ICT743 INTERNET OF THINGS SECURITY T325 BRIEF

All information in the Subject Outline is correct at the time of approval. KOI reserves the right to make changes to the Subject Outline if they become necessary. Any changes require the approval of the KOI Academic Board and will be formally advised to those students who may be affected by email and via Moodle.
Information contained within this Subject Outline applies to students enrolled in the trimester as indicated

1. General Information

1.1 Administrative Details

Associated HE Award(s)	Duration	Level	Subject Coordinator
Master of Information Technology (MIT)	1 trimester	Postgraduate	Dr Prabhu Singh prabhu.singh@koi.edu.au P: +61 (2) 9283 3583 L: 7-11, 11 York Street. Consultation: via Moodle or by appointment.

1.2 Core/Elective

This subject is
- a core subject for the Master of Information Technology (MIT) Cybersecurity
- an elective subject for the Master of Information Technology (MIT) General

1.3 Subject Weighting

Indicated below is the weighting of this subject and the total course points

Subject Credit Points	Total Course Credit Points
4	MIT (64 Credit Points)

1.4 Student Workload

Indicated below is the expected student workload per week for this subject

No. Timetabled Hours/Week*	No. Personal Study Hours/Week**	Total Workload Hours/Week***
3 hours/week plus supplementary online material	7 hours/week	10 hours/week

* Total time spent per week at lectures and tutorials
** Total time students are expected to spend per week in studying, completing assignments, etc.
*** Combination of timetable hours and personal study

1.5 **Mode of Delivery** Classes will be face-to-face or hybrid. Certain classes will be online (e.g., special arrangements).

1.6 Pre-requisites ICT722 Information Security

1.7 General Study and Resource Requirements

- Students are expected to attend classes with the weekly worksheets and subject support material provided in Moodle. Students should read this material before coming to class to improve their ability to participate in the weekly activities.
- Students will require access to the internet and their KOI email and should have basic skills in word processing software such as MS Word, spreadsheet software such as MS Excel and visual presentation software such as MS PowerPoint.

- Computers and WIFI facilities are extensively available for student use throughout KOI. Students are encouraged to make use of the campus Library for reference materials.

Software resource requirements specific to this subject: MS Imagine, Office 365, VMWare, Cooja emulator, Contiki, VMWare.

1.8 Academic Advising

Academic advising is available to students throughout teaching periods including the exam weeks. As well as requesting help during scheduled class times, students have the following options:

- Consultation times: A list of consultation hours is provided on the homepage of Moodle where appointments can be booked.
- Subject coordinator: Subject coordinators are available for contact via email. The email address of the subject coordinator is provided at the top of this subject outline.
- Academic staff: Lecturers and Tutors provide their contact details in Moodle for the specific subject. In most cases, this will be via email. Some subjects may also provide a discussion forum where questions can be raised.
- Head of Program: The Head of Program is available to all students in the program if they need advice about their studies and KOI procedures.
- Vice President (Academic): The Vice President (Academic) will assist students to resolve complex issues (but may refer students to the relevant lecturers for detailed academic advice).

2. Academic Details

2.1 Overview of the Subject

The Internet of Things (IoT) enables everyday objects to communicate by connecting to the Internet. IoT is expanding rapidly as both businesses and consumers adopt smart technologies. This subject provides fundamental knowledge about applications of the IoT and an understanding of the need for security and privacy for these applications. Students will gain practical experience in developing a secure IoT application in a simulated environment. The subject highlights the differences between specific IoT related security complexities with security complexities related to non-IoT technologies.

2.2 Graduate Attributes for Postgraduate Courses

Graduates of postgraduate courses from King's Own Institute will gain the graduate attributes expected from successful completion of a postgraduate degree under the Australian Qualifications Framework (2nd edition, January 2013). Graduates at this level will be able to apply advanced body of knowledge from their major area of study in a range of contexts for professional practice or scholarship and as a pathway for further learning.

