Middlesex University Mauritius

CST2310
IS Analysis & Design

Coursework 3 – Final Individual Assessment

Autumn/Winter term 2023/2024

Date of Submission: 12th April 2024

Student Name: Arusha Ramessur

Student ID Number: M00940320

Lab Tutor: Parvesh Seeburrun

Table of Contents

List of Figures

Question 1

a) Class diagram:

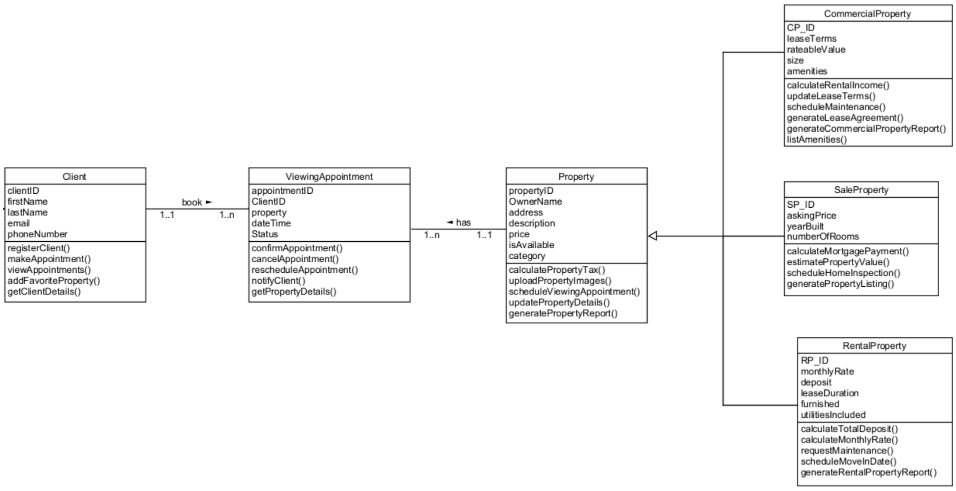


Figure 1 - Class Diagram

b) Define what Superclass and Subclass means. In your definition refer to the idea of Inheritance for the purposes of illustration.

The generalization relationship expresses that the attributes and operations that are specified for a general class (superclass) are passed on to its subclasses. The superclass class is known to be the parent class whereas the subclass is known as the child class. Therefore, the generalization relationship is also referred to as inheritance.
(Seidl et al., 2012).

A subclass inherits all the characteristics of its superclass. This means the subclass possesses all class attributes and operations of the superclass. The subclass may also have further attributes and operations independently of its superclass.
(Bennett, Mcrobb and Farmer, 2014).

Example of generalization:

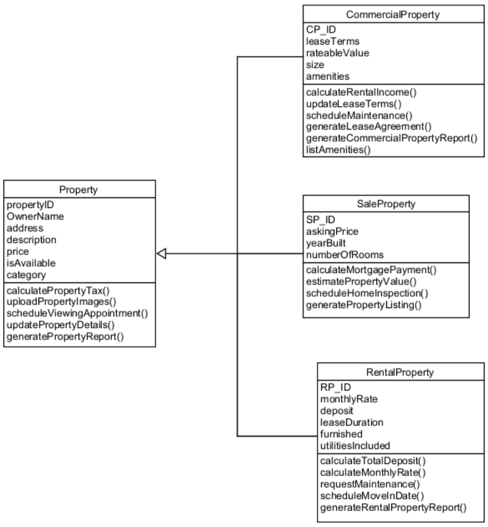


Figure 2 - Example of generalization

Question 2

a) What are the three fundamental things shown on a Use Case Diagram and what do these three things represent?

The 3 fundamental things shown on a use case diagram are:

- Actors:
  The actors work and interact with the system. Actors represent the roles that a person, another system or even a hardware device take on when communicating with the particular use cases in the system.
  (Bennett, Mcrobb and Farmer, 2014).

