**
	24SJPECCT634	OT Threat Prevention	3-0-0-0		**3**
	24SJPECCT636	Privacy Regulations and Compliance	3-0-0-0		**3**
	24SJPECCT635	**Biometric Security**	**3-0-0-1**		**5/3**

Open Electives offered to other branches

OPEN ELECTIVE 1: 24SJOECST61N

SLOT	COURSE CODE	COURSES	L-T-P-R	HOURS	CREDIT
O	24SJOECST611	Data Structures	3-0-0-0	**3**	3
	24SJOECST612	Data Communication	3-0-0-0		3
	24SJOECST613	Foundations of Cryptography	3-0-0-0		3
	24SJOECST614	Machine Learning for Engineers	3-0-0-0		3
	24SJOECST615	Object Oriented Programming	3-0-0-0		3

SEMESTER S5
APPLIED CRYPTOGRAPHY

Course Code	**24SJPCCCT501**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:1:0:0	**ESE Marks**	60
Credits	4	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. Understand the fundamental principles of cryptography and network security.
2. Learn and apply cryptographic techniques and protocols.
3. Analyse the security mechanisms of symmetric and asymmetric cryptography.
4. Explore advanced cryptographic applications and emerging trends.
5. Implement security solutions in cloud computing, quantum computing, and IoT.

Module No.	Syllabus Description	Contact Hours
1	**Introduction to Cryptography and Security** **Introduction to Cryptography**: Definition and History of Cryptography - Importance and Applications - Key Terminologies and Concepts - Types of Attacks **Classical Encryption Techniques**: Substitution Ciphers: Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polybius Square Transposition Ciphers: Rail Fence, Columnar Transposition **Steganography:** Principles of Steganography, Types of Steganography, Steganography Versus Digital Watermarking, Types of Digital Watermarking, Goals of Digital Watermarking. **Quick Review of Number Theory**: Prime Numbers, Modular Arithmetic, Greatest Common Divisor, Fermat's and Euler's Theorems, Chinese Remainder Theorem	**10**
2	**Cryptographic Concepts and Techniques** **Symmetric Key Cryptography**: Block Ciphers: DES, 3DES, AES (Block Level only) - Stream Ciphers: RC4 - Modes of Operation: ECB, CBC, CFB, OFB, CTR **Asymmetric Key Cryptography**: Principles of Public Key Cryptosystems- RSA Algorithm-Diffie-Hellman Key Exchange-Elliptic Curve Cryptography	**10**
3	**Cryptographic Hash Functions**: Hash Function Requirements and Properties, SHA-256, SHA-3, MD5, HMAC **Message Authentication and Cryptographic Protocols** **Message Authentication Codes:** Structure and Usage, CMAC, GMAC, Digital Signatures: RSA, DSA, ECDSA **Cryptographic Protocols**: Key Management and Distribution, Public Key Infrastructure (PKI), SSL/TLS Protocol	**11**

4	**Secure Electronic Transactions**: E-commerce Security Requirements, Payment Protocols - SET, 3D Secure, Cryptographic Tokens **Advanced Cryptographic Applications and Emerging Trends** **Advanced Cryptographic Techniques**: Homomorphic Encryption, Zero- Knowledge Proofs **Quantum Cryptography**: Basics and Algorithms; **Cryptography in Cloud Computing and IoT**: Security Challenges and Cryptographic Solutions in Cloud Computing, Challenges and Cryptographic Solutions in IoT	**11**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)
Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)
In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Students will be able to understand the fundamental principles and historical context of cryptography, including key terminologies and classical encryption techniques.	**K3**
CO2	Students will be able to implement and analyze symmetric and asymmetric cryptographic algorithms, hash functions, and message authentication codes.	**K3**
CO3	Students will demonstrate the ability to apply cryptographic protocols to secure communication, key management, and electronic transactions.	**K2**

CO4	Students will be able to understand advanced cryptographic applications and emerging trends, including security in cloud computing, IoT, and quantum computing.	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**
CO1	✓	✓						✓			
CO2	✓	✓			✓			✓			
CO3	✓	✓	✓		✓			✓	✓		
CO4	✓		✓	✓	✓			✓			✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Cryptography and Network Security: Principles and Practices	William Stallings	Pearson	8th Ed, 2021
2	Introduction to Modern Cryptography: Principles and Protocols	Jonathan Katz and Yehuda Lindell	CRC Press	2020 (3rd Edition)

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Applied Cryptography: Protocols, Algorithms, and Source Code in C	Bruce Schneier	Wiley	2015
2	Cryptography and Network Security: Black Book	William Easttom	Dreamtech Press	2017
3	Understanding Cryptography: A Textbook for Students and Practitioners	Christof Paar and Jan Pelzl	Springer	2009
4	Network Security Essentials: Applications and Standards	William Stallings	Pearson	2016

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://www.youtube.com/watch?v=iTVyKbDCJrA
2	https://www.youtube.com/watch?v=UxtR-CB69Rw
3	https://www.youtube.com/watch?v=FOk8TN7HQLo
4	https://www.youtube.com/watch?v=9XC4mY_3X2I

SEMESTER S5
NETWORK AND SYSTEM SECURITY

Course Code	**24SJPCCCT502**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:1:0:0	**ESE Marks**	60
Credits	4	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. Enables learners to understand network security domain, the techniques for network protection
2. This course helps learners identify attacks and defenses in data and wireless networks.
3. Cryptography and Network Security: Principles and Practices enables the students to the basic functionalities and hardening of Windows and Linux operating system.
4. This course helps to identify the attacks and security in internet and web service.

Module No.	Syllabus Description	Contact Hours
1	**Module-1 (Principles of Network Security)** Principles of network security, Network Security Terminologies, CIA TRIAD Components of Network Security- Network Firewall-types, rules, personal firewalls, Intrusion Detection and Prevention System, Advanced Threat Protection, Network access Control, Web filtering. Network Security Policies. Network segments, Perimeter Defense, NAT, Penetration testing.	**10**
2	**Module-2 (Network Security**) Network Attacks, Services and Mechanisms, Network Security model, Network security and their relation to Steganography, Security in Data Networks, Wireless Device security issues- GPRS security, GSM security, IPsecurity. Wireless Transport Layer Security-Secure Socket Layer, Wireless Transport Layer Security - WAP Security, WAP security Architecture, WAP Gateway.	**10**
3	**Module-3 (System Security**) **Windows Security:** Attacks against windows system, Authentication and access control, Upgrades and Patches, System Hardening and Secure Configuration. **Linux Security**- Attacks in Linux system, Physical security, Controlling the configuration, Authentication and access control, Upgrades and Patches, Operating Linux safely.	**9**
4	**Module-4 (Web Security)** Web Browser and Client risk- How a web browser works, Web browser attacks, Operating safely, Web security- How HTTP works, Server and Client contents, Attacking Web servers, Web Services. E-mail security- The e-mail risk, Protocols, Authentication, Domain Name System – DNS basics, Purpose of DNS, Security Issues with DNS, DNS attacks.	**10**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	15	10	10	40

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Explain network security domain, the techniques for network protection and explore new tools and attacks in Network security domain.	**K1**
CO2	Identify the attacks and defense in wireless and data networks.	**K2**
CO3	Explain the functionalities and hardening of windows and Linux operating systems.	**K1**
CO4	Explain the various attacks as well as security measures in Internet and Web services.	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓		✓			✓		✓	✓
CO2	✓	✓	✓		✓			✓		✓	✓
CO3	✓	✓	✓		✓			✓		✓	✓
CO4	✓	✓	✓		✓			✓		✓	✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Network Security Bible	Eric Cole, Ronald Krutz, James W. Conley,	Wiley India Pvt Ltd, 2010	1st Edition, 2010
2	Principles of Information Security	Michael A Whitman, Herbert J.Mattord	Cengage Learning	4thEdition , 2016

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Network Security Essentials	William Stallings	Pearson Education	4th Edition, 2011
2	Fundamentals of Network security	Michael A Whitman, Herbert J.Mattord	Tata McGraw-Hill	1st Edition, 2011

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://nptel.ac.in/courses/106106129 https://onlinecourses.swayam2.ac.in/nou24_cs13/preview
2	https://onlinecourses.nptel.ac.in/noc24_cs80/preview https://nptel.ac.in/courses/106106129
3	https://nptel.ac.in/courses/106106129 https://www.udemy.com/course/web-security-and-bug-bounty-learn-penetration-testing/
4	https://nptel.ac.in/courses/106106129

SEMESTER 5
MACHINE LEARNING
(Common to CS/AD/CA/CC)

Course Code	**24SJPCCST503**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. To impart the fundamental principles of machine learning in computer and science.
2. To provide an understanding of the concepts and algorithms of supervised and unsupervised learning.

Module No.	Syllabus Description	Contact Hours
1	**Introduction to ML :-** Machine Learning vs. Traditional Programming, Machine learning paradigms- supervised, semi-supervised, unsupervised, reinforcement learning. Parameter Estimation - Maximum likelihood estimation (MLE) and maximum aposteriori estimation (MAP), Bayesian formulation. **Supervised Learning :-** Feature Representation and Problem Formulation, Role of loss functions and optimization. Regression - Linear regression with one variable, Linear regression with multiple variables : solution using gradient descent algorithm and matrix method.	**9**
2	**Classification** - Logistic regression, Naïve Bayes, KNN, Decision Trees – ID3, Generalisation and Overfitting - Idea of overfitting, LASSO and RIDGE regularization, Idea of Training, Testing, Validation Evaluation measures – Classification - Precision, Recall, Accuracy, F-Measure, Receiver Operating Characteristic Curve(ROC), Area Under Curve (AUC). Regression - Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), R Squared/Coefficient of Determination.	**9**
3	SVM – Linear SVM, Idea of Hyperplane, Maximum Margin Hyperplane, Non-linear SVM, Kernels for learning non-linear functions Neural Networks (NN) - Perceptron, Neural Network - Multilayer feed- forward network, Activation functions (Sigmoid, ReLU, Tanh), Back propagation algorithm.	**9**

4	**Unsupervised Learning** Clustering - Similarity measures, Hierarchical Clustering - Agglomerative Clustering, partitional clustering, K-means clustering Dimensionality reduction - Principal Component Analysis, Multidimensional scaling Ensemble methods - bagging, boosting; Resampling methods - Bootstrapping, Cross Validation. Practical aspects - Bias-Variance tradeoff.	**9**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24 marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 subdivisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Illustrate Machine Learning concepts and basic parameter estimation methods.	**K2**
CO2	Demonstrate supervised learning concepts (regression, classification).	**K3**
CO3	Illustrate the concepts of Multilayer neural network and Decision trees	**K3**
CO4	Describe unsupervised learning concepts and dimensionality reduction techniques	**K3**
CO5	Use appropriate performance measures to evaluate machine learning models	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

COs \ POs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓									
CO2	✓	✓		✓	✓						
CO3	✓	✓		✓	✓						
CO4	✓	✓		✓	✓						✓
CO5		✓		✓	✓				✓		

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Introduction to Machine Learning	Ethem Alpaydin	MIT Press	4/e, 2020
2	Data Mining and Analysis: Fundamental Concepts and Algorithms	Mohammed J. Zaki | Wagner Meira	Cambridge University Press	1/e, 2016
3	Neural Networks for Pattern Recognition	Christopher Bishop	Oxford University Press	1/e, 1998

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Applied Machine Learning	M Gopal	McGraw Hill	2/e, 2018
2	Machine Learning using Python	Manaranjan Pradhan | U Dinesh Kumar	Wiley	1/e, 2019
3	Machine Learning: Theory and Practice	M.N. Murty, V.S. Ananthanarayana	Universities Press	1/e, 2024

Video Links (NPTEL, SWAYAM…)	
No.	**Link ID**
1	*https://nptel.ac.in/courses/106106202*

SEMESTER S5
MICROCONTROLLERS
(Common to CS/CC)

Course Code	**24SJPBCST504**	**CIE Marks**	60
Teaching Hours/Week (L:T:P:R)	3:0:0:1	**ESE Marks**	40
Credits	4	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. To introduce the ARM architecture and ARM-based microcontroller architecture.
2. To impart knowledge on the hardware and software components to develop embedded systems using STM32 microcontrollers.

