School of Design and Informatics

Supplemental Assessment Instrument Coversheet	(See CMP408 Assessment Brief for full portfolio submission information.)
Module Code:	CMP408
Module Title:	IoT and Cloud Secure Development
Lecturer:	Dr Abdul Razaq, Dr Gavin Hales, Dr Sanaz Kavianpour
Submission Date:	19th Dec. 2023 by 12 noon
Feedback Return Date:	15 working days
Feedback Type:	Written feedback on MyLearningSpace
Grading Criteria:	Refer to Page 6

Learning Outcomes

1. Design and develop systems that incorporate relevant security features for deployment in embedded IoT environments.
2. Critique the benefits and challenges of cloud technologies as a platform for IoT technology.

Submission Requirements

Your assessment must be submitted via MyLearningSpace. The maximum file size which can be submitted is 2.5GB.

Guidance on submitting via MyLearningSpace (Brightspace) is available at: https://intranet.abertay.ac.uk/library/digital-skills/mylearningspace/assessmentfeedback/ , but please contact the Support Enquiry Zone (SEZ) on 01382 308833 or sez@abertay.ac.uk if you have any problems with submitting your work.

Submission of your work after the submission date deadline will be deemed as late submission and will incur a penalty, including the possibility of the work being awarded a non-submission (NS) grade.

To avoid academic deceit and plagiarism, familiarise yourself with the relevant information on Academic Misconduct and procedures available on Abertay University's web pages: https://intranet.abertay.ac.uk/library/referencing/avoidingplagiarism/

You may also want to thoroughly inspect the content following this link in relation to the proper and improper use of AI (e.g., ChatGPT) to avoid academic misconduct: https://intranet.abertay.ac.uk/students/study-skills/guides/generative-ai/

Mini Project - (70% of module grade)

Your task is to undertake a small project related to IoT and Cloud Secure Development. The purpose of this assessment is to allow you to demonstrate the application of the skills you have learned in this module in a way that interests you and to explore the area in general.

You should think of a title or project area that interests you and discuss the suggested content and practical work you will do with class tutors. Some students may choose similar project topics, but each project should have individual practical content and individual documentation. You may wish to consider a project area that you can build on in later work. The project should combine aspects of IoT hardware , software, and cloud.

The practical work should be able to be completed on the equipment you have available and must be demonstrated in a video. Again, discuss any possible problems with your class tutors.

Important notes

- It would be advisable to undertake work that can be done in stages (meaning that some achievement should be possible). Essentially, you should be proving a concept.
- Documentation should be aimed at the other members of the class. Essentially, you should be explaining how to do something (hence, some background will be required in your write-up).
- Not fully achieving your final goal is quite acceptable. However, the documentation should reflect on why it wasn't achieved.

Example Project Ideas

Students are encouraged to think out of the box for intuitive ideas.

- Create an intrusion or ways to break the CMP408 Demo
- GPIO sniffing to hack CMP408 Demo
- A monitor system with an RPi device diver to upload device usage (CPU, Network, RAM, etc.) to AWS
- Interrupt handling and AJAX/PUSH notifications to clients
- HTML client for random number generator or seven-segment display Interface
- Humidity or temperature sensor with HTML interface to view current and saved values
- Weather report station with HTML interface to view current and saved values
- Configure RPi virtual machine with virtual GPIOs
- Configure RPi virtual machine as a server (audio, video, file, mail, etc.)
- Create an LED keyboard with individual keys assigned to each GPIO pin

- IoT device to survey user opinions using buttons and allow results to be seen on a web dashboard
- Vending Machine with web-based User Interface
- Weather report server with IoT environment monitoring

Note: It is common to get carried away with the project and find it difficult to complete. It is advisable that you start with a simple design and gradually include more functionality. Compile and test continuously and fix errors as they occur.

Requirements

Students are expected to adopt the best security practices in all three components of IoT, software, and cloud.

The application menu and submenus should have a consistent layout. Your work should be submitted with complete **source files** and **documentation**. Your project document should follow the below guidelines.

