Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	IOT Security
Course Code	CY-801
Semester	8
Course Category	Professional Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Fundamentals of computer networking (TCP/IP stack, OSI model, IPv4/IPv6)

• Programming proficiency in C and/or Python for embedded/IoT development

• Basic understanding of security concepts and cryptography (confidentiality, integrity, symmetric/asymmetric encryption)

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	Topics	Hours
1	**Foundations of IoT, Networking & Cryptography** - Introduction to IoT: vision, enabling technologies, benefits & drawbacks - IoT layered model (device, connectivity, data, analytics, value, human, regulations) - Basic IoT architecture (devices, gateways, cloud, edge) - Fundamentals of computer networking: TCP/IP stack, IPv4/IPv6, 6LoWPAN basics - Core security principles: confidentiality, integrity, availability, least-privilege, defense-in-depth - Basic cryptography concepts: symmetric vs. asymmetric encryption, hash functions, digital signatures (conceptual only) - Security-by-design mindset for IoT - Common IoT vulnerabilities (weak authentication, unprotected communications, insecure firmware, lack of updates)	5
2	**IoT Communication Protocols & Standards**	6

	- Application-layer protocols: MQTT, CoAP, HTTP/HTTPS, WebSockets, DDS, AMQP - MQTT deep-dive: broker installation (Mosquitto), configuration, TLS/SSL, authentication mechanisms - Transport-layer protocols: TCP, UDP and their security extensions (TLS, DTLS) - Network-layer protocols: IPv4, IPv6, 6LoWPAN - Link-layer & wireless standards: Ethernet, Wi-Fi, Wi-MAX, Cellular (LTE/5G), Bluetooth, Zigbee, Z-Wave, 6LoWPAN - Wired interface standards: UART/USART, I²C, SPI, JTAG, Ethernet PHY - Device provisioning & certificate enrollment basics - Overview of AWS IoT architecture and device-management services	
3	**IoT Threat Landscape & Attack Vectors** - OWASP Top 10 for IoT and mapping to attack surface components - Hardware attacks: tampering, side-channel leakage, firmware modification - Software attacks: malware, code injection, insecure APIs - Network-protocol attacks: MQTT/CoAP hijacking, DNS spoofing, eavesdropping - Industrial IoT threats: guest-hopping, VM escape, supply-chain compromises - Cryptographic attacks: dictionary/brute-force, rainbow tables, hash collisions (conceptual) - Social-engineering attacks: phishing, pharming, device defacement - Privacy-focused attacks and data-theft scenarios - Threat-modeling methods for IoT (STRIDE, ATT&CK for IoT) - Basic risk analysis & threat-assessment workflow	7
4	**Secure IoT Design & Implementation** - Security-by-design process for IoT products - Secure/Trusted boot, TPM basics, remote attestation, tamper-resistant hardware - ARM TrustZone architecture (hardware & software stacks) - Identity & Access Management for IoT: AAA, credential types, role-based and attribute-based models - Cryptographic key management for constrained devices - Building prototypes with Raspberry Pi: hardware basics, circuit interfacing, C & Python	8

	programming - End-to-end MQTT security: TLS, client certificates, ACLs, token-based auth - AWS IoT programming fundamentals (device shadows, rules engine) - Secure OTA firmware update mechanisms - Secure coding practices for embedded C/Python and device hardening checklist	
5	**Cloud, Edge & Data Management Security for IoT** - Cloud service models (IaaS, PaaS, SaaS) and deployment types (public, private, hybrid) - IoT-cloud integration patterns and core AWS IoT services - Cloud security controls for IoT: network segmentation, IAM policies, encryption at rest & in transit, Zero-Trust networking - Edge analytics & AI-driven security monitoring - Data lifecycle in IoT: collection, aggregation, normalization, storage, reporting, alerting - Data classification (public, private, sensitive, confidential, proprietary) and protection policies - Privacy-by-Design and IoT Privacy Impact Assessment (PIA) - Regulatory landscape (GDPR, CCPA, industry-specific standards) and compliance monitoring - Incident-response planning and forensic readiness for IoT environments - IDS/IPS techniques for IoT, system-integrity validation, anti-malware controls	8
6	**Applied IoT Security - Case Studies, Governance & Emerging Topics** - Case studies: smart home, smart grid, smart healthcare, smart cities, smart retail, smart industry - Domain-specific risk & impact analysis (vulnerabilities, potential consequences) - IoT ethics, privacy considerations, and legal/regulatory frameworks (international law, standards, compliance) - Development of comprehensive IoT security policies and governance structures (NIST CSF, ISO/IEC 27001) - Security lifecycle management: design, implementation, operation, maintenance, secure disposal - Emerging trends: AI-enabled security analytics, post-quantum cryptography for IoT, new lightweight protocols (e.g., MQTT-SN, LwM2M) - Metrics, continuous monitoring, and security-as-	8

	code for IoT deployments - Future research challenges and directions in IoT and cryptography	