King's Own Institute's generic graduate attributes for a master's level degree are summarised below:

	KOI Postgraduate Degree Graduate Attributes	**Detailed Description**
	Knowledge	Current, comprehensive and coherent knowledge, including recent developments and applied research methods
	Critical Thinking	Critical thinking skills to identify and analyse current theories and developments and emerging trends in professional practice
	Communication	Communication and technical skills to analyse and theorise, contribute to professional practice or scholarship, and present ideas to a variety of audiences

	Research and Information Literacy	Cognitive and technical skills to access and evaluate information resources, justify research approaches and interpret theoretical propositions
	Creative Problem Solving Skills	Cognitive, technical and creative skills to investigate, analyse and synthesise complex information, concepts and theories, solve complex problems and apply established theories to situations in professional practice
	Ethical and Cultural Sensitivity	Appreciation and accountability for ethical principles, cultural sensitivity and social responsibility, both personally and professionally
	Leadership and Strategy	Initiative, leadership skills and ability to work professionally and collaboratively to achieve team objectives across a range of team roles Expertise in strategic thinking, developing and implementing business plans and decision making under uncertainty
	Professional Skills	High level personal autonomy, judgement, decision-making and accountability required to begin professional practice

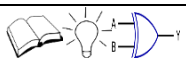
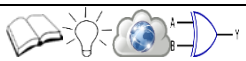
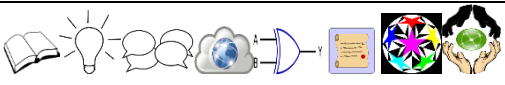
Across the courses, these skills are developed progressively at three levels:

- **Level 1 Foundation –** Students learn the skills, theories and techniques of the subject and apply them in stand-alone contexts
- **Level 2 Intermediate –** Students further develop skills, theories and techniques of the subject and apply them in more complex contexts, beginning to integrate the application with other subjects
- **Level 3 Advanced** – Students have a demonstrated ability to plan, research and apply the skills, theories and techniques of the subject in complex situations, integrating the subject content with a range of other subject disciplines within the context of the course

Generally, skills gained from subjects in the Graduate Certificate and Graduate Diploma are at levels 1 and 2 while other subjects in the Master's degree are at level 3.

2.3 Subject Learning Outcomes

Listed below, are key knowledge and skills students are expected to attain by successfully completing this subject:

Subject Learning Outcomes	Contribution to Course Graduate Attributes
a) Analyse security and privacy challenges and the requirements of IoT applications	
b) Identify and categorise security vulnerabilities and attacks in an IoT environment	
c) Apply security techniques and technologies to secure IoT applications according to enterprise requirements	
d) Design and develop an IoT application in a simulated environment, identify its security issues, and propose solutions	

2.4 Subject Content and Structure

Below are details of the subject content and how it is structured, including specific topics covered in lectures and tutorials. Reading refers to the texts unless otherwise indicated.

Weekly Planner:

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
Week 1 27 Oct	Introduction to the IoT	Ch. 1 [A. Awad and J.l Abawajy] Ch. 1 [B. Russell and D. Duren]	Group project introduced Introduction to Cooja emulator, testing simple scenarios Formative not graded
Week 2 03 Nov	Securing the IoT	Ch. 1 [V. Sharma and G. Joshi] Ch.1 [S. Li and Li Xu]	Discussion of group project Testing single node scenarios in Cooja Tutorial is graded
Week 3 10 Nov	Security architecture of IoT	Ch. 4 [V. Sharma and G. Joshi] Ch. 2 [S. Li and Li Xu]	Discussion of group projects, IoT application requirement and scope needs to be finalised and approved by tutor. Testing multi node scenarios in Cooja Tutorial is graded
Week 4 17 Nov	Vulnerabilities, attacks, and countermeasures	Ch. 2 [V. Sharma and G. Josh Ch. 2 [B. Russell and D. Duren]	Testing different sensor scenario in Cooja Tutorial is graded
Week 5 24 Nov	Security and vulnerability in the IoT	Ch. 2 [A. Awad and J.l Abawajy] Ch. 3 [S. Li and Li Xu]	Discussion of group projects. Testing IPv6 network in Cooja Tutorial is graded **Assessment 2 due: Quiz**
Week 6 01 Dec	IoT node authentication	Ch. 4 [S. Li and Li Xu]	Discussion of group project Testing scenarios to measure power consumption in Cooja Tutorial is graded
Week 7 08 Dec	Cryptographic fundamentals for IoT security engineering	Ch. 6 [V. Sharma and G. Joshi] Ch. 7 [V. Sharma and G. Joshi] Ch. 7 [A. Awad and J.l Abawajy] Ch. 6 [B. Russell and D. Duren]	Testing CoAP clients in Cooja Tutorial is graded
Week 8 15 Dec	Identity and access management solutions for the IoT systems and other security tools	Ch. 15 [V. Sharma and G. Joshi] Ch. 7 [B. Russell and D. Duren]	Discussion of group projects. Testing routing protocols in Cooja Tutorial is graded
Week 9 05 Jan	Mitigating IoT privacy concerns	Ch. 9 [A. Awad and J.l Abawajy] Ch.8 [B. Russell and D. Duren]	Discussion of group projects. Testing security threats in Cooja on a single node. Case Study 1 discussed