Module No.	**Syllabus Description**	**Contact Hours**
1	**Introduction to ARM Cortex-M Architecture: -** Overview of Embedded Systems, Applications of Embedded Systems, Introduction to Embedded C, Microcontrollers vs. Microprocessors, Classification of processors, Overview of ARM Cortex-M Series, Introduction to the Cortex-M23 and Cortex-M33 processors and the Armv8-mArchitecture, ARM Core Features: Registers, Memory, and Bus Architecture, Comparison with previous generations of Cortex-M processors.	**9**
2	**STM32 Microcontroller Overview and Peripheral Programming:-** Introduction to STM32 Family, STM32U575 Features and Specifications, Power Management and Low-Power Features Libraries, Introduction to Integrated Development Environment and HAL, Writing, and Debugging Your First Program(LED Interfacing), Interfacing Seven-Segment Display, LCD Display, and Matrix Keypad, Relay Interfacing, Analog to Digital Conversion: Potentiometer, temperature sensor, LDR, Microphone, Digital to Analog Conversion: Simple DAC Output Generation, Generating a Sine Wave, Audio Signal Generation, Interrupt Handling, Timer and Counter Applications: Basic Timer Configuration, Timers as Counters, Timer-Based Real-Time Clock (RTC)	**11**
3	**Communication Protocols and USB:-** Serial port terminal Application, Serial communication (USART, I2C, SPI, CAN), Interfacing an I2C Temperature Sensor and Displaying Data on an LCD, writing to and Reading from an SPI-based EEPROM, Configuring and Implementing CAN Communication between Multiple STM32U575 Microcontrollers, Creating a USB HID Device for Keyboard / Mouse Emulation.	**10**

4	**IoT, Wireless Communication, and RTOS:-** Introduction to IoT, IoT Architecture, Protocols (MQTT, CoAP), IoT Security Principles and Common Threats Wireless Communication: Interfacing GSM (Call, SMS, Internet), Bluetooth Communication Basics, LoRa Communication Basics and Applications, Designing an IoT-Based Home Automation System, Introduction to RTOS Concepts, FreeRTOS with STM32: Task Creation, Scheduling, and Management, RTOS Timers, Delays, and RTC Integration, Inter-task Communication: Queues and Semaphores. **Trust Zone Technology:** Introduction to ARM Trust Zone, Trust Zone Architecture and Features, Secure and Non-Secure Worlds: Configuration and Management, Implementing Trust Zone in STM32U575, Advanced Debugging and Optimization: Code and Memory Optimization Techniques, Debugging Strategies and Tools	**14**

Suggestion on Project Topics

- Identify real world problems requiring hardware solutions and develop them using peripheral devices. Some of the examples would be - Home automation, Small home/office security system, ARM based voice response system etc.

Course Assessment Method (CIE: 60 marks, ESE: 40 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Project	Internal Ex-1	Internal Ex-2	Total
5	**30**	**12.5**	**12.5**	**60**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 2 marks **(8x2 =16 marks)**	2 questions will be given from each module, out of which 1 question should be answered. Each question can have a maximum of 2 subdivisions. Each question carries 6 marks **(4x6 = 24 marks)**	**40**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcomes		Bloom's Knowledge Level (KL)
CO1	Explain the architectural features and instructions of the ARM microcontrollers.	**K2**
CO2	Develop applications involving interfacing of external devices and I/O with ARM microcontroller.	**K3**
CO3	Use various communication protocols of interaction with peer devices and peripherals.	**K3**
CO4	Demonstrate the use of a real time operating system in embedded system applications.	**K3**
CO5	Apply hardware security features of ARM in real world applications.	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓								✓
CO2	✓	✓	✓								✓
CO3	✓	✓	✓	✓	✓						✓
CO4	✓	✓	✓	✓	✓						✓
CO5	✓	✓	✓	✓							✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	The Definitive Guide to ARM Cortex-M3 and Cortex-M4 Processors	Joseph Yiu	Newnes - Elsevier	3/e, 2014
2	Mastering STM32	Carmine Noviello	Learnpub	2/e, 2022

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	ARM System Developer's Guide	Andrew N. Sloss, Dominic Symes, Chris Wright	Morgan Kaufman	1/e, 2008
2	Embedded System Design with Arm Cortex-M Microcontrollers	Cem Ünsalan, Hüseyin Deniz Gürhan Mehmet Erkin Yücel	Springer	1/e, 2022
3	Introduction to ARM ® Cortex-M Microcontrollers	Jonathan W. Valvano	Self-Published	5/e, 2014

PBL Course Elements

L: Lecture (3 Hrs.)	**R: Project (1 Hr.), 2 Faculty Members**		
	Tutorial	**Practical**	**Presentation**
Lecture delivery	Project identification	Simulation/ Laboratory Work/ Workshops	Presentation (Progress and Final Presentations)
Group discussion	Project Analysis	Data Collection	Evaluation

Question answer Sessions/ Brainstorming Sessions	Analytical thinking and self-learning	Testing	Project Milestone Reviews, Feedback, Project reformation (If required)
Guest Speakers (Industry Experts)	Case Study/ Field Survey Report	Prototyping	Poster Presentation/ Video Presentation: Students present their results in a 2 to 5 minutes video

Assessment and Evaluation for Project Activity

Sl. No	Evaluation for	Allotted Marks
1	Project Planning and Proposal	5
2	Contribution in Progress Presentations and Question Answer Sessions	4
3	Involvement in the project work and Team Work	3
4	Execution and Implementation	10
5	Final Presentations	5
6	Project Quality, Innovation and Creativity	3
Total		**30**

1. **Project Planning and Proposal (5 Marks)**
   - Clarity and feasibility of the project plan
   - Research and background understanding
   - Defined objectives and methodology
2. **Contribution in Progress Presentation and Question Answer Sessions (4 Marks)**
   - Individual contribution to the presentation
   - Effectiveness in answering questions and handling feedback
3. **Involvement in the Project Work and Team Work (3 Marks)**
   - Active participation and individual contribution
   - Teamwork and collaboration
4. **Execution and Implementation (10 Marks)**
   - Adherence to the project timeline and milestones
   - Application of theoretical knowledge and problem-solving
   - Final Result
5. **Final Presentation (5 Marks)**
   - Quality and clarity of the overall presentation
   - Individual contribution to the presentation
   - Effectiveness in answering questions
6. **Project Quality, Innovation, and Creativity (3 Marks)**
   - Overall quality and technical excellence of the project
   - Innovation and originality in the project
   - Creativity in solutions and approaches

SEMESTER S5
CRYPTOGRAPHY LAB

Course Code	**24SJPCCCL507**	**CIE Marks**	50
Teaching Hours/Week (L: T:P: R)	0:0:3:0	**ESE Marks**	50
Credits	2	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Lab

Course Objectives:

1. Develop Practical Skills in Cryptographic Techniques: To equip students with hands-on experience in implementing and analyzing various cryptographic algorithms, including classical ciphers, symmetric encryption, and asymmetric encryption techniques.
2. Enhance Understanding of Cryptographic Principles and Applications: To enable students to demonstrate and apply fundamental cryptographic principles in real-world scenarios, ensuring data integrity, confidentiality, and authentication through practical coding exercises.
3. Foster Proficiency in Secure Communication and Memory Management: To cultivate students' ability to design and implement secure communication protocols and to simulate memory allocation and garbage collection using linked lists, integrating cryptographic methods with effective memory management techniques.

A minimum of ten experiments must be completed as part of the course requirements.

Expt. No.	Experiments
1	Represent a string (char pointer) with a value "Hello world". The program should XOR each character in this string with 0 and displays the result*
2	Represent string (char pointer) with a value "Hello world" The program should AND, OR, and XOR each character in this string with 127 and display the result.*
3	Perform encryption and decryption using the following algorithms* a. Ceaser cipher b. Substitution cipher c. Hill Cipher
4	Implementation of Encryption and Decryption using DES*
5	Implementation of RSA Encryption Algorithm*
6	Implementation of Hash Functions*
7	Implementation of Blowfish algorithm logic
8	Implement the Diffie-Hellman Key Exchange mechanism*
9	Implement RC4 logic using Java*
10	Encrypt the text "Hello world" using Blowfish.*
11	Implement the SIGNATURE SCHEME –Digital Signature Standard*
12	Implement LSB Steganography.

PRACTICE QUESTIONS

1. Write a C program that contains a string (char pointer) with a value “Hello world”. The program should XOR each character in this string with 0 and displays the result.
2. Write a C program that contains a string (char pointer) with a value “Hello world”. The program should AND, OR, and XOR each character in this string with 127 and display the result.
3. Write a Java program to perform encryption and decryption using the following algorithms
    a. Caeser cipher
    b. Substitution cipher
    c. Hill Cipher
4. Write a C/JAVA program to implement DES Encryption and Decryption
5. Write a C/JAVA program to implement RSA Encryption Algorithm
6. Write a C/JAVA program to implementation of Hash Functions.
7. Write a C/JAVA program to implement the Blowfish algorithm logic.
8. Write the RC4 logic in Java Using Java cryptography; encrypt the text Hello world using Blowfish. Create your own key using Java key tool.
9. Write a C/JAVA program to implement the Diffie-Hellman Key Exchange mechanism
10. Implement the SIGNATURE SCHEME –Digital Signature Standard
11. Embed a short text message (up to 8 characters) into the least significant bits of the image's pixel data. Read the modified image and extract the hidden message.

Course Assessment Method (CIE: 50 marks, ESE: 50 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Preparation/Pre-Lab Work experiments, Viva and Timely completion of Lab Reports / Record (Continuous Assessment)	Internal Examination	Total
5	25	20	50

Note: Students are instructed to submit only the fair record for both Continuous Internal Evaluation (CIE) and End Semester Examinations (ESE). Rough records are not required.

End Semester Examination Marks (ESE):

Procedure/ Preparatory work/Design/ Algorithm	Conduct of experiment/ Execution of work/ troubleshooting/ Programming	Result with valid inference/ Quality of Output	Viva voce	Record	Total
10	15	10	10	5	50

- ***Submission of Record: Students shall be allowed for the end semester examination only upon submitting the duly certified record.***
- ***Endorsement by External Examiner:*** *The external examiner shall endorse the record*

Course Outcomes (COs)

At the end of the course students should be able to:

	Course Outcome	Bloom's Knowledge Level (KL)
CO1	Students will implement various classical and modern cipher techniques to understand the process of securing information.	**K3**
CO2	Students will code and distinguish between symmetric and asymmetric cryptographic methods, gaining practical knowledge of both types.	**K3**
CO3	Students will explore and implement different encryption techniques and message authentication codes (MACs) to ensure data integrity and security.	**K3**
CO4	Students will write programs to implement the DES (Data Encryption Standard) and RSA (Rivest-Shamir-Adleman) algorithms, understanding their mechanisms and uses.	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO- PO Mapping (Mapping of Course Outcomes with Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓	✓	✓	✓	✓	✓			✓
CO2	✓	✓	✓	✓	✓	✓	✓	✓			✓
CO3	✓	✓	✓	✓	✓	✓	✓	✓			✓
CO4	✓	✓	✓	✓	✓	✓	✓	✓			✓

Text Books

Sl. No	Title of the Book	Name of the Author/s	Name of the Publisher	Edition and Year
1	Applied Cryptography: Protocols, Algorithms and Source Code in C	Bruce Schneier	Wiley	2015

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://cse29-iiith.vlabs.ac.in/ (AICTE Virtual Labs)

Continuous Assessment (25 Marks)

1. Preparation and Pre-Lab Work (7 Marks)

- Pre-Lab Assignments: Assessment of pre-lab assignments or quizzes that test understanding of the upcoming experiment.
- Understanding of Theory: Evaluation based on students' preparation and understanding of the theoretical background related to the experiments.

2. Conduct of Experiments (7 Marks)

- Procedure and Execution: Adherence to correct procedures, accurate execution of experiments, and following safety protocols.

- Skill Proficiency: Proficiency in handling equipment, accuracy in observations, and troubleshooting skills during the experiments.
- Teamwork: Collaboration and participation in group experiments.

3. Lab Reports and Record Keeping (6 Marks)

- Quality of Reports: Clarity, completeness and accuracy of lab reports. Proper documentation of experiments, data analysis and conclusions.
- Timely Submission: Adhering to deadlines for submitting lab reports/rough record and maintaining a well-organized fair record.

4. Viva Voce (5 Marks)

- Oral Examination: Ability to explain the experiment, results and underlying principles during a viva voce session.

Final Marks Averaging: The final marks for preparation, conduct of experiments, viva, and record are the average of all the specified experiments in the syllabus.

Evaluation Pattern for End Semester Examination (50 Marks)

1. **Procedure/Preliminary Work/Design/Algorithm (10 Marks)**
   - Procedure Understanding and Description: Clarity in explaining the procedure and understanding each step involved.
   - Preliminary Work and Planning: Thoroughness in planning and organizing materials/equipment.
   - Algorithm Development: Correctness and efficiency of the algorithm related to the experiment.
   - Creativity and logic in algorithm or experimental design.

2. **Conduct of Experiment/Execution of Work/Programming (15 Marks)**
   - Setup and Execution: Proper setup and accurate execution of the experiment or programming task.
3. **Result with Valid Inference/Quality of Output (10 Marks)**
   - Accuracy of Results: Precision and correctness of the obtained results.
   - Analysis and Interpretation: Validity of inferences drawn from the experiment or quality of program output.
4. **Viva Voce (10 Marks)**
   - Ability to explain the experiment, procedure results and answer related questions
   - Proficiency in answering questions related to theoretical and practical aspects of the subject.
5. **Record (5 Marks)**
   - Completeness, clarity, and accuracy of the lab record submitted

SEMESTER S5

NETWORK AND SYSTEM SECURITY LAB

Course Code	**24SJPCCCL508**	**CIE Marks**	50
Teaching Hours/Week (L: T:P: R)	0:0:3:0	**ESE Marks**	50
Credits	2	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Lab

Course Objectives:

1. Familiarize tools to prevent latest threats
2. Analyze the network traffic using sniffing tools.
3. Use network scanning tools
4. Familiarize various Steganography tools
5. Use tools for Penetration testing

A minimum of ten experiments must be completed as part of the course requirements.