Report

The documentation should **efficiently** describe the work you have undertaken. Your report should **not** exceed more than **1500 words**. Do **NOT** write in the 1st person narrative. You should use a formal writing style for your report.

- Title
- Introduction
    - Importance or relevance of this topic to IoT & Cloud Secure Development
    - Objectives – the tasks or steps that you hope to complete in order to meet the project aim. These should be bullet points.
- Procedure/Methodology
    - This section should explain in detail what you have done for your Project and the relevant security aspects (what did you do to make it secure?)
    - Include any relevant screenshots, diagrams, or pictures. (these should be clearly labelled and referenced in your text, e.g., see Figure 1 for an example of…)
- Conclusion
    - Summarise the Project
    - Discuss how well you met the aim identified in the introduction
- References & Bibliography
    - All sources should be included and written in the Harvard Style of Referencing (6 to 12 references)
    - All references should be cited where applicable in the text of your report
- **Appendices if necessary**

Poster

The project poster should follow the provided template. You can change the colour, theme, or design; however, you must include the sections provided with the template. The students can include (text, images, etc.) their mini-project report in the poster.

Video Demo

A short (around 2 – 5 mins) video demo should be included demonstrating the functionality of your application and highlighting any significant parts of the project. This video will be used to give the markers a better understanding of your project and will reinforce the Report and Poster. The video should be in a common video format such as MP4. The video must be uploaded to MLS. However, you can provide a link to the video on OneDrive/YouTube if there is a valid reason.

You should make sure that the video is accessible to module staff. Examiners will be unable to mark any inaccessible content.

You must talk to staff 2 weeks before the deadline to arrange an in-person demonstration if you are unable to submit a video demo.

IoT, Software and Cloud

These **three** components are implementation based. Students must demonstrate combinations of ideas developed over the module lectures and labs.

The IoT component can be presented with the actual physical device (RPi or any similar platform).

The Software part should demonstrate software design, architecture, and best development practices. Students can use sf.net or similar sources for this component; however, the project report should clearly indicate your contribution and changes.

The Cloud component should integrate various services to form a cohesive system.

Submission Details

Mini Project Submission Details

You should upload a Project ZIP file with PDF Project Report AND PDF Project Poster as part of your portfolio submission. All of your project-related files **(source code, video demo, data, etc.)** should be added to a ZIP file named StudentName-ID.zip; please use your name and student ID to make this filename. You should also upload your Mini Project report as StudentName-ID-Report.pdf and your project poster as StudentName-ID-Poster.pdf.

You should check the zip file on another machine before it is submitted to ensure that it includes all the correct files.

The **FINAL** portfolio submission date/time is on page 1 of this document.

Required Submission Items:

1. StudentName-12345678.zip - Evidence of your implementation that can include your project artefacts such as source code, images, binaries etc.
2. StudentName-12345678-Report.pdf - Your project report in PDF format (Do not upload compressed version).
3. StudentName-12345678-Poster.pdf - Your project poster in PDF format.
4. StudentName-12345678-Video.mp4 - Your project video in MLS-supported format.

Plagiarism

Please see university regulations on plagiarism. Students are encouraged to have discussions and collaboration; however, only original work should be submitted. Plagiarism may result in a zero mark being recorded for the coursework and may result in further action being taken. Please see the University regulations, codes & policies: https://intranet.abertay.ac.uk/library/referencing/avoidingplagiarism/

Students must specify clearly where they obtain material. **This MUST include specific web addresses in the reference section.** You must also check any copyright statements on websites that you use for source material.

Generic Marking Scheme

1. IoT - contribution to the IoT physical device - HW
2. Software - contribution to the system architecture and design in various aspects - such as kernel patching, system call, library, device driver, GUI, web pages, etc.
3. Cloud - contribution to Cloud component with multiple services - MQTT, Store, DB, EC2, web app, AI, etc.