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
			Tutorial is graded **Assessment 3 due**
Week 10 12 Jan	Cloud security for the IoT	Ch. 19 [V. Sharma and G. Joshi] Ch. 8 [A. Awad and J.I Abawajy] Ch.10 [B. Russell and D. Duren]	Discussion of group projects. Testing security threats in Cooja in multi node scenarios Case Study 2 discussed Tutorial is graded
Week 11 19 Jan	Security in enabling technology	Ch. 6 [S. Li and Li Xu]	Discussion of group projects Group project report completion and preparation for presentation and demonstration**.** **Assessment 4 due: Group project Report**
Week 12 27Jan (Tue)	Revision	All chapters	**Revision** **Assessment 4 due: Project demonstration**
Week 13 02 Feb	Study review week and Final Exam Week		
Week 14 09 Feb	Examinations Continuing students - enrolments for T126 open		Please see exam timetable for exam date, time and location
Week 15 16 Feb	Student Vacation begins New students - enrolments for T126 open		
Week 16 23 Feb	• Results Released • Review of Grade Day for T325 – see Sections 2.6 and 3.2 below for relevant information. • Certification of Grades NOTE: More information about the dates will be provided at a later date through Moodle/KOI email.		
T126 2 Mar 2026			
Week 1 02 Mar	Week 1 of classes for T126		

2.5 Teaching Methods/Strategies

Briefly described below are the teaching methods/strategies used in this subject:

- *Lectures* (1 hours/week) are conducted in seminar style and address the subject content, provide motivation and context and draw on the students' experience and preparatory reading.
- *Tutorials* (2 hours/week) include class discussion of case studies and research papers, practice sets and problem-solving and syndicate work on group projects. Tutorials often include group exercises and so contribute to the development of teamwork skills and cultural understanding. Tutorial participation is an essential component of the subject and contributes to the development of many of the graduate attributes (see section 2.2 above). Tutorial participation contributes towards the assessment in many subjects (see details in Section 3.1 for this subject). Supplementary tutorial material such as case studies, recommended readings, review questions etc. will be made available each week in Moodle.
- *Online* teaching resources include class materials, readings, model answers to assignments and exercises and discussion boards. All online materials for this subject as provided by KOI will be found in the Moodle page for this subject. Students should access Moodle regularly as material may be updated at any time during the trimester
- *Other contact* - academic staff may also contact students either via Moodle messaging, or via email to the email address provided to KOI on enrolment.

2.6 Student Assessment

Assessment is designed to encourage effective student learning and enable students to develop and demonstrate the skills and knowledge identified in the subject learning outcomes. Assessment tasks during the first half of the study period are usually intended to maximise the developmental function of assessment (formative assessment). These assessment tasks include weekly tutorial exercises (as indicated in the weekly planner) and low stakes graded assessments (as shown in the graded assessment table). The major assessment tasks where students demonstrate their knowledge and skills (summative assessment) generally occur later in the study period. These are the major graded assessment items shown in the graded assessment table.

Final grades are awarded by the Board of Examiners in accordance with KOI's Assessment and Assessment Appeals Policy. The definitions and guidelines for the awarding of final grades are:

- *HD High distinction* (85-100%): an outstanding level of achievement in relation to the assessment process.
- *D Distinction* (75-84%): a high level of achievement in relation to the assessment process.
- *C Credit* (65-74%): a better than satisfactory level of achievement in relation to the assessment process.
- *P Pass* (50-64%): a satisfactory level of achievement in relation to the assessment process.
- *F Fail* (0-49%): an unsatisfactory level of achievement in relation to the assessment process.
- *FW:* This grade will be assigned when a student did not submit any of the compulsory assessment items.