6. References

Textbooks:

1. Brian Russell and Drew Duren, "Practical Internet of Things Security", Packt Publishing, 2016

2. Hu, Fei. Security and privacy in Internet of things (IoTs): Models, Algorithms, and st Implementations, 1 edition,CRC Press, 2016.

3. David Etter, " IoT Security: Practical guide book " Create Space, 1st Edition, 2016.

4. Zaigham Mahmood, Shijiazhuang, "Security, Privacy and Trust in the IoT Environment" Springer Publications, 2019.

Reference Books:

1. Giancarlo Fortino and Carlos E. Palau "Interoperability, Safety and Security in IoT" Springer Publications 2017.

2. Whitehouse O. Security of things: An implementers' guide to cyber-security for internet of thingsdevices and beyond, 1 edition, NCC Group, 2014

3. Brian Russell, Drew Van Duren, "Practical Internet of Things Security: Design a security framew ork for an Internet connected ecosystem", 2nd Edition, 2018.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-801.1	Identify and list the components of the IoT layered model, basic networking stacks (TCP/IP, IPv4/IPv6, 6LoWPAN) and core cryptographic concepts (symmetric/asymmetric encryption, hash functions, digital signatures).	Identify	Remember
CY-801.2	Explain the operation, security features, and typical use-cases of major IoT communication protocols (MQTT, CoAP, HTTP/HTTPS, DTLS, 6LoWPAN) and describe	Explain	Understand

	how AWS IoT services support device provisioning and management.		
CY-801.3	Implement a secure IoT prototype on a Raspberry Pi that uses TLS-protected MQTT, client certificates, and role-based ACLs, and demonstrate an over-the-air (OTA) firmware update process.	Implement	Apply
CY-801.4	Analyze a given IoT deployment by mapping OWASP IoT Top 10 threats to its attack surface, applying STRIDE and ATT&CK for IoT to produce a risk-assessment report with prioritized mitigations.	Analyze	Analyze
CY-801.5	Evaluate cloud and edge security controls (IAM policies, network segmentation, encryption at rest/in-transit, Zero-Trust networking) and design a compliant data-lifecycle and incident-response plan that satisfies GDPR/CCPA requirements for an IoT solution.	Evaluate	Evaluate
CY-801.6	Create a comprehensive IoT security governance framework--including policies, secure-by-design processes, continuous monitoring metrics, and integration of emerging technologies such as AI-driven analytics and post-quantum cryptography--for a selected domain (e.g., smart healthcare).	Create	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	2	1	-	-	-	1	-	2
CO2	3	2	2	2	3	2	-	-	-	3	-	2
CO3	2	1	3	2	3	2	-	-	1	2	1	2
CO4	2	3	2	3	2	2	-	1	1	3	2	2
CO5	2	2	3	2	3	3	2	2	1	2	2	2
CO6	2	2	3	2	3	3	1	3	2	3	2	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	2	1
CO3	2	3	1
CO4	3	2	3
CO5	3	2	3
CO6	3	2	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Digital Privacy and Social Engineering Defense
Course Code	CY-802
Semester	8
Course Category	Professional Elective Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Fundamentals of computer networks and Internet protocols (TCP/IP, DNS, HTTP, etc.)

• Introductory cybersecurity concepts including basic cryptography, threat modeling, and security controls (confidentiality, integrity, availability)

• Awareness of privacy principles and data-protection regulations (e.g., GDPR, CCPA)