Expt. No.	Experiments
1	Preventing PC against latest threats using Windows Defender.
2	Data hiding using Xiao Steganography
3	Website mirroring using HTTrack
4	Monitor, capture and analyze network packets using Wireshark.
5	Network mapping and analysing. Using Nmap
6	Port Scanning using Angry IP Scanner or Advanced IP Scanner.
7	Penetration testing and Vulnerability Scanning using Burp Suit.
8	Password Cracking-Use John The ripper /hydra

PRACTICE QUESTIONS

1. You need to protect a Windows computer from malware and viruses without installing any third-party software. Which built-in tool can you use to scan and remove malicious threats?
2. A user reports that their computer is behaving strangely, and you suspect malware. Which default Windows tool would you use to perform a quick or full system scan to identify and eliminate the threat?
3. You need to troubleshoot network latency issues by examining the timing of packet transmissions. Which tool will help you capture and analyze the packet flow to identify the cause of the delay?
4. To verify the integrity of communication between two endpoints on your network, you want to capture and analyze the packets being exchanged. Which tool would be best suited for this task?
5. You need to scan a network to discover active devices and identify open ports on each device. Which tool can you use to perform this network discovery and security auditing?
6. You need to create an offline copy of a website for analysis and reference. Which tool can you use to download the entire site, including HTML, images, and other files?
7. You want to back up a website's content and structure to ensure you have a local copy in case the site becomes unavailable. Which tool should you use to accomplish this task efficiently?
8. You need to hide sensitive data within an image file to ensure it remains undetected by unauthorized users. Which tool would you use to embed and later extract this hidden information?
9. During a network inventory process, you want to quickly discover and document all the IP addresses currently in use. Which tool would help you perform this task efficiently?
10. To test the security of a web application, you need to perform automated vulnerability scanning and manual testing for common web application flaws. Which tool provides integrated features for both types of testing?

Course Assessment Method (CIE: 50 marks, ESE: 50 marks)
Continuous Internal Evaluation Marks (CIE):

Attendance	Preparation/Pre-Lab Work experiments, Viva and Timely completion of Lab Reports / Record (Continuous Assessment)	Internal Examination	Total
5	25	20	50

Note: Students are instructed to submit only the fair record for both Continuous Internal Evaluation (CIE) and End Semester Examinations (ESE). Rough records are not required.

End Semester Examination Marks (ESE):

Procedure/ Preparatory work/Design/ Algorithm	Conduct of experiment/ Execution of work/ troubleshooting/ Programming	Result with valid inference/ Quality of Output	Viva voce	Record	Total
10	15	10	10	5	50

- ***Submission of Record: Students shall be allowed for the end semester examination only upon submitting the duly certified record.***
- ***Endorsement by External Examiner:*** *The external examiner shall endorse the record*

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Familiarize tools to prevent latest threats	**K3**
CO2	Analyze the network traffic using sniffing tools	**K3**
CO3	Use network scanning tools	**K3**
CO4	Familiarize various Steganography tools	**K3**
CO5	Use tools for Penetration testing	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO- PO Mapping (Mapping of Course Outcomes with Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓	✓	✓			✓			✓
CO2	✓	✓	✓	✓	✓			✓			✓
CO3	✓	✓	✓	✓	✓			✓			✓
CO4	✓	✓	✓	✓	✓			✓			✓
CO5	✓	✓	✓	✓	✓			✓			✓

Continuous Assessment (25 Marks)

1. **Preparation and Pre-Lab Work (7 Marks)**
   - Pre-Lab Assignments: Assessment of pre-lab assignments or quizzes that test understanding of the upcoming experiment.
   - Understanding of Theory: Evaluation based on students' preparation and understanding of the theoretical background related to the experiments.
2. **Conduct of Experiments (7 Marks)**
   - Procedure and Execution: Adherence to correct procedures, accurate execution of experiments, and following safety protocols.
   - Skill Proficiency: Proficiency in handling equipment, accuracy in observations, and troubleshooting skills during the experiments.
   - Teamwork: Collaboration and participation in group experiments.
3. **Lab Reports and Record Keeping (6 Marks)**
   - Quality of Reports: Clarity, completeness and accuracy of lab reports. Proper documentation of experiments, data analysis and conclusions.
   - Timely Submission: Adhering to deadlines for submitting lab reports/rough record and maintaining a well-organized fair record.
4. **Viva Voce (5 Marks)**
   - Oral Examination: Ability to explain the experiment, results and underlying principles during a viva voce session.

Final Marks Averaging: The final marks for preparation, conduct of experiments, viva, and record are the average of all the specified experiments in the syllabus.

Evaluation Pattern for End Semester Examination (50 Marks)

1. **Procedure/Preliminary Work/Design/Algorithm (10 Marks)**
   - Procedure Understanding and Description: Clarity in explaining the procedure and understanding each step involved.
   - Preliminary Work and Planning: Thoroughness in planning and organizing materials/equipment.
   - Algorithm Development: Correctness and efficiency of the algorithm related to the experiment.
   - Creativity and logic in algorithm or experimental design.

2. **Conduct of Experiment/Execution of Work/Programming (15 Marks)**
   - Setup and Execution: Proper setup and accurate execution of the experiment or programming task.

3. **Result with Valid Inference/Quality of Output (10 Marks)**
   - Accuracy of Results: Precision and correctness of the obtained results.
   - Analysis and Interpretation: Validity of inferences drawn from the experiment or quality of program output.

4. **Viva Voce (10 Marks)**
   - Ability to explain the experiment, procedure results and answer related questions
   - Proficiency in answering questions related to theoretical and practical aspects of the subject.

5. **Record (5 Marks)**
   - Completeness, clarity, and accuracy of the lab record submitted.

PROGRAM ELECTIVE 2: 24SJPECCT52N

SEMESTER S5

NETWORK FUNDAMENTALS FOR CLOUD

Course Code	24SJPECCT521	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	Basic knowledge of networking concepts and familiarity with operating systems	**Course Type**	Theory

Course Objectives:

1. To understand core networking concepts, such as IP addressing, subnetting, and routing.
2. To implement cloud networking solutions, including designing and configuring virtual networks and security settings.
3. To troubleshoot network issues within cloud environments.
4. To integrate cloud and on-premises networks, managing hybrid systems effectively

Module No.	Syllabus Description	Contact Hours
1	**Introduction to Networking Concepts and Cloud Computing: -** Basics of Computer Networks: Overview of Network Types: LAN, WAN, Pan, OSI and TCP/IP Models. IP Addressing and Subnetting: IPv4 vs. IPv6 Addressing, Subnetting Concepts and Techniques. Introduction to Cloud Computing: Cloud Computing Models: IaaS, PaaS, SaaS. Cloud Architecture Overview. Networking in Cloud Environments: Importance of Networking inCloud, Interaction Between Traditional Networks and Cloud Infrastructures.	**9**
2	**Networking Protocols and Cloud Connectivity: -** TCP/IP Protocol Suite: Deep Dive into TCP/IP Protocols, Role of TCP/IP in Cloud Environments.	**9**

	DNS and DHCP in the Cloud, DNS Configuration in Cloud, DHCP in Cloud Networks. Virtual Private Networks (VPN): VPN Implementation in Cloud, Securing VPNs for Cloud Connectivity. Load Balancing in Cloud: Load Balancer Types and Configurations, Implementing Load Balancers in Cloud. Virtual Private Cloud (VPC), VPC Configuration and Management, VPC Peering and Gateways. Hybrid Cloud Connectivity, Integrating Public and Private Clouds, Challenges and Solutions in Hybrid Cloud Connectivity.	
3	**Cloud Networking Components, Architectures, and Security:** Virtual Networking and SDN: Virtual Networks (VNet) Configuration, Principles of SDN and Implementation in Cloud, Network Function. Virtualization (NFV) and Microservices: NFV Components and Architecture, Networking for Containers (Docker, Kubernetes). Cloud Network Design Principles: Designing for Scalability and Flexibility, Redundancy and Disaster Recovery Planning. Security in Cloud Networks: Cloud-Native Security Controls, Intrusion Detection and Prevention Systems (IDPS), Identity and Access Management (IAM), Encryption Techniques and Zero-Trust Architecture.	**9**
4	**Monitoring, Troubleshooting, and Optimizing Cloud Networks: -** Network Monitoring in Cloud: Tools for Cloud Network Monitoring, Setting Up Alerts and Dashboards. Troubleshooting Cloud Networks: Common Cloud Networking Issues and Solutions, Using Diagnostic Tools (e.g., Traceroute, Ping). Network Traffic Analysis and Optimization: Analyzing Traffic Patterns in Cloud Networks, Performance Tuning and Cost- Effective Network Configuration. Automation in Cloud Network Management: Automating Network Configuration and Management, Using Infrastructure as Code (IaC)Tools.	**9**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)
Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	15	10	10	40

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Illustrate Fundamental Networking Concepts and Cloud Computing Basics.	**K2**
CO2	Explain IP Addressing and Subnetting Techniques.	**K2**
CO3	Apply Networking Protocols and Cloud Connectivity Solutions.	**K3**
CO4	Illustrate Cloud Networking Components and SecurityMeasures	**K2**
CO5	Troubleshooting and Optimization Techniques in CloudNetworks.	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓									✓
CO2	✓	✓									✓
CO3	✓	✓									✓
CO4	✓	✓									✓
CO5	✓	✓	✓	✓	✓						✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Computer Networking: A Top-Down Approach	James F. Kurose and KeithW. Ross	Pearson Publications	Eight Edition, 2017.
2	Cloud Computing: Concepts, Technology & Architecture	Thomas Erl, Ricardo Puttini, and Zaigham Mahmood	Prentice Hall Publications	First edition, 2013.

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Cloud Networking: Understanding Cloud-based Data Center Networks	Gary Lee and Lee Hwee Kuan	CRC Press	First edition, 2017.
2	Network Security Essentials: Applications and Standards	William Stallings	Pearson Publications	Sixth edition, 2020.
3	AWS Certified Advanced Networking Official Study Guide: Specialty Exam	Brad Bulger, Ather Khan, and Stephen Cole	Wiley Publications	First edition, 2020.

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://youtu.be/fErDcUtd8fA?si=vk5rYduwokgAqUMh
2	https://youtu.be/3NDhETVfrp0?si=MyOfYaRDJRJ0gn9F
3	https://youtu.be/RWgW-CgdIk0?si=HN9mHIo4w9-J4IaJ
4	https://youtu.be/YmYWevNdcik?si=8dO1vCGjO1yPQ8XE

SEMESTER S5

BLOCK CHAIN AND CRYPTO CURRENCY

Course Code	**24SJPECCT522**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. To undertake path-breaking research that creates new computing technologies and solutions for industry and society at large.
2. To create cryptocurrencies and give a strong technical understanding of Blockchain technologies with an in-depth understanding of applications, open research challenges, and future directions.

Module No.	Syllabus Description	Contact Hours
1	INTRODUCTION TO BLOCKCHAIN Block chain- Public Ledgers, Blockchain as Public Ledgers – Block in a Blockchain, Transactions-The Chain and the Longest Chain – Permissioned Model of Blockchain, Cryptographic -Hash Function, Properties of a hash function-Hash pointer and Merkle tree	**9**
2	BITCOIN AND CRYPTOCURRENCY A basic crypto currency, Creation of coins, Payments and double spending, FORTH – the precursor for Bitcoin scripting, Bitcoin Scripts, Bitcoin P2P Network, Transaction in Bitcoin Network, Block Mining, Block propagation and block relay	**9**
3	BITCOIN CONSENSUS Bitcoin Consensus, Proof of Work (PoW)- Hash-cash PoW, Bitcoin PoW, Attacks on PoW, monopoly problem- Proof of Stake- Proof of Burn - Proof of Elapsed Time – Bitcoin Miner, Mining Difficulty, Mining Pool-Permissioned model and use cases.	**9**
4	HYPERLEDGER FABRIC & ETHEREUM Architecture of Hyperledger fabric v1.1- chain code- Ethereum: Ethereum network, EVM, Transaction fee, Mist Browser, Ether, Gas, Solidity. BLOCK-CHAIN APPLICATIONS. Blockchain Applications in Supply Chain Management, Logistics, Smart Cities, Finance and Banking, Insurance, etc.- Case Study.	**9**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)
Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

	Course Outcome	Bloom's Knowledge Level (KL)
CO1	Understand emerging abstract models for Blockchain Technology	**K2**
CO2	Identify major research challenges and technical gaps existing between theory and practice in the crypto currency domain.	**K4**
CO3	It provides conceptual understanding of the function of Blockchain as a method of securing distributed ledgers, how consensus on their contents is achieved, and the new applications that they enable.	**K2**
CO4	Apply hyperledger Fabric and Ethereum platform to implement the Block chain Application	**K3**
CO5	Understand the applications of blockchain in various fields.	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyze, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓								✓
CO2	✓	✓	✓								✓
CO3	✓	✓	✓								✓
CO4	✓	✓	✓								✓
CO5	✓	✓	✓								✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3, 4th Edition	Bashir and Imran	Kindle Edition	2023
2	"Mastering Bitcoin: Unlocking Digital Cryptocurrencies",	Andreas Antonopoulos Drescher	O'Reilly	2023
3	Handbook of Research on Blockchain Technology		Elsevier Inc. ISBN: 978012819816	2020.