- Use cases:
  A use case describes functionality expected from the system to be developed. Use cases represent what the customer wants the system to do, that is, the customer's requirements of the system. Use cases represent a set of interactions between the system and its actors to accomplish a specific goal. The use cases show what the future system is for. *(Seidl et al., 2012).*

- The system:
  The system encompasses a number of functions, which are the use cases that are executed. It defines the scope of the system being modeled and knows what is inside the system. *(Bittner & Spence, 2008).*

b) Use case diagram:

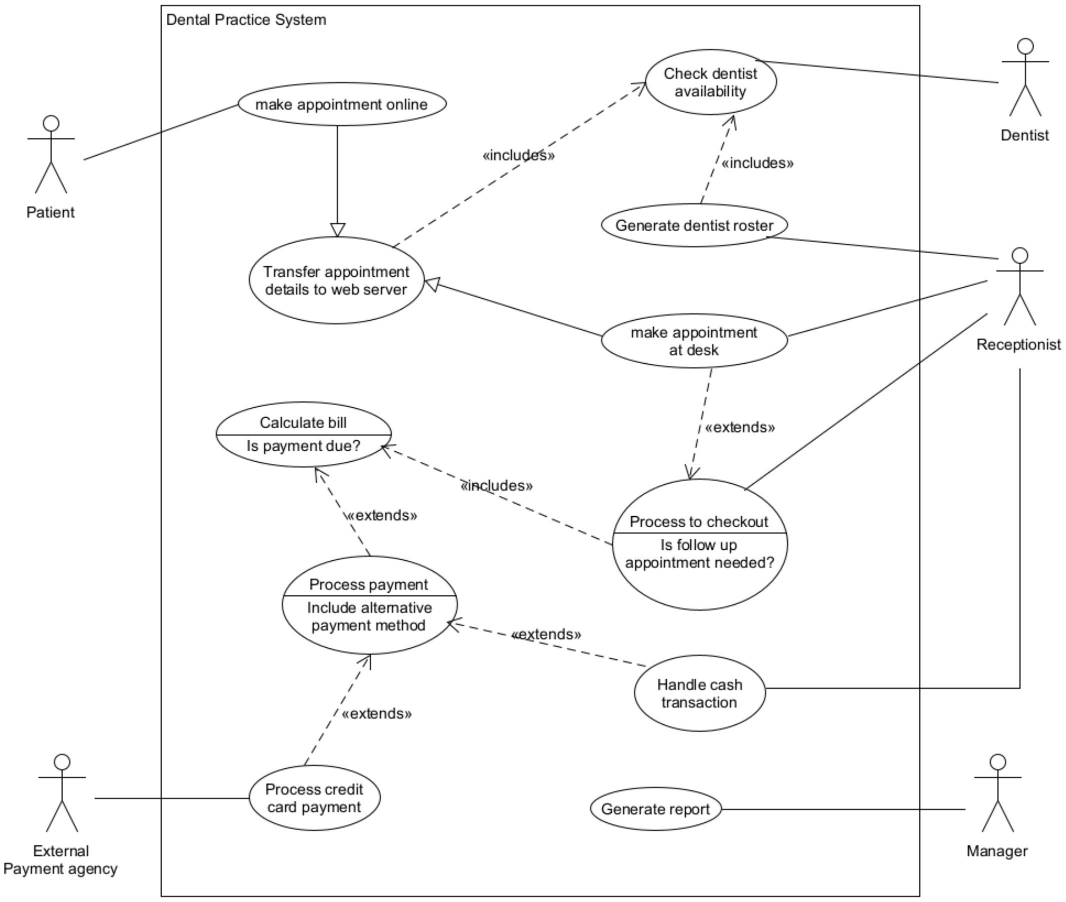
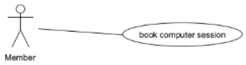


Figure 3 - Use Case Diagram

Question 3

a) Sequence diagram:



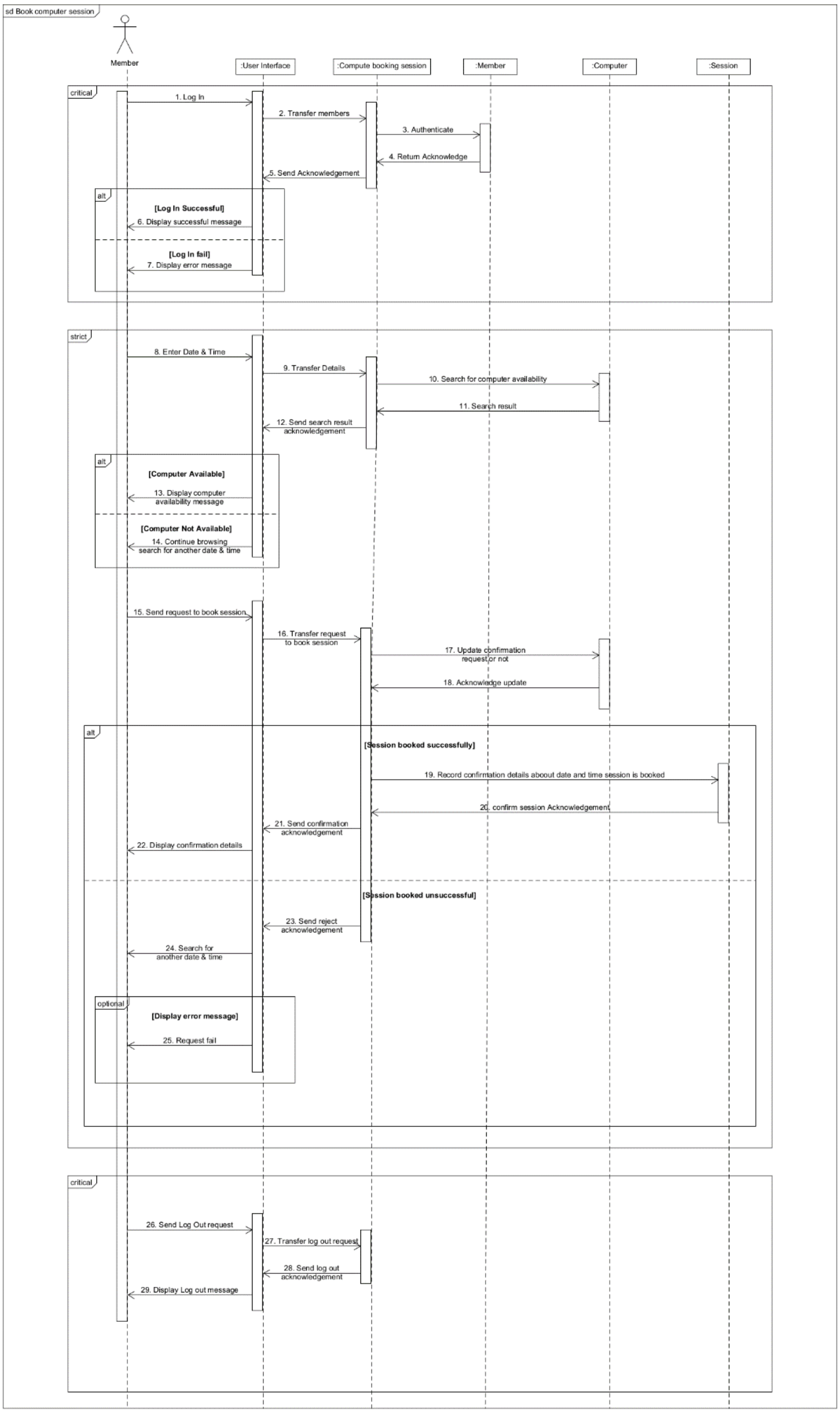

sd Book computer session
Member
:User Interface
:Compute booking session
:Member
:Computer
:Session
critical
1. Log In
2. Transfer members
3. Authenticate
4. Return Acknowledge
5. Send Acknowledgement
alt
[Log In Successful]
6. Display successful message
[Log In fail]
7. Display error message
strict
8. Enter Date & Time
9. Transfer Details
10. Search for computer availability
11. Search result
12. Send search result acknowledgement
alt
[Computer Available]
13. Display computer availability message
[Computer Not Available]
14. Continue browsing search for another date & time
15. Send request to book session
16. Transfer request to book session
17. Update confirmation request or not
18. Acknowledge update
alt
[Session booked successfully]
19. Record confirmation details aboout date and time session is booked
20. confirm session Acknowledgement
21. Send confirmation acknowledgement
22. Display confirmation details
[Session booked unsuccessful]
23. Send reject acknowledgement
24. Search for another date & time
optional
[Display error message]
25. Request fail
critical
26. Send Log Out request
27. Transfer log out request
28. Send log out acknowledgement
29. Display Log out message