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	Topics	Hours
1	**Foundations of Digital Privacy & Human Factors** - Digital-privacy fundamentals: definition, privacy vs. security, types of personal & sensitive data, digital footprint & online identity - Core privacy concepts: anonymity, pseudonymity, unlinkability, unobservability - Economics of privacy: data brokers, surveillance capitalism, value of personal data - Human-factor principles in security: basic psychology, Cialdini's 6 influence principles, common cognitive biases - Introduction to social engineering: definition, why people are the weakest link, high-level attack-lifecycle overview	7
2	**Legal, Regulatory, and Ethical Landscape** - Major privacy regulations: GDPR, CCPA/CPRA, Indian DPDP Act 2023, HIPAA, ePrivacy Directive, IT Act 2000 - Core regulatory principles: lawful processing, consent, data-subject rights (access, rectification,	6

	erasure, portability), purpose limitation, data minimisation - Privacy Impact Assessments (PIA) & Data-Protection Impact Assessments (DPIA) - Compliance & audit basics; privacy-by-design & privacy-by-default implementation - Cyber-law relevant to social engineering: IT Act §§ 66C/66D, CFAA, Computer Misuse Act, relevant case law - Ethical considerations & responsible disclosure in privacy research and penetration testing - Standard frameworks: NIST Privacy Framework, ISO/IEC 27701 (privacy extension to ISO 27001)	
3	**Privacy-Enhancing Technologies & Technical Controls** - Cryptography basics: symmetric & asymmetric encryption, hash functions, digital signatures - Network-level PETs: mix-nets, Tor architecture & onion routing, VPNs, proxies, I2P - Privacy-preserving data techniques: k-anonymity, LINDDUN threat modelling, data-anonymisation, pseudonymisation, tokenisation, data-masking, data-minimisation - Data-loss-prevention (DLP) tools, secure deletion methods, metadata stripping (MAT2, ExifTool) - Anti-tracking & anti-fingerprinting: browser fingerprinting basics, super-cookies, privacy-focused extensions (JShelter, uBlock Origin) - Practical privacy controls: configuration hardening, secure defaults, privacy-by-design checklists	8
4	**Social Engineering Theory & Reconnaissance** - Detailed social-engineering attack lifecycle: reconnaissance -> engagement -> exploitation -> exit - OSINT fundamentals: passive vs. active footprinting, open-source data sources - Core OSINT tooling: Maltego, SpiderFoot, theHarvester, Recon-ng, Shodan, HaveIBeenPwned - Doxxing pipelines and counter-doxxing techniques - Pre-texting & role-playing scenarios; influence frameworks (Cialdini, Hadnagy's SE Pyramid) - Psychological profiling of targets; susceptibility assessment models - Mapping SE techniques to ATT&CK for Social Engineering	5
5	**Social Engineering Attack Vectors & Practical Labs**	8

	- Phishing ecosystem: email phishing, spear-phishing, whaling, clone phishing, QR-code (quishing) attacks - Technical email security: SPF, DKIM, DMARC analysis and mitigation - Vishing & deep-fake voice attacks; telephony security controls - Smishing & mobile-device security: app-permission hardening, SMS-based attacks - Physical SE techniques: tailgating, piggybacking, dumpster diving, shoulder surfing, impersonation (IT support, law enforcement, HR) - Baiting & USB-drop attacks, quid-pro-quo schemes, malware delivery via SE - Business Email Compromise (BEC) and water-hole attacks - Hands-on labs: simulated phishing campaign (GoPhish), OSINT exercise, USB-baiting demonstration, red-team/blue-team debrief	
6	**Defense, Incident Response, Governance & Emerging Trends** - Designing security-awareness programs: scenario-based training, gamification, micro-learning, effectiveness metrics (click-rate, report-rate) - Incident-response for SE attacks: specialised IR playbook, forensic collection of malicious documents & phone records, mock-campaign debrief - Technical controls: email filtering, firewalls, IDS/IPS, EDR, MFA, Zero-Trust verification procedures - SOC role in monitoring SE; red-team vs. blue-team exercises, tabletop simulations - Privacy engineering & governance: privacy-by-design implementation, data-governance, IAM, least-privilege, Zero-Trust for human risk - Emerging challenges: AI/ML-generated deepfakes, quantum-computing impact on encryption, biometric privacy, social-credit systems, evolving surveillance capitalism - Career pathways in privacy, social-engineering defence, certifications (CISSP, CIPP, OSCP, GSEC)	8

6. References

Textbooks:

1. The Art of Deception: Controlling the Human Element of Security by Kevin Mitnick.

2. Handbook of Social Engineering Red Team and Blue Team: A Cyber Security Handbook by Ali Abdallah.

3. Social Engineering: The Art of Human Hacking by Christopher Hadnagy.

Reference Books:

1. Data Privacy and GDPR Handbook - Sanjay Sharma

2. "Data and Goliath" - Bruce Schneier

3. "Privacy on the Line" - Whitfield Diffie and Susan Landau

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-802.1	Recall and describe fundamental digital-privacy concepts, the distinction between privacy and security, types of personal data, and core human-factor principles such as Cialdini's influence principles and common cognitive biases.	Recall	Remember
CY-802.2	Explain the principal provisions of major privacy regulations (GDPR, CCPA/CPRA, DPDP Act 2023, HIPAA, ePrivacy) and assess their implications for implementing privacy-by-design and privacy-by-default controls.	Explain	Understand
CY-802.3	Configure and demonstrate at least three privacy-enhancing technologies (e.g., Tor, k-anonymity, data-masking) to protect data in transit and at rest within a simulated enterprise environment.	Configure	Apply
CY-802.4	Analyze a simulated social-engineering campaign by performing OSINT reconnaissance with tools such as Maltego and theHarvester, mapping findings to ATT&CK for Social Engineering, and identifying high-risk target profiles.	Analyze	Analyze

CY-802.5	Design a comprehensive security-awareness and incident-response program for social-engineering attacks, including phishing simulations, reporting metrics, and a forensic playbook for mitigation.	Design	Create
CY-802.6	Evaluate the impact of emerging technologies such as AI-generated deepfakes, quantum-resistant cryptography, and biometric privacy on privacy and social-engineering defenses, and propose strategic governance recommendations aligned with the NIST Privacy Framework and ISO/IEC 27701.	Evaluate	Evaluate

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	-	2	-	2	-	1	-	2
CO2	3	2	3	2	1	3	-	2	1	2	2	2
CO3	3	2	3	2	3	2	1	2	1	1	2	2
CO4	3	3	1	3	3	2	-	2	2	2	1	2
CO5	3	2	3	2	2	3	-	2	3	3	3	2
CO6	3	3	2	2	1	3	1	3	2	3	2	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	2	1	3
CO3	2	3	1
CO4	2	3	1
CO5	1	2	3
CO6	2	1	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Introduction to Entrepreneurship
Course Code	CY-803
Semester	8
Course Category	Humanities and Social Science
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Fundamental concepts of business and economics (e.g., basic micro-economics, market structures, and business terminology)

• Introductory computer literacy with a basic understanding of cybersecurity principles and data privacy

• Basic financial literacy, including simple accounting concepts and budgeting

2. Course Learning Objectives

• Guide students to develop an entrepreneurial mindset that integrates strategic thinking, ethical decision-making, and a foundational cyber-security awareness essential for modern venture creation.

• Enable learners to systematically generate, evaluate, and validate business ideas using design-thinking, lean-startup, and analytical tools (e.g., SWOT, PESTLE, Business Model Canvas) while identifying early cyber-risk considerations.

• Equip students with the knowledge and practical skills to construct comprehensive business plans, navigate legal and regulatory requirements, and address intellectual-property and data-privacy issues for start-ups.

• Introduce and contextualize diverse financing, operational, marketing, and technology management strategies, emphasizing hands-on application and security-focused operational practices for sustainable venture growth.

• Prepare learners to formulate and implement growth, scaling, and sustainability strategies, leveraging entrepreneurship development programs, incubator ecosystems, and continuous cyber-resilience practices.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full Marks**	**Assignment Full Marks**	**Attendance Full Marks**	**Total Marks**
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
Total				100 Marks

5. Course Modules

Module	**Topics**	**Hours**
1	**Foundations of Entrepreneurship & Entrepreneurial Mindset** - Definition and concept of entrepreneurship - Evolution and history of entrepreneurship - Role of entrepreneurship in society and economic development - Core entrepreneurial traits, values and attitudes - Motivation theories and psychological drivers for entrepreneurs - Common myths and realities about	7