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://youtu.be/fu8SFiO948A?feature=shared
2	https://www.youtube.com/live/hixM4u7ep58?feature=shared
3	https://youtu.be/fw3WkySh_Ho?feature=shared

SEMESTER S5

AI IN CYBER SECURITY

Course Code	**24SJPECCT523**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	24SJPECCT413 Introduction to AI and ML	**Course Type**	Theory

Course Objectives:

1. Understand the application of AI in various aspects of Cyber Security
2. Identify and describe Machine Learning techniques used in threat detection.
3. Utilize AI-based tools for cybersecurity tasks.
4. Apply AI-driven data analysis to identify and mitigate cyber threats.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	**AI in Cyber Security** **Role of AI in Cyber Security:** Introduction to the role of AI in cybersecurity: how AI is transforming cyber defenses, Discussion on the current state of cyber threats and how AI can mitigate them **Review of Basic Cyber Threats**: Overview of basic cyber threats: malware, phishing, DDoS attacks, etc. Introduction to AI Tools in Cyber Security: Overview of commonly used AI tools (e.g., antivirus software, intrusion detection systems) **Case Studies: AI Applications in Cyber Security** Case Study 1: How AI stopped a major phishing campaign (e.g., Google's Safe Browsing) Case Study 2: Using AI to detect anomalies in network traffic (e.g., DARPA's Cyber Grand Challenge)	**9**
2	**Machine Learning in Threat Detection** **Application of Supervised Learning in Threat Detection**: Introduction to supervised learning: concepts and algorithms, Practical examples of supervised learning in detecting malware **Introduction to Unsupervised Learning Techniques for Anomaly Detection:** Overview of unsupervised learning: clustering, anomaly detection Case Study: Unsupervised learning in detecting insider threats (e.g., detecting insider trading in financial institutions)	**9**

3	**AI-Based Tools and Techniques in Cyber Security** **Overview of AI-Powered Cybersecurity Tools:** Introduction to advanced AI-powered tools: firewalls, intrusion detection systems, Discussion on how AI enhances traditional cybersecurity tools, AI-based firewalls and their real-world applications **Introduction to AI-Driven Data Analysis Techniques:** Basic concepts of AI-driven data analysis in cybersecurity Case Study: How AI-driven data analysis thwarted a cyber-attack (e.g., IBM's Watson in Cybersecurity)	**9**
4	**Ethical Considerations and Challenges in AI for Cyber Security** **Ethical Implications of AI in Cyber Security:** Ethical issues surrounding AI in cybersecurity (privacy, bias, etc.) **Challenges in Implementing AI for Cyber Security:** Technical challenges in AI-based cybersecurity (data quality, model robustness), Future Trends and Ethical Balances in AI and Cyber Security, Emerging trends in AI for cybersecurity Case Study: Privacy concerns with AI-driven surveillance (e.g., AI in facial recognition by law enforcement)	**9**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Mark (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	To describe the role of AI in modern cybersecurity.	**K2**
CO2	To explain the application of supervised learning in threat detection.	**K2**
CO3	To analyze real-world applications of AI in virus detection and intrusion prevention.	**K3**
CO4	To explain the ethical implications of AI in cybersecurity, including privacy and bias issues.	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓						✓		
CO2	✓	✓	✓						✓		
CO3	✓	✓	✓	✓	✓				✓		
CO4	✓	✓				✓		✓	✓		

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Artificial Intelligence in Cyber Security: Theories and Applications	Himanshu Upadhyay, Steven Lawrence Fernandes, Tarun Kumar Sharma, Tushar Bhardwaj	Springer International Publishing	2023
2	Artificial Intelligence in Cyber Security.	Rahul Neware Khaja Mannanuddin, Mukesh Madanan, Dr. Shikha Gupta	Book Rivers	2022

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Artificial Intelligence in Cybersecurity	Leslie F. Sikos	Springer International Publishing	2018
2	Artificial Intelligence for Cybersecurity: Techniques, Challenges and Research	Mark Stamp	Springer International Publishing	2022
3	Machine Learning and Security: Protecting Systems with Data and Algorithms	Clarence Chio, David, Freeman	O'Reilly Media	2018

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	Cyber Security and Privacy by Prof. Saji K Mathew (NPTEL)
2	Applied Accelerated Artificial Intelligence By Prof. Satyajit Das, Prof. Satyadhyan Chickerur, Prof. Bharatkumar Sharma, Prof. Adesuyi Tosin, Prof.Ashrut Ambastha
3	Applied Accelerated Artificial Intelligence By Prof. Satyajit Das, Prof. Satyadhyan Chickerur, Prof. Bharatkumar Sharma, Prof. Adesuyi Tosin, Prof.Ashrut Ambastha
4	Applied Accelerated Artificial Intelligence By Prof. Satyajit Das, Prof. Satyadhyan Chickerur, Prof. Bharatkumar Sharma, Prof. Adesuyi Tosin, Prof.Ashrut Ambastha

SEMESTER S5

ADVANCED INDUSTRIAL CYBER SECURITY

Course Code	**24SJPECCT524**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	24SJPECCT414 FUNDAMENTALS OF INDUSTRIAL CONTROL SYSTEM SECURITY	**Course Type**	Theory

Course Objectives:

1. Enables the learners to understand the advanced concepts of Network Security and Endpoint Security.

2. Enables the learners to apply the best practices in each phase of SDLC and gain an insight on data classification and data loss prevention.

3. Enables learners to manage the full life cycle of digital entities, gain skills in deploying SIEM systems and apply threat intelligence to improve organizational security.

4. Enables the learners to understand the Compliance and regulatory controls and gain knowledge on emerging technologies related to industrial cyber security.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	**Network Security Controls:** Firewalls - Types of Firewalls, Configuration of Firewalls, Intrusion Detection and Prevention Systems (IDPS), Virtual Private Networks (VPNs), Network Segmentation. Endpoint Security: Antivirus and Antimalware, Endpoint Detection and Response (EDR), Patch Management, Device Encryption.	**9**
2	**Application Security Controls:** Secure Software Development Lifecycle (SDLC), Code Review and Static Analysis, Web Application Firewalls (WAF), Database Security. Data Protection Controls: Data Classification and Handling, Data Loss Prevention (DLP), Encryption (At Rest, In Transit), Backup and Recovery.	**9**
3	**Identity and Access Management (IAM):** Identity Lifecycle Management, Single Sign-On (SSO), Federation and Trust Models, Privileged Access Management (PAM). **Security Monitoring and Incident Response:** Security Information and Event Management (SIEM), Threat Intelligence, Incident Response Planning, Forensics and Post-Incident Analysis	**9**
4	**Compliance and Regulatory Controls:** General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI DSS). Emerging Trends and Technologies: Zero Trust Architecture, Artificial Intelligence in Cyber Security, Block chain for Security, Quantum Computing Implications. Case Study: Analysis of Real-World Cyber security Incidents	**10**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)
Continuous Internal Evaluation Mark (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination-2 (Written)	Total
5	15	10	10	40

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Able to configure firewall rules and policies and identify different types of malwares.	**K2**
CO2	Integrate security practices into each phase of SDLC and apply the principles of encryption for data protection	**K3**
CO3	Design and implement Identity management processes and understand the role of SIEM systems in analyzing security events.	**K3**
CO4	Understand the compliance and regulatory controls and gain knowledge on emerging technologies related to industrial cyber security.	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓					✓	✓		
CO2	✓	✓	✓					✓	✓		
CO3	✓	✓	✓					✓	✓		
CO4	✓	✓	✓					✓	✓		

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Network Security Essentials: Applications and Standards.	William Stallings	Pearson	6th Edition, 2016
2	Network Intrusion Detection and Prevention: Concepts and Practices	Ali A Ghorbani, Wei Lu, Mahabod Tavallaee	Springer-Verlag New York Inc.	1st Edition, 2010
3	Malware Analyst's Cookbook and DVD: Tools and Techniques for fighting malicious code	Michael Ligh, Steven Adair, Blake Heartstein	Wiley	1st Edition, 2010
4	Software Security: Building Security	Gary McGraw	Addison-Wesley	1st Edition, 2006
5	Identity and Access Management: Business Performance through Connected Intelligence	Ertem Osmanoglu	Syngress	1st Edition, 2013
6	Zero Trust Networks: Building Secure systems in Untrusted Networks	Evan Gilman, Doug Barth	O'Reilly	1st Edition, 2017

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Web Application Security: Exploitation and Countermeasures for Modern Web Applications	Leslie F. Sikos	Orielly and Associates Inc.	2nd Edition, 2020
2	Security Information and Event Management Implementation	David Miller, Shon Harris, Allen Harper, Stephen Wandyke, Chris Blask	McGraw Hill Education	2nd Edition, 2010
3	Block chain Basics: A Non-Technical Introduction in 25 steps	Daniel Drescher	Apress	1st edition, 2017

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	http://www.digimat.in/nptel/courses/video/106105031/L40
2	https://nptel.ac.in/courses/128106006
3	https://onlinecourses.nptel.ac.in/noc24_cs85/preview
4	https://onlinecourses.nptel.ac.in/noc24_cs121/preview http://www.digimat.in/nptel/courses/video/106104220/L01.html

SEMESTER 5
SOFTWARE PROJECT MANAGEMENT
(Common CS/CA/AD/CC)

Course Code	**24SJPECST521**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. To learn the techniques to effectively plan, manage, execute, and control projects within time and cost targets with a focus on Information Technology and Service Sector.
2. To learn agile project management techniques such as Scrum and DevOps.

Module No.	**Syllabus Description**	**Contact Hours**
1	**Project scheduling and feasibility study: -** Project Overview and Feasibility Studies - Identification, Market and Demand Analysis, Project Cost Estimate, Financial Appraisal; Project Scheduling - Project Scheduling, Introduction to PERT and CPM, Critical Path Calculation, Precedence Relationship, Difference between PERT and CPM, Float Calculation and its importance, Cost reduction by Crashing of activity.	**8**
2	**Resource Scheduling, Cost Control and Project management Features:-** Cost Control and Scheduling - Project Cost Control (PERT/Cost), Resource Scheduling & Resource Levelling; Project Management Features – Risk Analysis, Project Control, Project Audit and Project Termination.	**8**
3	**Agile Project Management: -** Agile Project Management - Introduction, Agile Principles, Agile methodologies, Relationship between Agile Scrum, Lean, DevOps and IT Service Management (ITIL; Other Agile Methodologies - Introduction to XP, FDD, DSDM, Crystal.	**9**

4	**Scrum and DevOps in project management:-** Scrum - Various terminologies used in Scrum (Sprint, product backlog, sprint backlog, sprint review, retro perspective), various roles (Roles in Scrum), Best practices of Scrum, Case Study; DevOps- Overview and its Components, Containerization Using Docker, Managing Source Code and Automating Builds, Automated Testing and Test-Driven Development, Continuous Integration, Configuration Management, Continuous Deployment, Automated Monitoring, Case Study.	**11**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)
Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)
In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24 marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 subdivisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)
At the end of the course students should be able to:

Course Outcomes		Bloom's Knowledge Level (KL)
CO1	Understand how effectively plan, and schedule projects within time and cost targets	**K2**
CO2	Apply project estimation and evaluation techniques to real world problem	**K3**
CO3	Discuss different Agile Project Methodologies	**K2**
CO4	Apply various SCRUM practices in project management.	**K3**
CO5	Demonstrate the techniques used in DevOps.	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓							✓	✓
CO2	✓	✓	✓							✓	✓
CO3	✓	✓	✓							✓	✓
CO4	✓	✓	✓							✓	✓
CO5	✓	✓	✓							✓	✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Succeeding with Agile: Software Development Using Scrum	Mike Cohn	Addison-Wesley	1/e, 2009

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Agile Product Management with Scrum	Roman Pichler	Addison-Wesley	1/e, 2010
2	Agile Project Management with Scrum	Ken Schwaber	Microsoft Press	1/e, 2004

Video Links (NPTEL, SWAYAM…)	
No.	**Link ID**
1	https://archive.nptel.ac.in/noc/courses/noc19/SEM2/noc19-cs70/
2	https://www.youtube.com/watch?v=TPEgII1OilU
3	https://www.youtube.com/watch?v=7Bxdds2siU8

SEMESTER 5
DATA MINING
(Common to CS/CA/CC)

Course Code	**24SJPECST525**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:1	**ESE Marks**	60
Credits	5/3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. To provide a thorough understanding of the key processes and concepts involved in data mining and data warehousing within application domains.
2. To enable students to understand the different data pre-processing techniques, fundamentals and advanced concepts of classification, clustering, association rule mining, text mining and web mining, and apply these techniques in real-world scenarios

Module No.	Syllabus Description	Contact Hours
1	**Data Mining Fundamentals: -** Data Mining - concepts and applications, Knowledge Discovery in Database Vs Data mining, Architecture of typical data mining system, Data Mining Functionalities Data warehouse - Differences between Operational Database Systems and Data Warehouses, Multidimensional data model- Warehouse schema, OLAP Operations, Data Warehouse Architecture.	**8**
2	**Data Preprocessing: -** Data Preprocessing - Need of data preprocessing, Data Cleaning- Missing values, Noisy data, Data Integration and Transformation. Data Reduction - Data cube aggregation, Attribute subset selection, Dimensionality reduction, Numerosity reduction, Discretization and concept hierarchy generation.	**9**
3	**Classification And Clustering: -** Classification - Introduction, Decision tree construction principle, Information Gain, Gini index, Decision tree construction algorithm - ID3, Neural networks, back propagation, Rule-Based Algorithms - Generating Rules from a DT, Generating Rules from a Neural Net. Clustering - Introduction to clustering, distance measures, Clustering Paradigms, Partitioning Algorithm - k means, Hierarchical Clustering, DBSCAN	**9**

4	**Association Rule Analysis and Advanced Data Mining: -** Association Rule Mining - Concepts, Apriori algorithm, FP Growth Algorithm. Web Mining - Web Content Mining, Web Structure Mining- Page Rank, Web Usage Mining- Preprocessing, Data structures, Pattern Discovery, Pattern Analysis. Spatial Mining - Spatial Queries, Spatial Data Structures, Thematic Maps, Image Databases.	**10**

Criteria for Evaluation (Evaluate and Analyse): 20 marks

Students must be asked to identify problems involving large datasets and identify the right solution from the concepts already learned. A comparison of the results with a similar approach also needs to be performed to assess the Knowledge Level 5.