Figure 4 - Sequence Diagram

b) **Explain how Sequence Diagrams model the dynamic structure of the system.**

Class diagrams capture the system's building blocks (classes) and their relationships, representing the static structure. Sequence diagrams, in contrast, illustrate the dynamic interactions between these classes over time and focus on the message flow between objects in a specific scenario. This dynamic aspect allows developers and stakeholders to visualize the behavior of the system in various scenarios, aiding in the understanding of how different components collaborate to achieve specific functionalities. In other words, class diagrams define the "who" (classes) and "what" (relationships) of the system, while sequence diagrams show the "how" (message flow) and "when" (activation time) of its functionalities.
(Larman & Kruchten, 2005).

Question 4

a) **In 2015 TalkTalk had a cyber-attack committed on its website, where approximately 157,000 of its customers' personal details were accessed. In response the UK Information Commissioner's Office declared: "Telecoms company TalkTalk has been issued with a record £400K fine by the ICO for security failings that allowed a cyber-attacker to access customer data 'with ease'". The General Data Protection Regulation (GDPR) as it applies in the UK, is adopted via the Data Protection Act 2018. Article 5 of the GDPR sets out seven key principles. Identify the data protection principle that can be cited to substantiate the action taken by the ICO against TalkTalk? Make sure you cite the reference(s) to show where you sourced this information from. Use Harvard Referencing and ensure that you have both intext reference(s) and the full reference(s) provided.**

The data protection principle that can be cited to substantiate the action taken by the ICO against TalkTalk is the principle of integrity & confidentiality, outlined in Article 5(1)(f) of the General Data Protection Regulation (GDPR).

According to Article 5(1)(f) of the GDPR, personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures. *(ICO, 2017).*

The ICO's action against TalkTalk for security failings that allowed a cyber-attacker to access customer data 'with ease' aligns with this principle, as TalkTalk failed to implement adequate security measures to protect its customers' personal data from unauthorized access. *(Hern, 2016).*

b) **Amongst other things the GDPR introduces: 1) increases in territorial scope; 2) increases in penalties; 3) matters on consent and 4) breach notifications; 5) rights on data erasure and 6) privacy by design. For any 3 listed explain what duties are placed on: data controllers/processors and/or systems designers. Make sure you substantiate these explanations via the citation of reference(s). Use Harvard Referencing and ensure that you have both intext reference(s) and the full reference(s) provided.**

1. Increases in Penalties:

Data controllers/processors have the duty to ensure compliance with the GDPR to avoid penalties. They must implement effective measures to mitigate potential damage resulting from infringements, collaborate with supervisory authorities during investigations, and demonstrate compliance with GDPR requirements. Intentional infringements, failure to mitigate damages, or lack of collaboration with authorities can increase penalties. For severe violations listed in Article 83(5) of the GDPR, fines can be up to €20 million or 4% of the total global turnover of the preceding fiscal year, whichever is higher. Even for less severe violations in Article 83(4), fines can be up to €10 million or 2% of the total global turnover, whichever is higher. *(Haag & Logemann, 2021).*

2. Matters on Consent:

Data controllers/processors have several duties regarding consent under Article 7 of the GDPR. They must be able to demonstrate that data subjects have consented to the processing of their personal data. Consent must be obtained in a clear, intelligible, and easily accessible form, separate from other matters, and presented in plain language. Data subjects have the right to withdraw their consent at any time, and withdrawing consent should be as easy as giving it. Data controllers/processors are responsible for informing data subjects of their right to withdraw consent before obtaining consent for processing activities. *(Haag & Logemann, 2021).*

3. Privacy by Design:

System designers have significant duties under Article 25 of the GDPR to integrate privacy into the design of systems and processes. They must implement appropriate technical and organizational measures, considering factors such as the state of the art, cost, nature, scope, context, and purposes of processing, as well as the risks to individuals' rights and freedoms. These measures should aim to implement data protection principles effectively, such as data minimization, and ensure that only necessary personal data are processed for each specific purpose. By default, personal data should not be made accessible without the individual's intervention. *(Haag & Logemann, 2021).*

c) **Security controls can be viewed as being a combination of manual and automated measures that can be used to safeguard information systems to ensure that they perform according to management standards. There are four broad categories of controls: physical, software, electronic and**

management. Select any 4 technologies, from across these four categories, and explain how they work to protect information systems. Make sure you substantiate these explanations via the citation of reference(s). Use Harvard Referencing and ensure that you have both intext reference(s) and the full reference(s) provided.