	entrepreneurship - Overview of the entrepreneurial ecosystem (incubators, accelerators, networks) - Introductory cyber-security mindset for founders (why security matters from day 1)	
2	**Entrepreneurship Landscape, Types & Environment** - Types of entrepreneurship (women, rural, social, SSI, SME, digital) - Entrepreneur vs. manager vs. intrapreneur - Forms of business ownership and legal structures - Impact of SMEs on economic growth - Key environmental factors: socio-economic, political, legal, technological - Government policies, acts, regulations and institutional support for start-ups - Support structures: DIC, SFCs, SIDBI, NSIC, MSME-DI, E-Cell, EDP overview - Digital transformation and its influence on the entrepreneurial environment	6
3	**Idea Generation & Opportunity Identification** - Sources of new business ideas (trends, problems, technology) - Creative problem-solving techniques (brainstorming, SCAMPER, mind-mapping) - Design thinking and customer-discovery process - Lean Startup & Business Model Canvas for rapid idea validation - Opportunity screening, feasibility assessment and market-gap analysis - Basic tools for assessing business opportunities (SWOT, PESTLE, Porter's 5 forces) - Preliminary business concept development - Early-stage cyber-risk identification (data, privacy, compliance)	8
4	**Business Planning, Legal & Ethical Foundations** - Structure and components of a business plan - Writing a concise executive summary and detailed project report (DPR) - Steps to set up a new venture: registration, licensing, location, layout - Legal requirements for small businesses (Companies Act, GST, labor laws) - Intellectual property basics (trademarks, patents, copyrights) - Data protection, privacy laws and cyber-security compliance - Business ethics and ethical decision-making for	7

	entrepreneurs - Using the business plan for management, monitoring and risk mitigation	
5	**Financing, Operations, Marketing & Technology Management** - Financing options for start-ups: bootstrapping, angel investors, crowdfunding, government schemes - Basics of working-capital management and simple financial controls (no advanced math) - Introduction to financial statements and cash-flow monitoring - Operations fundamentals: production planning, inventory basics, quality basics (TQM) - Human-resource basics: recruitment, motivation, building effective teams - Marketing fundamentals for start-ups: positioning, branding, digital marketing, social media - Technology adoption, internet advertising and e-commerce basics - Cyber-security basics for operations (patch management, access control, incident response)	6
6	**Growth, Scaling, Sustainability & Development Programs** - Growth and expansion strategies (market penetration, diversification, partnerships) - Scaling the business: lean scaling, resource planning, managing complexity - Building sustainable business models (triple-bottom-line, social impact) - Lifecycle management from idea to mature venture - Business model innovation and go-to-market scaling tactics - Role of Entrepreneurship Development Programme (EDP) phases in scaling - Leveraging E-Cell, incubators and institutional support for growth - Cyber-resilience and continuous improvement (security audits, compliance updates)	8

6. References

Textbooks:

1. Poornima M. Charantimath - "Entrepreneurship Development and Small Business Enterprise" (Pearson)

2. Paul Burns - "Entrepreneurship and Small Business" (Palgrave / Bloomsbury imprint)

Reference Books:

1. NCERT / Open Text - "Introduction to Entrepreneurship" (Open Textbook Library / KPU Pressbooks)

2. NCERT / Other Indian HE materials - "Entrepreneurship and Small Business Management"

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-803.1	Define and differentiate the core concepts of entrepreneurship--including its evolution, societal role, and the foundational cyber-security mindset for founders--by listing at least five entrepreneurial concepts and three security principles.	Define	Remember
CY-803.2	Explain the major types of entrepreneurship, legal business structures, and key components of the entrepreneurial ecosystem, and describe how basic cyber-security regulations (e.g., data-protection and privacy laws) integrate with each element.	Explain	Understand
CY-803.3	Apply creative problem-solving techniques (such as SCAMPER or mind-mapping) and the Business Model Canvas to generate a viable business idea, and conduct an initial cyber-risk assessment using a checklist of data, privacy, and compliance threats.	Apply	Apply
CY-803.4	Analyze a complete business plan to identify strengths and weaknesses in market analysis, financial projections, legal compliance, intellectual-property considerations, and cyber-security controls, and produce a structured critique report.	Analyze	Analyze

CY-803.5	Evaluate alternative financing and operational strategies for a startup, recommending the optimal mix of funding sources, operational controls, and cyber-security measures based on a provided case study.	Evaluate	Evaluate
CY-803.6	Design a comprehensive, secure, and scalable venture model that incorporates growth and scaling strategies, sustainability metrics, and a continuous cyber-resilience framework, and present a prototype pitch deck demonstrating the plan.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	1	1	1	-	2	1	1	-	1	-	1
CO2	2	2	1	1	1	3	1	2	-	2	1	1
CO3	3	2	3	2	2	2	1	1	2	2	2	1
CO4	2	3	2	3	2	3	2	2	2	3	2	1
CO5	2	2	3	2	2	3	2	2	2	2	3	1
CO6	3	2	3	2	3	3	3	2	3	3	3	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	1	2
CO2	2	1	3
CO3	2	2	3
CO4	2	1	3
CO5	2	1	3
CO6	3	2	3