End Semester Examination Marks (ESE):

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24 marks)**	2 questions will be given from each module, out of which 1 question should be answered. Each question can have a maximum of 3 subdivisions. Each question carries 9 marks. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Understand the key process of data mining and data warehousing concepts in application domains.	**K2**
CO2	Apply appropriate pre-processing techniques to convert raw data into suitable format for practical data mining tasks	**K3**
CO3	Illustrate the use of classification and clustering algorithms in various application domains	**K3**
CO4	Comprehend the use of association rule mining techniques	**K3**
CO5	Explain advanced data mining concepts and their applications in emerging domains	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓									✓
CO2	✓	✓	✓	✓	✓						✓
CO3	✓	✓	✓	✓	✓						✓
CO4	✓	✓	✓	✓	✓						✓
CO5	✓	✓									✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Data Mining Concepts and Techniques	JaiweiHan, Micheline Kamber	Elsevier	3/e, 2006
2	Data Mining: Introductory and Advanced Topics	Dunham M H	Pearson Education	1/e, 2006

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Introduction to Data Mining	Pang-Ning Tan, Michael Steinbach	Addison Wesley	1/e, 2014
2	Data Mining: Concepts, Models, Methods, and Algorithms	Mehmed Kantardzic	Wiley	2/e, 2019

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://youtu.be/ykZ-_UGcYWg?si=qiqynQyjI1sNNiHE
2	https://youtu.be/NSxEiohAH5o?si=ZIJHMiRvpFcNQNMA
3	https://youtu.be/VsYKqOokgaE?si=rgndBZqpzB29LUGg
4	https://youtu.be/N_whCVtfL9M?si=VPMH9NP4vdAaiuPe

SEMESTER S6
COMPILER DESIGN
(Common to CS/CC)

Course Code	**24SJPCCST601**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:1:0:0	**ESE Marks**	60
Credits	4	**Exam Hours**	2 Hrs 30 Min.
Prerequisites (if any)	NA	**Course Type**	Theory

Course Objectives:

1. To provide a comprehensive understanding of the compiler construction process through its various phases viz. lexical analysis, parsing, semantic analysis, code generation, and optimization.
2. To introduce compiler construction tools like Lex and YACC and use them in lexical analysis and parsing.

Module No.	Syllabus Description	Contact Hours
1	Introduction - Compiler Structure, The Front End; The Optimizer; The Back End. Scanners - Recognizing Words, Regular Expressions, From Regular Expression to Scanner: Implementing Scanners. ***Hands-on:*** *Recognizing Words with Lex, Regular Expressions in Lex*	**8**
2	Parsing - Introduction, Expressing Syntax, Top-Down Parsing - Transforming A Grammar: Eliminating Left Recursion; Left- Factoring To Eliminate Backtracking, Recursive Descent Parsers, Table-Driven LL(1) Parsers	**10**
3	Bottom-Up Parsing - Shift Reduce Parser, The LR(1) Parsing Algorithm, Building LR(1) Tables, Errors in the Table Construction, Reducing the Size of LR (1) Tables. ***Hands-on:*** *Building a calculator with YACC* Intermediate Representations: An IR Taxonomy, Graphical IRs- Syntax-Related Trees, Graphs; Linear IRs, Three-Address Code. Syntax-Driven Translation: Introduction, Translating Expressions, Translating Control-Flow Statements	**14**
4	Code generation: Code Shape - Arithmetic Operators, Boolean and Relational Operators, Control-Flow Constructs (Conditional Execution, Loops and Iteration), Procedure Calls Code Optimization - Introduction, Opportunities for Optimization, Scope of Optimization Local Optimization: Local Value Numbering, Tree-Height Balancing Regional Optimization: Loop Unrolling Global Optimization: Finding Uninitialized Variables with Live Sets, Global Code Placement	**14**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)
Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	15	10	10	40

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24 marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 subdivisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Use lexical analysis techniques to build a scanner for a given language specification. (Cognitive Knowledge Level: Apply)	**K3**
CO2	Construct parse trees for input programs using parsing algorithms and detect syntactic errors. (Cognitive Knowledge Level: Apply)	**K3**
CO3	Develop semantic analysis techniques to check program correctness. (Cognitive Knowledge Level: Apply)	**K3**
CO4	Build intermediate code representations by applying intermediate code generation techniques. (Cognitive Knowledge Level: Apply)	**K3**
CO5	Optimize generated code using code optimization strategies to improve performance. (Cognitive Knowledge Level: Apply)	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓		✓						✓
CO2	✓	✓	✓		✓						✓
CO3	✓	✓	✓		✓						✓
CO4	✓	✓	✓		✓						✓
CO5	✓	✓	✓		✓						✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Engineering a Compiler	Keith D. Cooper, Linda Torczon	Elsevier Science	3/e, 2023
2	Lex and YACC	John R. Levine, Tony Mason, Doug Brown	O' Reily	2/e, 1992

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Compilers – Principles Techniques and Tools	Aho A.V., Ravi Sethi and D. Ullman.	Addison Wesley,	2/e, 2010.
2	Compiler Construction - Principles and Practice	Kenneth C Louden	Thomson Learning	1/e, 2007
3	Compiler Design in C	Allen Holub	Prentice-Hall software series	1/e, 1990
4	Modern Compiler Implementation in C	Andrew W. Appel	Cambridge University Press	2/e, 2004

SEMESTER S6
CYBER FORENSICS

Course Code	**24SJPCCCT602**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. To understand about Computer Forensics and the procedures for investigations and incident response.
2. To study about data acquisition and to have an understanding of different forensic acquisition tools.
3. To explore the various cyber threats, attacks and the different anti forensic techniques.
4. To study the theory behind Network Forensics, Mobile Forensics and various types of Forensics.

Module No.	**Syllabus Description**	**Contact Hours**
1	**Cyber Forensics and Investigations:** Introduction- Computer Forensic Investigations - Forensics Investigation Process -Preparing for computer investigations, understanding Public and private investigations. Data Acquisition - storage formats for digital evidence, determining the best acquisition method -Forensic Protocol for Evidence Acquisition - Digital Forensics Standards and Guidelines – Incident Response stages -Digital Evidence – identification, collection, processing, seizing documenting and storing - contingency planning for image acquisitions.	**9**
2	**Cyber Forensics Tools and Types of Forensics:** **Cyber Forensics Tools**-Computer Forensics software and hardware tools - Open Source and Proprietary -Challenges in Cyber Forensics, Skills Required to Become a Cyber Forensic Expert Physical Requirements of a Cyber forensics Lab, Types of Cyber forensics. **File System Forensics**-Working with windows and CLI systems- file systems, exploring Microsoft file structures, examining FAT and NTFS disks, whole disk encryption, the windows registry, Microsoft start up tasks- Windows7, Windows 8, Windows 10- Examining UNIX and LINUX disk structures and boot processes, understanding Disk drives, Solid State storage devices.	**9**

3	**OS and Network Forensics** Windows Forensics-Live Response: Data Collection- Introduction, Locard's Exchange Principle, Order of Volatility - Volatile and Non Volatile Data Live-Response Methodologies: Data Analysis, Windows Memory Analysis, Rootkits and Rootkit detection. Linux Forensics: Live Response- Data Collection- Data Analysis- Log Analysis, Keyword Searches, User Activity, Network Connections, Running Processes, Open File Handlers, The Hacking Top Ten and Reconnaissance Tools. Network Forensics: The OSI Model, Forensic Footprints, Seizure of Networking Devices, Network Forensic Artifacts, ICMP Attacks, Drive-By Downloads, Network Forensic Analysis Tools, Network Log analysis, Case Study: Wireshark. Web Attack Forensics: OWASP Top 10, Web Attack Tests, Penetration Testing. Mobile Device Forensics and Internet of Anything- Cloud Forensics.	**9**
4	**Cyber Security and Anti Forensics** **Cyber Security**: Cybercrimes, Types of Cybercrimes –Cyber Security Steps taken to protect ICT and prevent Misuse of Internet- IT Act 2000 and amendments- Email and Social Media Investigations-. Cyber Technology- Technological/Governance/Judicial/Legal Aspects and perspectives of Cyber Forensics/Security. Cyber-attack Frameworks- Mitre Framework-Crypto currency. **Anti-Forensics** Anti-forensic Practices - Data Wiping and Shredding- Data Remanence, Degaussing, Case Study: USB Oblivion, Eraser - Trail Obfuscation: Spoofing, Data Modification, Case Study: Timestamp – Encryption, Case Study: VeraCrypt, Anti-forensics Detection Techniques	**9**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination-2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Explain the basic concepts in cyber forensics, forensics Investigation Process and the usage of Cyber Forensics Tools in investigations	**K2**
CO2	Infer the basic concepts of file systems, its associated attribute definitions	**K2**
CO3	Utilize the methodologies used in memory analysis and network analysis for detection of artifacts	**K3**
CO4	Explain the basic concepts in cyber security and study the essence of IT Act.	**K2**
CO5	Summarize anti forensics practices and data hiding methods.	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓				✓					✓
CO2	✓	✓									✓
CO3	✓	✓	✓	✓	✓						✓
CO4	✓	✓	✓	✓	✓						✓
CO5	✓	✓			✓						✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Guide to computer forensics and investigations	Bill Nelson, Amelia Philipps and Christopher Steuart	Cengage	6th Edition 2020
2	File System Forensic Analysis	Brian Carrier	Pearson Education, Inc.	1st Edition,2005
3	Windows Forensic Analysis DVD Toolkit	Harlan Carvey	Syngress	2nd Edition,2009
4	Unix and Linux Forensic Analysis DVD Toolkit	Chris Pogue, Cory Altheide, Tode Haverkos	Syngress	1st Edition,2008
5	Fundamentals of Network Security	E. Maiwald	McGraw-Hill	1st Edition, 2017
6	Network Security Essentials Applications and Standards	William Stallings	Pearson Education	6th Edition, 2018

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
I	Information Security and Cyber Forensics-- NPTEL/SWAYAM By Prof. Pratosh Bansal | Devi Ahilya Vishwavidyalaya, Indore
II/III	Digital Forensics-- NPTEL/SWAYAM By Dr. Jeetendra Pande | Uttarakhand Open University, Haldwani
IV	Cyber Security and Privacy By Prof. Saji K Mathew | IIT Madras

SEMESTER S6
ETHICAL HACKING AND IOT SECURITY

Course Code	**24SJPBCCT604**	**CIE Marks**	60
Teaching Hours/Week (L: T:P: R)	3:0:0:1	**ESE Marks**	40
Credits	4	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. To learn ethical hacking and security challenges in computer networking.
2. To protect the network system using firewalls and filters, about the legal, professional and ethical issues.