Grades	Comment	Criteria
A/A+	Excellent	Clear and complete understanding of IoT and Cloud Secure Development. Decisions made are logical. Project documentation is clear and concise. Cybersecurity countermeasures are clear and concise. The Project could easily be replicated by a peer.
B/B+	Very Good	Clear and almost complete understanding of concepts of IoT and Cloud Secure Development. Project documentation is clear. Relevant cybersecurity countermeasures are discussed. The Project could be replicated by a peer.
C/C+	Good	Overall, a good understanding of the IoT and Cloud Secure Development. Some of the more integrative aspects or detailed knowledge may be missing. Project documentation covers the project work. Some cybersecurity countermeasures are discussed. The Project could be replicated by a peer with a little research.
D/D+	Satisfactory	A basic understanding of the IoT and Cloud Secure Development. Project documentation covers the topic but may lack in areas (e.g., future work or discussion). Cybersecurity countermeasures are discussed but may not be comprehensive. The Project could be replicated by a peer with some research.
MF	Marginal Fail	A marginally unsatisfactory understanding of some aspects of the IoT and Cloud Secure Development. Knowledge of details and integrative concepts may be mostly missing. The Project could not be replicated by a peer.
F	Fail	A poor or confused knowledge of the material.
NS	No Submission	

Grade	Definition	Description

A	Excellent: Outstanding Performance	Excellent work based on a thorough understanding of the kernel and userspace and security threats originating from such systems. Outstanding performance and achievement overall. The work has considerably exceeded the threshold standard. The characteristics of work at this standard are: The student has developed an excellent understanding of the operation of systems at a low level, i.e., kernel, driver operation, etc., and the security implications arising from such systems. The student had demonstrated excellent skills to design and develop systems that incorporate relevant security features for deployment in embedded IoT environments. The student has developed an excellent understanding of the benefits and challenges of cloud technologies as a platform for IoT technology.
B	Very Good: Commendable Performance	A very good standard of performance and achievement overall. The work is sound and well above the threshold standard, and the student has developed a very good understanding of kernel and userspace and security threats originating from such systems. The characteristics of work at this standard are: The student has developed a very good understanding of the operation of systems at a low level, i.e., kernel, driver operation, etc., and the security implications arising from such systems. The student had demonstrated very good skills to design and develop systems that incorporate relevant security features for deployment in embedded IoT environments. The student has developed a very good understanding of the benefits and challenges of cloud technologies as a platform for IoT technology.
C	Good: Competent Performance	An above competent performance and achievement overall. The work has exceeded the threshold standard, and the student has developed a good understanding of kernel and userspace and security threats originating from such systems. The characteristics of work at this standard are: The student has developed a good understanding of the operation of systems at a low level, i.e., kernel, driver operation, etc., and the security implications arising from such systems. The student had demonstrated good skills to design and develop systems that incorporate relevant security features for deployment in embedded IoT environments. The student has developed a good understanding of the benefits and challenges of cloud technologies as a platform for IoT technology.

D	Satisfactory: Threshold Performance	A satisfactory performance overall (as specified in the detailed marking/grading schemes for each assessment). The work overall is at the threshold standard, and the student has developed a basic understanding of kernel and userspace and security threats originating from such systems. The characteristics of work at this standard are: The student has developed a satisfactory understanding of the operation of systems at a low level, i.e., kernel, driver operation, etc., and the security implications arising from such systems. The student had demonstrated satisfactory skills to design and develop systems that incorporate relevant security features for deployment in embedded IoT environments. The student has developed a satisfactory understanding of the benefits and challenges of cloud technologies as a platform for IoT technology.
MF	Marginal Fail	The work overall is just below the threshold standard, and the student does not have a complete understanding of the kernel and userspace and security threats originating from such systems. Work just below the threshold standard is characterised by the candidate demonstrating: The student has developed a marginally unsatisfactory understanding of the operation of systems at a low level, i.e., kernel, driver operation, etc., and the security implications arising from such systems. The student had demonstrated marginally unsatisfactory skills to design and develop systems that incorporate relevant security features for deployment in embedded IoT environments. The student has developed a marginally unsatisfactory understanding of the benefits and challenges of cloud technologies as a platform for IoT technology. There should be a reasonable expectation that students in this grade category will be able to demonstrate competence through further study and assessment (e.g., re-assessment).
F	Clear Fail	Performance well below the threshold level. Some or very limited evidence of the achievement of the outcomes.