3. CYBERSECURITY IN THE INTERNET OF THE FUTURE

SCHOOL	ENGINEERING		
DEPARTMENT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDIES	POSTGRADUATE		
COURSE CODE		**SEMESTER**	1ο
COURSE TITLE	Cybersecurity in the Internet of the Future		

INDEPENDENT TEACHING ACTIVITIES *(In case credits are allocated to distinct parts of the course, e.g., Lectures, Laboratory Exercises, etc. If credits are allocated uniformly to the entire course, state the weekly teaching hours and total credits.)*	**WEEKLY TEACHING HOURS**	**CREDITS**
Lectures	3	8

COURSE CONTENT

The course includes the following teaching units:

1. **Fundamental Concepts**
   - Attackers and special categories (internal attackers)
   - Application and System Vulnerabilities
   - Types of Threats and Attack Methods
   - Security Services and Mechanisms (Controls)

2. **Cryptography**
   - Classical Cryptosystems (Substitution, Transposition, DES, AES)
   - Public Key Encryption (Diffie-Hellman, RSA)
   - Digital Signatures
   - PKI and digital certificates
   - Stream and Block Ciphers
   - Hash Algorithms
   - Cryptographic network protocols (Transport Layer Security - TLS)

3. **Operating System Protection**

   - Objects and protection methods
   - Memory and addressing protection
   - Access Control Mechanisms
   - File protection mechanisms
   - Authentication Mechanisms

4. **Network and Distributed System Security**

   - Network threats
   - Network Security Mechanisms (controls)
   - Security Protocols and Standards on the Internet
   - Wireless Network Security
   - 5G Network Security
   - Firewalls

5. **Cloud Computing Security**

   - Data Security in the cloud
   - Identity and Access Management (IAM)
   - Disaster Recovery and Business Continuity Planning (DR/BCP) in the cloud
   - Intrusion Detection and Incident Response in the cloud

6. **Elements and Properties of Secure and Trusted Distributed Systems**

   - Assurance Techniques
   - Trusted Systems
   - Classes, Vulnerabilities, and Attacks on Distributed Systems
   - Distributed Systems Security
   - Access Control and ID Management
   - Data Security
   - Attacks on P2P systems

7. **Blockchain Technology in Trusted Distributed Systems**

   - Distributed (peer-based) Systems
   - Immutability
   - Cryptographic Identity
   - Consensus Algorithms (POW, POS, Next-gen: PBFT)
   - Applications of Blockchain
   - The Byzantine Generals' Problem
   - BGP solution with Blockchain
   - Blockchain Database, Block, Block Structure, Hash, Miner, Transaction, Consensus mechanism
   - Public and Private Blockchain

8. **Blockchain Security and Privacy**

- Blockchain Attacks
- CAP elements in Blockchain
- Security and Confidentiality Elements of Blockchain
- Security and Privacy Requirements for online transactions on Blockchain
- Attack Resistance (DDoS, Double-Spending, Majority [51%] Consensus Attack, Pseudonymity)
- Security and Privacy Techniques used in Blockchain (Mixing, Anonymous Signatures, Homomorphic Encryption - HE, Attribute-based Encryption - ABE, Secure Multi-Party Computation, Non-Interactive Zero-Knowledge (NIZK) Proof, The Trusted Execution Environment-Based Smart Contracts, Game-based Smart Contracts)

9. **Intrusion Detection in the Internet of Things (IoT)**

- Intrusion Detection Techniques
- Intrusion Detection Systems (IDSs)
- Tools, methods, and technologies used
- Intrusion Detection and Game Theory
- Intrusion Detection in Cloud Computing
- Problems and limitations in IDSs
- Machine Learning Anomaly Detection
- Machine Learning Categories
- Supervised learning for Intrusion Detection
- Unsupervised learning for Intrusion Detection
- Comparison of IDS implementations based on placement
- Comparison of Security Issues and Countermeasures
- IoT Architecture and Attacks/Levels
- IoT Attacks: Taxonomy
- GAN for Distributed ID in IoT

10. **Digital Forensics**

- Methodology application
- Digital Forensics requirements
- File System Forensics
- Application Forensics
- Cloud Computing Forensics
- IoT Forensics
- Network Forensics