Module No.	**Syllabus Description**	**Contact Hours**
1	Definition of Ethical Hacking, Phases, Effects of Hacking, Hacker – Types of Hacker, Ethical Hacker, Role of Security and Penetration Tester, Penetration Testing Methodologies – OSSTMM, NIST, OWASP, Categories of Penetration Test, Types of Penetration Tests, Vulnerability Assessment. Tools for Foot Printing, Conducting Competitive Intelligence, Google Hacking, Scanning, Enumeration, Trojans & Backdoors, Virus & Worms, Proxy & Packet Filtering, Denial of Service, Social Engineering Attacks – Shoulder Surfing, Dumpster Diving, Piggybacking.	**11**
2	Vulnerability Data Resources – Exploit Databases – Network Sniffing – Types of Sniffing – MITM Attacks – ARP Attacks – Denial of Service Attacks – Hijacking Session with MITM Attack – DNS Spoofing – ARP Spoofing Attack Manipulating the DNS Records – DHCP Spoofing – Remote Exploitation – Attacking Network Remote Services – Brute Force Attacks – Types, Hydra Tool – Attacking SQL – Network Protection Systems: Routers to Reduce Network Attacks, Protecting with Firewalls, Protecting with Intrusion Detection and Prevention Systems, Using Honeypots – Vulnerability, Penetration Testing, Session Hijacking, Web Server, SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobile Phone Hacking. Servers – Testing for Weak Authentication. Routers, Firewall & Honey pots, IDS &IPS, Web Filtering, Vulnerability, Penetration Testing, Session Hijacking, Web Server, SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobiles, Phone Hacking.	**11**

3	What is IoT, Genesis of IoT, IoT and Digitization, IoT Impact, Convergence of IT and IoT, IoT Challenges, IoT Network Architecture and Design, Drivers Behind New Network Architectures, Comparing IoT Architectures, A Simplified IoT Architecture, The Core IoT Functional Stack, IoT Data Management and Compute Stack. Smart Objects: The "Things" in IoT, Sensors, Actuators, and Smart Objects, Sensor Networks, Connecting Smart Objects, Communications Criteria, IoT Access Technologies. IP as the IoT Network Layer, The Business Case for IP, The need for Optimization, Optimizing IP for IoT, Profiles and Compliances, Application Protocols for IoT, The Transport Layer, IoT Application Transport Methods.	**11**
4	Data and Analytics for IoT, An Introduction to Data Analytics for IoT, Machine Learning, Big Data Analytics Tools and Technology, Edge Streaming Analytics, Network Analytics, Securing IoT, A Brief History of OT Security, Common Challenges in OT Security, Differences between IT and OT Security Practices and Systems, Formal Risk Analysis Structures: OCTAVE and FAIR.	**11**

Course Assessment Method (CIE: 60 marks, ESE: 40 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Project	Internal Ex-1	Internal Ex-2	Total
5	**30**	**12.5**	**12.5**	**60**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 2 marks **(8x2 =16 marks)**	• 2 questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 2 sub divisions. • Each question carries 6 marks. **(4x6 = 24 marks)**	**40**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Explain the basic concepts of Ethical hacking	**K2**
CO2	Utilize the tools to conduct competitive intelligence and social engineering.	**K3**
CO3	Appreciate the security considerations in IoT.	**K2**
CO4	Outline the fundamentals of IoT and its underlying physical and logical architecture	**K2**
CO5	Implement IoT applications using the available hardware and software.	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓									✓
CO2	✓	✓									✓
CO3	✓	✓									✓
CO4	✓	✓									✓
CO5	✓	✓	✓	✓	✓						✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	"Hands on ethical hacking and network defense", Cengage Learning.	Michael T Simpson, Kent Back man, James Corley		2nd edition, 2010
2	"Ethical Hacking and Penetration Testing Guide"	Rafay Baloch	CRC Press	2014.
3	"Internet of Things: A hands-on approach"	Arshadeep Bahga, Vijay Madisetti,	University Press	2015 (First edition)

4	Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems,	Dr. Ovidiu Vermesan, Dr. Peter Friess	River Publishers	2013

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	"Certified Ethical Hacker: A Study Guide", Wiley Publishing, Inc., 2010.	Kimberly Graves,	Wiley Publishing, Inc.	2010
2	"Hacking Exposed 7 :Network Security Secrets & Solutions"	Stuart Mc Clure, Joel Scambray,	McGraw-Hill publishing,	edition 7, 2012
3	"IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things"	David Hanes, Gonzalo Salgueiro, Patrick rossetete, Robert Barton, Jerome Henry ,	Pearson Education	1st Edition
4	"Internet of Things: Architecture and Design Principles"	Rajkamal	McGraw Hill (India) Private Limited	

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://www.youtube.com/watch?v=fNzpcB7ODxQ
2	https://www.youtube.com/@HackerSploit
3	https://www.youtube.com/watch?v=7zWVxrjjIpE
4	https://www.youtube.com/playlist?list=PL1ljc761XCiaTRgucelgZS8pbTEyt1BjX

PBL Course Elements

L: Lecture (3 Hrs.)	R: Project (1 Hr.), 2 Faculty Members		
	Tutorial	**Practical**	**Presentation**
Lecture delivery	Project identification	Simulation/ Laboratory Work/ Workshops	Presentation (Progress and Final Presentations)
Group discussion	Project Analysis	Data Collection	Evaluation
Question answer Sessions/ Brainstorming Sessions	Analytical thinking and self-learning	Testing	Project Milestone Reviews, Feedback, Project reformation (If required)
Guest Speakers (Industry Experts)	Case Study/ Field Survey Report	Prototyping	Poster Presentation/ Video Presentation: Students present their results in a 2 to 5 minutes video

Assessment and Evaluation for Project Activity

Sl. No	Evaluation for	Allotted Marks
1	Project Planning and Proposal	5
2	Contribution in Progress Presentations and Question Answer Sessions	4
3	Involvement in the project work and Team Work	3
4	Execution and Implementation	10
5	Final Presentations	5
6	Project Quality, Innovation and Creativity	3
Total		**30**

1. Project Planning and Proposal (5 Marks)

- Clarity and feasibility of the project plan
- Research and background understanding
- Defined objectives and methodology

2. Contribution in Progress Presentation and Question Answer Sessions (4 Marks)

- Individual contribution to the presentation
- Effectiveness in answering questions and handling feedback

3. Involvement in the Project Work and Team Work (3 Marks)

- Active participation and individual contribution
- Teamwork and collaboration

4. Execution and Implementation (10 Marks)

- Adherence to the project timeline and milestones
- Application of theoretical knowledge and problem-solving
- Final Result

5. Final Presentation (5 Marks)

- Quality and clarity of the overall presentation
- Individual contribution to the presentation
- Effectiveness in answering questions

6. Project Quality, Innovation, and Creativity (3 Marks)

- Overall quality and technical excellence of the project
- Innovation and originality in the project
- Creativity in solutions and approaches

SEMESTER S6
CYBER FORENSIC LAB

Course Code	**24SJPCCCL607**	**CIE Marks**	50
Teaching Hours/Week (L: T:P: R)	0:0:3:0	**ESE Marks**	50
Credits	2	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	24SJPCCCT602	**Course Type**	Lab

Course Objectives:

1. The course aims to master Cyber Forensics procedures and get hands-on exposure to different Cyber Forensics tools.
2. The course aims to offer hands-on experience on integrity check of files and use it for security implementations.
3. The course aims to offer exposure to live and static forensic analysis.

A minimum of nine experiments must be completed as part of the course requirements.

Expt. No.	Experiments
1	Registry Viewing and Editing using native tools of Operating Systems.
2	Hex analysis using Hex Workshop tool Using Hex Workshop perform file signature analysis. Write down the hex values of popular file types
3	Familiarization with Bit-level Forensic Analysis of Evidential Image using FTK / Encase / ProDiscover Tools Image Acquisition and perform static analysis to mount an image of a drive.
4	Hash code generation, comparison of files using tools like HashCalc Using HashCalc write down the Hash values of popular hashing algorithms.
5	Command line Analysis of disk images using The SleuthKit(TSK) tool
6	File System Forensic Analysis using Autopsy tool. Using Autopsy perform file signature analysis. Write down the investigation report.
7	Network Protocol Analysis and Security Scanning using Nmap
8	Live Forensics and Memory Dump Analysis using LiME and Volatility Framework
9	Network Log analysis

Course Assessment Method (CIE: 50 marks, ESE: 50 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Preparation/Pre-Lab Work experiments, Viva and Timely completion of Lab Reports / Record (Continuous Assessment)	Internal Examination	Total
5	25	20	50

Note: Students are instructed to submit only the fair record for both Continuous Internal Evaluation (CIE) and End Semester Examination (ESE). Rough records are not required.

End Semester Examination Marks (ESE):

Procedure/ Preparatory work/Design/ Algorithm	Conduct of experiment/ Execution of work/ troubleshooting/ Programming	Result with valid inference/ Quality of Output	Viva voce	Record	Total
10	15	10	10	5	50

- ***Submission of Record: Students shall be allowed for the end semester examination only upon submitting the duly certified record.***
- ***Endorsement by External Examiner:*** *The external examiner shall endorse the record*

Course Outcomes (COs)

At the end of the course students should be able to:

	Course Outcome	Bloom's Knowledge Level (KL)
CO1	Use the Windows Registry and Registry Editor.	**K3**
CO2	Use the different Cyber Forensics Tools for static and dynamic forensics analysis.	**K3**
CO3	Familiarize file signature analysis and applications.	**K3**
CO4	Use FTK or Encase or ProDiscover tools for bit level forensic analysis of evidential image.	**K3**
CO5	Prepare an investigation report following the chain of custody.	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO- PO Mapping (Mapping of Course Outcomes with Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓									
CO2	✓	✓									
CO3	✓	✓									
CO4	✓	✓									
CO5	✓	✓			✓						

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Guide to computer forensics and investigations	Bill Nelson, Amelia Philipps and Christopher Steuart	Cengage	6th Editio n 2020
2	Windows Forensic Analysis DVD Toolkit	Harlan Carvey	Syngress	2nd Edition,2009
3	Unix and Linux Forensic Analysis DVD Toolkit	Chris Pogue, Cory Altheide, Tode Haverkos	Syngress	1st Edition,2008

Continuous Assessment (25 Marks)

1. **Preparation and Pre-Lab Work (7 Marks)**

   - Pre-Lab Assignments: Assessment of pre-lab assignments or quizzes that test understanding of the upcoming experiment.
   - Understanding of Theory: Evaluation based on students' preparation and understanding of the theoretical background related to the experiments.

2. **Conduct of Experiments (7 Marks)**

   - Procedure and Execution: Adherence to correct procedures, accurate execution of experiments, and following safety protocols.
   - Skill Proficiency: Proficiency in handling equipment, accuracy in observations, and troubleshooting skills during the experiments.
   - Teamwork: Collaboration and participation in group experiments.

3. **Lab Reports and Record Keeping (6 Marks)**

   - Quality of Reports: Clarity, completeness and accuracy of lab reports. Proper documentation of experiments, data analysis and conclusions.
   - Timely Submission: Adhering to deadlines for submitting lab reports/rough record and maintaining a well-organized fair record.

4. **Viva Voce (5 Marks)**

   - Oral Examination: Ability to explain the experiment, results and underlying principles during a viva voce session.

Final Marks Averaging: The final marks for preparation, conduct of experiments, viva, and record are the average of all the specified experiments in the syllabus.

Evaluation Pattern for End Semester Examination (50 Marks)

1. **Procedure/Preliminary Work/Design/Algorithm (10 Marks)**

   - Procedure Understanding and Description: Clarity in explaining the procedure and understanding each step involved.
   - Preliminary Work and Planning: Thoroughness in planning and organizing materials/equipment.
   - Algorithm Development: Correctness and efficiency of the algorithm related to the experiment.
   - Creativity and logic in algorithm or experimental design.

2. **Conduct of Experiment/Execution of Work/Programming (15 Marks)**

   - Setup and Execution: Proper setup and accurate execution of the experiment or programming task.

3. **Result with Valid Inference/Quality of Output (10 Marks)**
   - Accuracy of Results: Precision and correctness of the obtained results.
   - Analysis and Interpretation: Validity of inferences drawn from the experiment or quality of program output.

4. **Viva Voce (10 Marks)**
   - Ability to explain the experiment, procedure results and answer related questions
   - Proficiency in answering questions related to theoretical and practical aspects of the subject.

5. **Record (5 Marks)**
   - Completeness, clarity, and accuracy of the lab record submitted

SEMESTER 6
MINI PROJECT: Socially Relevant Project

Course Code	**24SJPCCSP608**	**CIE Marks**	50
Teaching Hours/Week (L: T:P: R)	0:0:0:3	**ESE Marks**	50
Credits	2	**Exam Hours**	
Prerequisites (if any)	None	**Course Type**	Project

Preamble: The objective of this course is to apply the fundamental concepts of Artificial Intelligence / Machine Learning principles for the effective development of an application/research project. Mini project enables the students to boost their skills, widen the horizon of thinking and their ability to resolve real life problems. The students are expected to design and develop a software/hardware project to innovatively solve a real-world problem.

Course Outcomes: After the completion of the course the student will be able to

CO#	Course Outcomes
CO1	Identify technically and economically feasible problems of social relevance **(Cognitive Knowledge Level: Apply)**
CO2	Identify and survey the relevant literature for getting exposed to related solutions **(Cognitive Knowledge Level: Apply)**
CO3	Perform requirement analysis and identify design methodologies and develop adaptable and reusable solutions of minimal complexity by using modern tools and advanced programming techniques (**Cognitive Knowledge Level: Apply)**
CO4	Prepare technical report and deliver presentation **(Cognitive Knowledge Level: Apply)**
CO5	Apply engineering and management principles to achieve the goal of the project **(Cognitive Knowledge Level: Apply)**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
CO2	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
CO3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CO4	✓	✓	✓	✓	✓			✓	✓	✓	✓
CO5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Split-up of Continuous Internal Evaluation: 50 Marks

Attendance	**05 marks**
Project Guide	**15 marks**
Project Report	**10 marks**
Evaluation by the Committee	**20 marks**
Total	**50 marks**

(Will be evaluating the level of completion and completion of Functionality /specifications, presentation, oral examination, work knowledge and involvement)

Split-up of End Semester Examination: 50 Marks

The marks will be distributed as

Presentation marks	: 20
Demonstration	: 20 marks
Viva	: 10 marks.
Total	**: 50 marks.**

Course Plan

Student Groups with 3 or 4 members should identify a topic of interest (Socially relevant) in consultation with Project Coordinator/Guide. Review the literature and gather information pertaining to the chosen topic. State the objectives and develop a methodology to achieve the objectives. Carryout the design/fabrication or develop codes/programs to achieve the objectives. Innovative design concepts, performance, scalability, reliability considerations, aesthetics/ergonomic, user experience and security aspects taken care of in the project shall be given due weight.

The progress of the mini project is evaluated based on a minimum of two reviews. The review committee may be constituted with the Head of the Department or a senior faculty, Mini Project coordinator and project guide as the members. Innovative design concepts, reliability considerations, aesthetics/ergonomic aspects taken care of in the project shall be given due weight. The internal evaluation shall be made based on the progress/outcome of the project, reports and a viva-voce examination, conducted internally by a 3-member committee. A project report is required at the end of the semester. The product/application has to be demonstrated for its full design specifications.