1. Alarm Systems (Physical Control):

Alarm systems are physical security controls designed to detect unauthorized access or intrusion into a facility. They typically consist of sensors, such as motion detectors or door/window sensors, connected to a central monitoring station. When an unauthorized entry is detected, the alarm system triggers an audible and/or visual alarm to alert security personnel or authorities. Alarm systems act as a deterrent to potential intruders and provide early detection of security breaches, allowing for a rapid response to mitigate risks. *(Fennelly, 2017).*

2. Fingerprint Recognition (Electronic Control):

Fingerprint recognition is a biometric security control used to authenticate the identity of users accessing information systems. It works by capturing and analyzing unique patterns in an individual's fingerprints, which are then compared against stored templates to verify identity. Fingerprint recognition offers a high level of security as each person's fingerprint is unique and difficult to forge. It provides a convenient and reliable method of access control, enhancing the security of information systems by ensuring that only authorized users gain access. *(Jain et al., 2011).*

3. Encryption (Software Control):

Encryption is a software-based security control used to protect data by converting it into a coded form that can only be accessed with a decryption key. It ensures the confidentiality and integrity of sensitive information, both when stored and during transmission over networks. Encryption algorithms use complex mathematical techniques to scramble data, making it unreadable to unauthorized users. By implementing encryption, information systems can prevent unauthorized access and data breaches, even if attackers gain physical or electronic access to the data. *(Schneier, 2015).*

4. Disaster Recovery Plan (Management Control):

A disaster recovery plan is a management control that outlines procedures and protocols for restoring information systems and business operations in the event of a catastrophic event, such as natural disasters, cyberattacks, or equipment failures. It includes measures for data backup, system recovery, alternate site operations, and communication with stakeholders. A well-defined disaster recovery plan helps organizations minimize downtime, mitigate risks, and ensure continuity of operations during emergencies. *(Olanda, 2020).*

References

Bennett, S., Mcrobb, S. and Farmer, R. (2014). *Object-oriented systems analysis and design: using UML*. Johanneshov: MTM.

Bittner, K. and Spence, I. (2008) Use case modeling. Boston, MA: Addison Wesley.

Fennelly, L. (2017) *Effective physical security (fifth edition)*. Butterworth-Heinemann.

Haag, N.C. and Logemann, T. (2021) *Art. 5 GDPR – principles relating to processing of personal data*, *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/art-5-gdpr/.

Hern, A. (2016) *TalkTalk hit with record £400k fine over cyber-attack*, *The Guardian*. Available at: https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack.

Information Commissioner’s Office (ICO). (2017) Monetary penalty notice: TalkTalk Telecom Group PLC [MPN – TalkTalk - 20170807]. https://ico.org.uk/media/action-weve-taken/mpns/2014626/mpn-talktalk-20170807.pdf

Jain, A.K., Ross, A.A. and Nandakumar, K. (2011) *Introduction to biometrics*. New York: Springer.

Larman, C. and Kruchten, P. (2005) Applying UML and patterns: An introduction to object-oriented analysis and Design. New Jersey: Pearson Education.

Olanda (2020) *ITIL® 4 specialist high velocity it (HVIT) courseware*. ’s-Hertogenbosch: Van Haren Publishing.

Schneier, B. (2015) *Applied cryptography: Protocols, algorithms, and source code in C*. Indianapolis: John Wiley & Sons.

Seidl, M., Scholz, M., Huemer, C., Gerti Kappel and Springerlink (2012). *UML @ Classroom: An Introduction to Object-Oriented Modeling*. Cham: Springer International Publishing.