Subject Description Form

Subject Code	COMP5579
Subject Title	IoT Security: Principles, Protocols, and Practice
Credit Value	3
Level	5
Pre-requisite/ Co-requisite/ Exclusion	Nil
Objectives	This subject provides postgraduate students with comprehensive knowledge and practical skills in the evolving field of Internet of Things (IoT) security. Key topics include cryptographic foundations, network and wireless security, hardware protection and end-to-end IoT system security. Emphasizing both theory and application, the course enables students to understand core security principles, identify vulnerabilities unique to IoT environments, and design, implement, and assess effective security solutions tailored to diverse IoT applications. The course prepares students to be future-ready professionals with strong ethical awareness and lifelong learning capabilities in the evolving cybersecurity landscape.
Intended Learning Outcomes	Upon completion of the subject, students will be able to: <u>Category A: Professional / Academic Knowledge and Skills</u> a. Identify and analyse critical security issues across all layers of IoT systems, including device, network, and application domains. Understand how resource constraints and diverse deployment environments introduce unique vulnerabilities. b. Apply cryptographic, authentication, and secure communication techniques tailored for IoT architectures. Evaluate and implement protection strategies considering computational efficiency and system scalability. c. Assess hardware-level threats such as firmware tampering and side-channel attacks. Formulate mitigation strategies using secure boot, trusted hardware, and resilient firmware practices. <u>Category B: Attributes for All-Roundedness</u> d. Communicate complex security concepts, risks, and solutions clearly to both technical and non-technical audiences. Demonstrate professionalism in documentation, presentations, and collaborative discussions. e. Think critically and creatively to address evolving IoT security challenges in real-world scenarios. Engage in lifelong, self-directed learning to stay current with emerging technologies, standards, and threats.

Subject Synopsis/ Indicative Syllabus	1. Overview of IoT Security Landscape Examination of IoT architecture and its multilayer security threats, covering the perception, network, management, and application layers. Key challenges include constrained device capabilities, heterogeneous deployments, insecure interfaces, and large-scale data flow. 2. Applied Cryptography for IoT Application of cryptographic techniques in IoT systems, including hash functions for integrity, symmetric/asymmetric encryption for confidentiality, and digital signatures for authentication. Focus on lightweight cryptography, secure key distribution, and protocol adaptation for resource-constrained environments. 3. Physical and Hardware Security Analysis of hardware-based trust anchors such as Trusted Platform Modules (TPM) and secure boot mechanisms. Exploration of physical attack vectors including side-channel attacks (e.g., timing, power analysis), firmware-level threats, and countermeasures for tamper resistance. 4. Network and Wireless Communication Security Design of secure IoT communication networks, with emphasis on Public Key Infrastructure (PKI), IPSec, VPNs, and network access control. Focus on wireless technologies including Wi-Fi, Bluetooth, Zigbee, LoRaWAN, NB-IoT, 5G, and protocols like MQTT and CoAP, highlighting their unique security implications. 5. Data and Cloud Security Technologies End-to-end data protection techniques including secure key management, role-based access control (RBAC), intrusion detection systems (IDS), and secure data sharing models. Coverage of privacy-enhancing technologies such as data anonymization and differential privacy, along with enterprise-level cloud data protection strategies. 6. IoT Security Standards and Case Studies Overview of major IoT security standards including ISO/IEC 27001/27002, NIST SP 800 series, and HIPAA. Critical evaluation of real-world IoT security incidents and case studies across domains such as smart homes, smart grids, connected vehicles, industrial IoT, wearables, and mobile healthcare systems. 7. Emerging Threats and Research Trends in IoT Security Exploration of advanced threats including adversarial attacks on AI-powered IoT systems, firmware supply chain risks, and edge-cloud security integration. Discussion on future research directions, regulatory developments, and secure-by-design methodologies in next-generation IoT systems.

<table>
<tr><td>Teaching/Learning Methodology</td><td>1. Lectures and tutorials are employed to provide a structured overview of the subject, introduce key security concepts in IoT, and explain common vulnerabilities and mitigation techniques. These sessions also serve as interactive platforms for engaging students and gauging their progress through ongoing feedback.

2. Assignments and tests are designed to reinforce classroom learning, promote deeper conceptual understanding, and assess students' mastery of key topics at various stages of the course.

3. Case studies support experiential learning by allowing students to apply theoretical knowledge in practical settings. These activities are aimed at enhancing problem-solving abilities, fostering critical thinking, and developing hands-on skills essential for addressing real-world IoT security challenges.</td></tr>
<tr><td>Assessment Methods in Alignment with Intended Learning Outcomes</td><td>
<table>
<tr><td rowspan="2">Specific assessment methods/tasks</td><td rowspan="2">% weighting</td><td colspan="5">Intended subject learning outcomes to be assessed (Please tick as appropriate)</td></tr>
<tr><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td></tr>
<tr><td>1. Continuous Assessment</td><td>30%</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>• Assignments</td><td>10%</td><td>✓</td><td>✓</td><td>✓</td><td></td><td>✓</td></tr>
<tr><td>• Laboratory demonstration and reports</td><td>10%</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>• Final project</td><td>10%</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>2. Examination</td><td>70%</td><td>✓</td><td>✓</td><td>✓</td><td></td><td>✓</td></tr>
<tr><td>Total</td><td>100 %</td><td colspan="5"></td></tr>
</table>

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:

The assessment methods above fully address the intended learning outcomes.
<table>
<tr><th>Assessment Methods</th><th>Remark</th></tr>
<tr><td>Assignments and examination</td><td>The assignments and examination measure the application of knowledge to real-world IoT security scenarios, focusing on analytical and problem-solving skills.</td></tr>
</table>
</td></tr>
</table>

	Laboratory demonstration and reports	The laboratory demonstration and report test technical competence and communication through hands-on implementation, written documentation and oral presentation.
	Final project	The final project evaluates students' ability to think critically and creatively in developing practical IoT security solutions.

Student Study Effort Expected	Class contact:	
	▪ Lectures	30 Hrs.
	▪ Tutorial/Laboratory/Practice Classes	9 Hrs.
	Other student study effort:	
	▪ Lecture: preview/review of notes; homework/assignment; preparation for test/quizzes	35 Hrs.
	▪ Tutorial/Laboratory/Final project: preview of materials, revision and/or reports writing	40 Hrs.
	Total student study effort	114 Hrs.

Reading List and References

Textbook:

1. “Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem.” Brian Russell, and Drew Van Duren. Packt Publishing; 2nd edition (November 30, 2018).

2. Tang Q, Du F. Internet of things security: Principles and practice[M]. Springer, 2021.

Reference Materials:

1. “Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things.” Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods, No Starch Press, Apr 2021.

2. “The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things.” Aditya Gupta, Apress; 1st ed. edition (April 1, 2019).

3. “Hacking Connected Cars: Tactics, Techniques, and Procedures.” Alissa Knight, Wiley; 1st edition (March 17, 2020).

4. “The IoT Architect's Guide to Attainable Security and Privacy.” Damilare D. Fagbemi, David M Wheeler, and JC Wheeler, Auerbach Publications; 1st edition (October 4, 2019).

5. “IoT and Edge Computing for Architects: Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security.” Perry Lea, 2nd Edition, Packt Publishing (March 6, 2020).