Guidelines for the Report preparation

A bonafide report on mini project shall be submitted within one week after the final presentation. Minimum number of pages should be 30.

- Use Times New Roman font for the entire Report – Chapter / Section Title –Times New Roman 18, Bold; Heading 2 – Times New Roman 16, Bold; Heading 3 –

Times New Roman 14, Bold; Body- Times New Roman12, Normal.

- Line Spacing – Between Heading 2 – 3 lines, between lines in paragraph 1.5 lines.
- Alignments – Chapter / Section Title – Center, heading 2 & 3 should be Left Aligned. Ensure that all body text is paragraph justified.
- Figures & Tables – Ensure that all Figures and Tables are suitably numbered and given proper names/headings. Write figure title under the figure and table title above the table
- Suggestive order of documentation:
  i. Top Cover
  ii. Title page
  iii. Certification page
  iv. Acknowledgement
  v. Abstract
  vi. Table of Contents
  vii. List of Figures and Tables
  viii. Chapters
  ix. Appendices, if any
  x. References/Bibliography

PROGRAM ELECTIVE 3: 24SJPECCT63N

SEMESTER S6
CLOUD INFRASTRUCTRE AND SYSTEMS

Course Code	**24SJPECCT631**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. To provide students with a comprehensive understanding of cloud computing concepts and infrastructure.
2. To explore various cloud service models and deployment models.
3. To understand the security challenges and solutions in cloud computing environments.

Module No.	Syllabus Description	Contact Hours
1	**Traditional computing**: Limitations, Overview of Computing Paradigms: Grid Computing, Cluster Computing, Distributed Computing, Utility Computing, Cloud Computing, NIST reference Model, Basic terminology and concepts, Cloud characteristics, benefits and challenges, **Cloud delivery (service) models**: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as a- Service (SaaS), XaaS (Anything- as-a-service), Cloud deployment models: Public cloud, Community cloud, Private cloud, Hybrid cloud, Open Cloud Services.	**9**
2	Basic Terms and Concepts in Security, Threat Agents, Cloud Security Threats, Identity Management and Access Control, Cloud Security Working Groups, Elements of Cloud Security Model, Cloud Security Reference Model, Examining Cloud Security against Traditional Computing	**9**
3	Introduction to AWS, AWS history, AWS global Infrastructure, AWS Services, AWS Security Challenges, AWS ecosystem, Security Challenges and Services of Azure and Google Cloud, Comparison of AWS, Azure and Google cloud	**9**
4	Security Management in the Cloud Security Management Standards, Security Management in the Cloud, Availability Management: SaaS, PaaS, IaaS, Privacy Issues, Data Life Cycle, Key Privacy Concerns in the Cloud, Protecting Privacy, Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing, Legal and Regulatory Implications	**9**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	15	10	10	40

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	To provide students with a comprehensive understanding of cloud computing concepts and infrastructure	**K2**
CO2	To explore various cloud service models and deployment models	**K2**
CO3	To understand the security challenges and solutions in cloud computing environments	**K2**
CO4	To understand fundamental of Identity and Access Management and compliance	**K2**
CO5	Identify the industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyze, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓									✓
CO2	✓	✓	✓								✓
CO3	✓	✓									✓
CO4	✓	✓	✓	✓	✓						✓
CO5	✓	✓			✓						✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Cloud computing	Bhowmik, S.	Cambridge University Press, 2017	First edition ,2017
2	Cloud Computing Concepts, Technology & Architecture	Thomas, E., Zaigham, M., Ricardo, P	Prentice Hall,	First Edition,2013
3	Cloud Security: A Comprehensive Guide to Secure Cloud Computing	Ronald L. Krutz, Russell Dean Vines	Wiley Publishing, 2010	First edition ,2010
4	Cloud Security and Privacy	Tim Mather, SubraKumaraswamy, and ShahedLatif	O'Reilly Media, Inc., 2009	First edition 2009
5	Architecting Cloud Computing Solutions	Kevin L. Jackson, Scott Goessling	Packt Publishing	2021
6	Cloud Security Handbook	Eyal Estrin	Packt Publishing	2021
7	Learning AWS, Azure, and GCP	Manoj Reddy, Michael Washam	Packt Publishing	2022
8	Cloud Security and Compliance: A Practical Guide	Ben Potter, Scott Ward	O'Reilly Media	2021

SEMESTER S6
CRYPTOGRAPHIC ALGORITHMS IN BLOCKCHAIN

Course Code	**24SJPECCT632**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	24SJPECCT412	**Course Type**	Theory

Course Objectives:

1. To understand building blocks of Blockchain.
2. The course introduces the cryptographic principles behind blockchain

Module No.	**Syllabus Description**	**Contact Hours**
1	**Foundations of Blockchain** Blockchain Architecture –Challenges –Applications –Blockchain Design Principles -The Blockchain Ecosystem - The consensus problem - Asynchronous Byzantine Agreement - AAP protocol and its analysis - peer-to-peer network – Abstract Models - GARAY model - RLA Model-Proof of Work (PoW) -Proof of Stake (PoS) based Chains - Hybrid models.	7
2	**Fundamentals of Cryptography** Introduction to Cryptography, Symmetric cryptography – AES. Asymmetric cryptography – RSA. Elliptic curve cryptography, Digital signatures – RSA digital signature algorithms. Secure Hash Algorithms – SHA-256. Applications of cryptographic hash functions – Merkle trees, Distributed hash tables.	7
3	**Crypto Primitives, Securing and Interconnecting Public and Private Block Chains** Hash Function and Merle Tree-Security Properties- Security Considerations for b l o c k c h a i n Digital Signature-Public Key Cryptography-Bitcoin blockchain incentive structures- Nash Equilibriums- evolutionary stable strategies, -and Pareto efficiency (game theory) Weaknesses and news Points of Failure, Mitigation Methods, Redundancies and fallback methods.	7
4	**Blockchain Protocols** Ethereum tokens –Augur -Golem -Understanding Ethereum tokens -App Coins and Protocol Tokens - Blockchain Token Securities Law Framework - Token Economy - Token sale structure - Ethereum Subreddit.	6

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)
Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination-2 (Written)	Total
5	15	10	10	40

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Understand Blockchain ecosystem and its services in real world sceneries.	**K2**
CO2	Distinguish between Symmetric cryptography and asymmetric cryptography.	**K2**
CO3	Explain the working of AES algorithm.	**K2**
CO4	Understanding the methods for Securing and Interconnecting Public and Private Block Chains	**K2**
CO5	Acquaint the protocol and assess their computational requirements	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyze, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓		✓	✓						✓
CO2	✓	✓		✓	✓				✓		✓
CO3	✓	✓		✓	✓				✓		✓
CO4	✓	✓		✓	✓				✓		✓
CO5	✓	✓		✓	✓			✓			✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Blockchain enabled applications	Dhillon, V., Metcalf, D., and Hooper, M	CA: Apress, Berkeley	1st Edition, 2017
2	Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more	Imran Bashir	Packt Publishing	Third edition, 2020

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Blockchains, digital assets, smart contracts, decentralized autonomous organizations	Diedrich, H. Ethereum	Wildfire publishing, Sydney.	1st Edition, 2016
2	Blockchain Technology: Concepts and Applications	Kumar Saurabh, Ashutosh Saxena	Wiley Publications	1st Edition,2020
3	Blockchain Technology	Chandramouli Subramanian, Asha A, George, et al	Universities Press (India) Pvt. Ltd	First edition, August 2020
4	Distributed Ledger Technology: The Science of the Blockchain	Wattenhofer, R. P	Create space Independent Pub, Scotts Valley, California, US.	2nd Edition

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://youtu.be/mzPoUjQC4WU
2	https://youtu.be/LjEZzYe5uOo?feature=shared
3	https://youtu.be/3FnEwnOpo_k?feature=shared
4	https://youtu.be/v1MSq7m7lzA?feature=shared

SEMESTER S6
AI AND ML IN CYBER SECURITY DEFENSE

Course Code	**24SJPECCT633**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	24SJPECCT413 Introduction to AI and ML 24SJPECCT523 AI in Cyber Security	**Course Type**	Theory

Course Objectives:

1. To provide students with a comprehensive understanding of the importance, challenges, and promises of AI in the cybersecurity landscape.

2. To familiarize students with various machine learning techniques and their applications within the cybersecurity domain, including anomaly detection and intrusion detection.

3. To introduce students to generative AI concepts, algorithms, and models, and explore them applications in cybersecurity, including threat detection and incident response.

4. To equip students with the knowledge to identify potential security risks associated with AI and generative AI, and to develop best practices for securing AI systems in cybersecurity.

Module No.	Syllabus Description	Contact Hours
1	**Introduction: Role of AI in Cyber Security and Security Framework** Review of Artificial Intelligence in Cyber Security: Definition and Importance, Challenges and promises, Security Threats of Artificial Intelligence: Types and Examples **Machine Learning in Cyber Security** Introduction to Machine Learning: Concepts and Terminology, Applications of Machine Learning in the Cyber Security Domain, Machine Learning Tasks and Approaches: Supervised vs. Unsupervised Learning Anomaly Detection Techniques in Cybersecurity, Privacy Preserving Nearest Neighbour Search; Techniques and Applications, Machine Learning Applied to Intrusion Detection	**8**
2	**Fundamentals of Generative AI:** Concepts, Algorithms, and Models; Generative AI Techniques: Variational Autoencoders (VAEs), Generative Adversarial Networks (GANs), Transformer-Based Models Applications of Generative AI in Various Domains: Text Generation, Image Synthesis Case Study: Successful Generative AI Applications and their Impact	**10**
3	**Generative AI for Cybersecurity** **Overview of Cybersecurity Challenges and the Potential of Generative AI**: Applications of Generative AI in Cybersecurity; Anomaly Detection, Threat Hunting, Vulnerability Analysis Generative AI for Automated Incident Response and Mitigation Case Study: Generative AI in Real-World Cybersecurity Scenarios **Generative AI Security Risks and Challenges** Potential Security Risks Associated with Generative AI: Data Poisoning, Model Inversion, Adversarial Attacks,	**9**

4	**Overview of Generative AI Applications in Cybersecurity Defence:** Predictive Analytics for Threat Detection Using Generative AI, Automated Security Patch Generation and Vulnerability Management, Strengthening Encryption Protocols Case Study: Real-World Applications of Generative AI in Cybersecurity defence, Best Practices for Securing Generative AI Systems, Future Trends in Generative AI for Cybersecurity defence	**9**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Mark (CIE):

Attendance	Assignment/ Microproject	Internal Examination- 1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	To explain the significance of AI in cybersecurity, including its challenges and potential threats.	**K2**
CO2	To identify and apply machine learning techniques relevant to cybersecurity tasks, such as anomaly detection and intrusion detection.	**K3**
CO3	To evaluate the effectiveness of generative AI techniques in addressing cybersecurity challenges, including incident response and threat mitigation.	**K4**
CO4	To assess security risks related to AI systems and propose best practices for securing generative AI applications in cybersecurity.	**K4**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓								
CO2	✓	✓	✓								
CO3	✓	✓	✓								
CO4	✓	✓	✓					✓			

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Artificial Intelligence in Cyber Security: Theories and Applications	Himanshu Upadhyay, Steven Lawrence Fernandes, Tarun Kumar Sharma, Tushar Bhardwaj	Springer International Publishing	2023
2	Artificial Intelligence in Cyber Security.	Rahul Neware Khaja Mannanuddin, Mukesh Madanan, Dr. Shikha Gupta	Book Rivers	2022

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Hands-on Artificial Intelligence for Cybersecurity	Alessandro Parisi	Packt Publishing	2022
2	Artificial Intelligence for Cybersecurity: Techniques, Challenges and Research	Mark Stamp	Springer International Publishing	2022
3	Generative AI for Cybersecurity	Edited Volume	Springer	2023

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://www.youtube.com/watch?v=fC7V8QsPBec
2	https://www.youtube.com/watch?v=oJlb4jBbKWw

SEMESTER S6
OT THREAT PREVENTION

Course Code	**24SJPECCT634**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	Fundamentals and advanced Industrial Cyber Security	**Course Type**	Theory

Course Objectives:

1. Enables the learners to understand the Distinctions and Integration of OT and IT Systems and helps the students to identify the difference between OT and IT networks in Industrial Systems.
2. Enables the students to identify and classify OT Assets based on criticality.
3. Enables the learners to implement Access Control and Secure Network Access.
4. Enables the learners to monitor, analyze, and respond to Threats and Vulnerabilities

SYLLABUS

Module No.	**Syllabus Description**	**Contact Hours**
1	**Understanding OT and IT Systems** **Overview of OT and IT Systems:** Defining Operational Technology (OT) and Information Technology (IT), Key differences between OT and IT in terms of architecture, functionality, and security, Independent OT networks: Architecture, use cases, and benefits. **Integration of OT with IT Networks:** Drivers for OT-IT convergence, Challenges in integrating OT with IT networks, Common architectures for OT-IT integration	**9**
2	**Asset Identification and Criticality Classification: Identifying OT Assets:** Techniques for asset discovery in OT environments, Importance of maintaining an up-to-date asset inventory, Tools and technologies for OT asset identification **Criticality Classification:** Criteria for classifying OT assets based on criticality, Impact analysis of OT asset failure on overall operations, Prioritizing security efforts based on asset criticality **Risk Management and Compliance:** Applying risk management frameworks in integrated networks, Compliance considerations in OT-IT integration, Standards and best practices (e.g., NIST, IEC 62443)	**10**