Provided below is a schedule of formal assessment tasks and major examinations for the subject.

Assessment Type	When Assessed	Weighting	Learning Outcomes Assessed
Assessment 1: Weekly Tutorial	Week 2- Week 11	20%	a, b, c, d
Assessment 2: Quiz	Week 5	15%	a, b
Assessment 3:Individual Research activity (Individual report: 2000 words)	Week 9	30%	a, b, c, d

Assessment Type	When Assessed	Weighting	Learning Outcomes Assessed
Assessment 4: Group Project (Group report : 3000 words, Individual report: 600 words)	Week 11 – Report Week 12 - Demonstration Presentation	Group work: 20% Individual contribution: 10% Presentation: 5%	a, b, c, d

Requirements to Pass the Subject:

To gain a pass or better in this subject, students must gain a *minimum of 50%* of the total available subject marks.

2.7 Prescribed and Recommended Readings

Provided below, in formal reference format, is a list of the prescribed and recommended readings.

Prescribed Texts:

Sharma, V. & Joshi, G. (2023). Enhancing IoT Security: A Holistic Approach to Security for Connected Platforms. BPB Publications.

Awad, A.H., & Abawajy, J.H. (2022). Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications. Wiley-Ieee Press, Hoboken.

Recommended Readings:

Russell, B., & Van Duren, D., (2019) *Practical Internet of Things Security,* 2nd edition. Pack Publishing Ltd.

Li, S. and Da Xu, L. (2017), Securing the internet of things. Syngress.

Ryan, M.K. and Rozier, K.Y. (2024) 'A survey and analysis of recent IoT device vulnerabilities'.

Kokila, M. and Reddy, S., 2025. Authentication, access control and scalability models in Internet of Things Security–A review. Cyber Security and Applications, 3, p.100057.

Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S. and Islam, S.R., 2024. A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. Future Internet, 16(2), p.40.

Qaddos, A., Yaseen, M.U., Al-Shamayleh, A.S., Imran, M., Akhunzada, A. and Alharthi, S.Z., 2024. A novel intrusion detection framework for optimizing IoT security. Scientific Reports, 14(1), p.21789.

Awad, A.I., Ahmad, A., Choo, K.-K.R., and Hakak, S. (2023). Internet of Things Security and Privacy: Practical and Management Perspectives. Boca Raton: CRC Press.

Ghafoor, K.Z., Curran, K., Kong, J., and Sadiq, A.S. (2023). Security and Organization Within IoT and Smart Cities. Boca Raton: CRC Press.

Swathika, O.V., Karthikeyan, A., and Sanjeevikumar, P. (2023). IoT and Analytics in Renewable Energy Systems Volume 2: AI, ML, and IoT Deployment in Sustainable Smart Cities. Boca Raton: CRC Press.

Aziz, M., Elmedany, W. and Sharif, M.S. (2023) 'Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques'. Journal of Cyber Security Technology, pp.1–25. doi: https://doi.org/10.1080/23742917.2023.2228053.

Najmi, K.Y., AlZain, M.A., Masud, M., Jhanjhi, N.Z., Al-Amri, J. and Baz, M., (2023). A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability. *Materials Today: Proceedings*, *81*, pp.377-382.

Baho, S.A. and Abawajy, J. (2023) 'Analysis of Consumer IoT Device Vulnerability Quantification Frameworks'. Electronics, 12(5), p.1176.

Barrera, D., Bellman, C. and Van Oorschot, P. (2023) 'Security best practices: a critical analysis using IoT as a case study'. ACM Transactions on Privacy and Security, 26(2), pp.1-30.

Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E.C.P., Xiong, P., Iqbal, S., Lamontagne, P., Ray, S. and Ghorbani, A.A. (2023) 'Internet of things (IoT) security dataset evolution: Challenges and future directions'. Internet of Things, p.100780.