3	**Securing Access and Dynamic Network Segmentation:** **Securing Wired and Wireless Access:** Best practices for securing wired access in OT-IT networks, Wireless security protocols and their application in OT environments, Managing and securing remote access in integrated networks **Dynamic Network Segmentation:** Concepts of network segmentation and micro-segmentation, Implementing dynamic network segmentation in OT-IT environments. **Monitoring and Threat Detection:** Importance of continuous monitoring in integrated OT-IT networks, Tools and techniques for monitoring OT and IT systems.	**12**
4	**Analyzing Threats and Vulnerabilities:** Techniques for analyzing security data from integrated networks, Vulnerability management and patching in OT-IT systems, Incident detection and analysis for OT-IT integrated environments. **Incident Response and Recovery:** Developing incident response plans specific to OT-IT integration, Threat hunting and proactive security measures, Recovery strategies and business continuity planning for integrated networks.	**10**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)
Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)
In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Differentiate Between OT and IT Systems and Understand Their Integration.	**K2**
CO2	Identify, Inventory, and Classify OT Assets Based on Criticality.	**K2**
CO3	Implement Effective Access Control and Secure Network Access Mechanisms.	**K3**
CO4	Deploy Continuous Monitoring and Advanced Threat Detection Systems.	**K3**
CO5	Develop and Execute Comprehensive Incident Response and Recovery Plans.	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓	✓		✓		✓	✓		✓
CO2	✓	✓	✓	✓	✓	✓		✓	✓		✓
CO3	✓	✓	✓	✓	✓	✓			✓	✓	✓
CO4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CO5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Practical Industrial Cybersecurity: ICS, OT, and IIoT	Philip A. Craig	Delmar Cengage Learning	Thomson 2nd edition, 2013
2	Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS	Tyson Macaulay, Bryan L. Singer	CRC Press	Ist edition, 2012
3	Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure	Eric D. Knapp, Raj Samani	Syngress	Ist edition, 2013
4	Industrial Network Security : Securing Critical Infrastructure Networks for Smart Grid, SCADA and other Industrial Control Systems	Eric D Knapp Joel Thomas Langill	Syngress	2nd Edition, 2014
5	Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems	Pascal Ackerman	Packt Publishing	2nd Edition, 2021

6	Building an Effective Cybersecurity Program: Lessons Learned from an Industrial Control Systems Environment	Tari Schreider	Rothstein Publishing	Ist edition, 2017

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Industrial Automation using PLC, SCADA & DCS	R.G.Jamkar	Global Education Ltd	2nd Edition, 2018
2	Handbook of SCADA/Control Systems Security	Robert Radvanovsky, Jacob Brodsky	CRC Press	2nd Edition, 2016
3	Effective Cyber security: A Guide to Using Best Practices and Standards	William Stallings	Addison-Wesley Professional	1st edition , 2018

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://nptel.ac.in/courses/106/105/106105217/ https://nptel.ac.in/courses/108/105/108105088/
2	https://nptel.ac.in/courses/108/101/108101167/ https://nptel.ac.in/courses/106/105/106105217/
3	https://nptel.ac.in/courses/106/106/106106220/ https://nptel.ac.in/courses/108/108/108108122/
4	https://nptel.ac.in/courses/108/108/108108098/ https://nptel.ac.in/courses/106/105/106105217/

SEMESTER S5
PRIVACY REGULATIONS AND COMPLIANCE

Course Code	**24SJPECCT636**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:0	**ESE Marks**	60
Credits	3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

6. To provide students with in-depth knowledge of India's specific data privacy laws, data governance frameworks, and compliance requirements.
7. To provide students with knowledge on how local requirements align with or differ from global compliance expectations.
8. To provide students with the relevant technological ecosystems and emerging trends that influence data privacy, governance, and compliance in India and beyond.

Module No.	Syllabus Description	Contact Hours
1	**Foundations of Privacy Law in India** Evolution of privacy rights: Right to Privacy as fundamental right (Puttaswamy judgment), Constitutional principles and privacy jurisprudence, Overview of the Digital Personal Data Protection Act, 2023 (DPDPA), Overview of GDPR, Definitions: data principals, fiduciaries, personal vs sensitive data **The Digital Personal Data Protection Act, 2023** Core obligations of fiduciaries: consent, purpose limitation, data minimization Rights of data principals: access, correction, grievance redressal. Penalties for non-compliance and obligations for Significant Data Fiduciaries (impact assessments, data protection officers). Cross-border data transfers and localization requirements. Exemptions and lawful processing bases	**9**
2	**Sectoral Privacy Regulations** Financial sector: RBI, SEBI guidelines, PMLA obligations Healthcare: EHR Standards 2016, IT Rules 2011, telemedicine privacy Telecom and IT sector rules, E-commerce and digital platform governance **Legacy Frameworks and Transition** Information Technology Act, 2000 and amendments; IT (Reasonable Security Practices) Rules, 2011; Transition strategies and gap analysis for DPDPA compliance; Migration frameworks for enterprises **Compliance Implementation in Practice** Privacy by design and default in the Indian context; Data governance frameworks and audit methodologies; Privacy impact assessments, breach response, and incident handling; Consent management, privacy policies, and user rights frameworks; Alignment with ISO/IEC 27701, ISO/IEC 27001 and related security standards	**9**

3	**Global Standards and Internet Governance Ecosystem** International standards: ISO/IEC frameworks for security, privacy, and risk management Role of Internet governance bodies: ICANN – domain management and DNS privacy considerations, W3C – web standards and accessibility guidelines, ISOC – global Internet policy and best practices, ITU, IETF, and other bodies shaping communication protocols and privacy, Impact of standards on compliance and interoperability **Cross-Border and Comparative Privacy** DPDPA vs GDPR: key parallels and divergences US privacy laws (CCPA, HIPAA) and implications for Indian firms Data transfer mechanisms, adequacy frameworks, and compliance strategies Multinational operations: harmonizing global privacy requirements **Privacy Challenges in Emerging Technologies** AI-driven decision-making and algorithmic transparency IoT and smart devices: securing personal data flows Biometric data handling in Aadhaar-linked ecosystems Blockchain, distributed ledgers, and decentralized identity systems Digital health, telemedicine, and wearable privacy considerations	**9**
4	**Industry Case Studies:** Banking and financial compliance models**,** Healthcare data protection frameworks**,** E-commerce privacy risks and mitigation strategies**,** Government data handling and public accountability**,** Startups and SMEs: practical compliance challenges **Enforcement, Governance, and Ethical Issues:** **Data Protection Board of India**: powers, investigation, penalties**,** Appeals, dispute resolution, and enforcement trends **Corporate governance:** board oversight and privacy leadership**,** Proposed amendments, regulatory developments, and international cooperation Privacy-enhancing technologies and ethical dilemmas in data processing**,** Career paths in privacy, security, and compliance	**9**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination-2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

	Course Outcome	Bloom's Knowledge Level (KL)
CO1	Understand the obligations of data fiduciaries, rights of data principals, and lawful data processing requirements around the world.	**K2**
CO2	Explain sectoral privacy regulations, legacy frameworks, compliance practices and understand their role in data protection and governance.	**K2**
CO3	Describe global privacy standards, internet governance frameworks, and emerging technology challenges to understand their impact on compliance and data protection.	**K2**
CO4	Explain industry case studies, enforcement mechanisms, and ethical issues to understand practical compliance challenges and governance in data protection.	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓	✓		✓	✓				
CO2	✓	✓	✓	✓		✓	✓				
CO3	✓	✓	✓	✓		✓	✓				
CO4	✓	✓	✓	✓		✓	✓				

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	The General Data Protection Regulation: A Law for the Digital Age?	Lilian Mitrou	Springer	2017
2	Practical Guide to Digital Personal Data Protection Act, 2023 - Law and Compliance	Puneet Bhasin	OakBridge Publishing	2024
3	Personal Data Protection Rights	Ashit Kumar Srivastava, Yogesh Pratap Singh	Lexis Nexis	2025

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Data Protection Around the World: An Introduction	Elif Kiesow Cortez	Springer Link	2020
2	The EU General Data Protection Regulation (GDPR): A Practical Guide	Paul Voigt & Axel von dem Bussche	Springer	2024
3	The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?	Manon Oostveen & Kristina Irion	Springer	2018
4	Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches	R. Walters, Leon Trakman, Bruno Zeller	Springer	2019

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://www.youtube.com/watch?v=g_G2bFrkeHY&list=PLyqSpQzTE6M-jkJEzbS5oHJUp2GWPsq6e&index=30
2	https://www.youtube.com/watch?v=qtTFHNVUDBg&list=PLyqSpQzTE6M-jkJEzbS5oHJUp2GWPsq6e&index=38

SEMESTER S6
BIOMETRIC SECURITY

Course Code	**24SJPECCT635**	**CIE Marks**	40
Teaching Hours/Week (L: T:P: R)	3:0:0:1	**ESE Marks**	60
Credits	5/3	**Exam Hours**	2 Hrs. 30 Min.
Prerequisites (if any)	None	**Course Type**	Theory

Course Objectives:

1. To provide students with a comprehensive understanding of the principles, technologies, and processes involved in biometric systems, including various recognition techniques and performance measures.
2. To enable students to critically evaluate security issues, privacy concerns, and biometric standards, while exploring the practical applications of biometric systems across different fields.

Module No.	Syllabus Description	Contact Hours
1	Biometric fundamentals – Biometric technologies – Biometrics Vs traditional techniques – Characteristics of a good biometric system – Benefits of biometrics – Key biometric processes: verification, identification and biometric matching – Performance measures in biometric systems, FAR, FRR, FTE rate, EER and ATV rate, Applications of Biometric Systems, Security and Privacy Issues, Physiological Biometrics and Behavioral Biometrics.	**8**
2	Fingerprint recognition: Friction ridge patterns, Acquisition, Feature extraction, matching, indexing, synthesis, palm print. Face recognition: Introduction, image acquisition, face detection. Feature extraction of face recognition, matching, heterogeneous face recognition. Signature-scan, Keystroke Scan– components, working principles.	**11**
3	Iris recognition, Image acquisition, iris segmentation, normalization. Encoding and matching, quality assessment, performance evaluation Ear detection and recognition – challenges, gait and hand geometry. Feature extraction and matching	**8**
4	Security of bio-metric systems: adversary attacks, attacks on user interface, attacks on bio-metric processing, database attacks. Biometric standards, biometric databases	**7**

Course Assessment Method (CIE: 40 marks, ESE: 60 marks)
Continuous Internal Evaluation Marks (CIE):

Attendance	Internal Examination	*Evaluate*	*Analyse*	*Total*
5	**15**	**10**	**10**	**40**

Criteria for Evaluation (Evaluate and Analyse): 20 marks

End Semester Examination Marks (ESE):

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	2 questions will be given from each module, out of which 1 question should be answered. Each question can have a maximum of 3 sub divisions. Each question carries 9 marks. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

	Course Outcome	Bloom's Knowledge Level (KL)
CO1	Understand the fundamental concepts of biometric systems, including their technologies and key processes.	**K2**
CO2	Understand key performance metrics of biometric systems and their relevance to system accuracy.	**K2**
CO3	Apply various biometric recognition techniques, including fingerprint, face, iris, and palm print recognition, understanding the acquisition, feature extraction, and matching processes **and distinguish between physiological and behavioral biometrics**	**K3**
CO4	Identify potential security and privacy threats in biometric systems, and recommend strategies to mitigate attacks on biometric processing, user interfaces, and databases.	**K3**
CO5	Understand the biometric standards, databases, and their applications across different industries.	**K2**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	✓	✓	✓			✓					✓
CO2	✓	✓	✓		✓						✓
CO3	✓	✓	✓	✓	✓	✓	✓				✓
CO4	✓	✓		✓	✓	✓					✓
CO5	✓	✓	✓	✓	✓	✓					✓

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Introduction to Biometrics	Anil K. Jain, Arun A. Ross, Karthik Nandakumar,	Springer	2011
2	Handbook of Biometrics	Jain, P. Flynn, A. Ross	Springer	2008

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Biometric Technologies and Verification Systems	John R. Vacca	Elsevier	2007
2	Biometrics- Identity Verification in a Networked World	Samir Nanavati, Michael Thieme, Raj Nanavati	Wiley-dreamtech India Pvt Ltd, New Delhi	2003
3	Biometrics for Network Security	Paul Reid	Pearson Education, New Delhi	2004

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://www.youtube.com/watch?v=GMDggxifxqk&list=PLbMVogVj5nJSCwX0N6MAXPsKGWFRI5Y5m&index=1
2	https://www.youtube.com/watch?v=7aQgQGeZ_qo&list=PLbMVogVj5nJSCwX0N6MAXPsKGWFRI5Y5m&index=5
3	https://www.youtube.com/watch?v=ZEV3th6_olk&list=PLbMVogVj5nJSCwX0N6MAXPsKGWFRI5Y5m&index=8
4	https://www.youtube.com/watch?v=eNPAas0XgVI&list=PLbMVogVj5nJSCwX0N6MAXPsKGWFRI5Y5m&index=15