Tariq, U., Ahmed, I., Bashir, A.K. and Shaukat, K. (2023) 'A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review'. Sensors, 23(8), p.4117.

Sadhu, P.K., Yanambaka, V.P. and Abdelgawad, A. (2022) 'Internet of things: Security and solutions survey'. Sensors, 22(19), p.7433.

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M. and Stiller, B. (2022) 'Landscape of IoT security'. Computer Science Review, 44, p.100467.

Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A. and Arshad, H. (2022) 'The internet of things security: A survey encompassing unexplored areas and new insights'. Computers & Security, 112, p.102494.

Khan, A.R., Kashif, M., Jhaveri, R.H., Raut, R., Saba, T. and Bahaj, S.A. (2022) 'Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions'. Security and Communication Networks, 2022.

Rana, A.K. and Sharma, S. (2021) 'Contiki Cooja Security Solution (CCSS) with IPv6 routing protocol for low-power and lossy networks (RPL) in Internet of Things applications'. In: Mobile Radio Communications and 5G Networks: Proceedings of MRCN 2020. Singapore: Springer, pp.251-259.

Arora, S., Gambheer, R. and Vohra, M. (2021) Design of Secure IoT Systems: A Practical Approach Across Industries. McGraw Hill.

Mohanty, J., Mishra, S., Patra, S., Pati, B. and Panigrahi, C.R. (2021) 'IoT security, challenges, and solutions: a review'. In: Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 2, pp.493-504.

Khan, A.R., Kashif, M., Jhaveri, R.H., Raut, R., Saba, T. and Bahaj, S.A. (2021) 'Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions'. Security and Communication Networks, 2021.

Mohanta, B.K., Jena, D., Satapathy, U. and Patnaik, S. (2020) 'Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology'. Internet of Things, 11, p.100227.

Litoussi, M., Kannouf, N., El Makkaoui, K., Ezzati, A. and Fartitchou, M. (2020) 'IoT security: challenges and countermeasures'. Procedia Computer Science, 177, pp.503-508.

Liyanage, M., Braeken, A., Kumar, P. and Ylianttila, M. (2020) IoT Security: Advances in Authentication. Wiley.

Atlam, H.F. and Wills, G.B. (2020) 'IoT security, privacy, safety and ethics'. In: Digital twin technologies and smart cities. pp.123-149.

Useful Websites:

- Simmons, A. (2023) 'Internet of Things (IoT) Examples by Industry in 2023'. Available at: https://dgtlinfra.com/internet-of-things-iot-examples/
- LeBlanc, L. (2022) 'What is IoT Security?'. Available at: https://www.sierrawireless.com/iot-blog/what-is-iot-security/.
- Lauzier, J. (2020) 'Industrial IoT Security: Challenges and Solutions'. Available at: https://www.machinemetrics.com/blog/industrial-iot-security
- IoT Agenda (2024). TechTarget. Available at: https://internetofthingsagenda.techtarget.com/

***Suggested Periodicals*:**

- IEEE Internet of Things Journal: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6488907
- Journal of Cyber Security Technology: https://www.tandfonline.com/loi/tsec20
- Journal of Information Security and Applications: https://www.journals.elsevier.com/journal-of-information-security-and-applications.
- IEEE Internet of Things (2024). IEEE IoT Initiative. Available at: https://iot.ieee.org/

Conference/ Journal Articles:

Thabit, F., Can, O., Aljahdali, A.O., Al-Gaphari, G.H. and Alkhzaimi, H.A., 2023. Cryptography algorithms for enhancing IoT security. Internet of Things, 22, p.100759.

Ahmid, M. and Kazar, O., 2023. A comprehensive review of the internet of things security. Journal of Applied Security Research, 18(3), pp.289-305.

Alqarawi, G., Alkhalifah, B., Alharbi, N. and El Khediri, S., 2023. Internet-of-things security and vulnerabilities: case study. Journal of Applied Security Research, 18(3), pp.559-575.

Students are encouraged to read peer reviewed journal articles and conference papers. Google Scholar provides a simple way to broadly search for scholarly literature. From one place, you can search across many disciplines and sources: articles, theses, books, abstracts and court opinions, from academic publishers, professional societies, online repositories, universities and other web sites.