Networking and Data Exchange Extended

Question 1

21 marks

An e-commerce platform needs to securely exchange sensitive customer order details (e.g., customer name, address, order items, total amount) between its public-facing web server and its internal database system.

a) Data Exchange Format Justification: (7 marks) Compare JSON and XML as data exchange formats for transmitting customer order data from the web server to the internal database. Justify which format is more suitable for this e-commerce platform, providing two distinct reasons by referring to their key features and practical advantages or disadvantages in this context.

b) Network Protocol and Security: (8 marks) Explain how the HTTPS network transmission protocol ensures the confidentiality and integrity of this data during transfer over the internet. Contrast its role and underlying mechanisms with those of HTTP in terms of data protection.

c) Data Privacy Considerations: (6 marks) Identify two Australian Privacy Principles (APPs) relevant to handling sensitive customer order data in this e-commerce scenario. For each identified APP, explain how the e-commerce platform should implement it to ensure ethical data collection and use.

Marking Guide – Question 1

Part A

Marks	Criteria	Evidence of achievement
1	Identifies JSON	States JSON is a lightweight, text-based data format.
1	Identifies XML	States XML is a markup language with tags and nested structure.
1	Explains JSON advantage	Notes JSON has smaller file size or faster parsing.
1	Explains XML disadvantage	Notes XML is more verbose, complex, or slower to process.
1	Links JSON to web technologies	Explains JSON is natively supported in JavaScript and widely used in web APIs.
1	Contextual justification 1	Justifies JSON as more suitable due to efficiency in transmitting order data.
1	Contextual justification 2	Justifies JSON as more suitable due to easier integration with web/database systems.

Sample Response

JSON is a lightweight, text-based data format that represents data as key–value pairs. XML is a markup language that stores data in nested tags with attributes. JSON is more suitable for an e-commerce platform because:

- JSON is smaller and faster to parse than XML, which reduces bandwidth use and improves performance when transmitting large volumes of customer order data.
- JSON is natively supported in JavaScript and most modern web APIs, which simplifies integration between the web server and the database system.

In contrast, XML is more verbose, harder to read, and requires additional processing overhead. For an e-commerce system requiring efficiency and fast order processing, JSON provides practical advantages.

Part B

Marks	Criteria	Evidence of achievement
1	Identifies HTTP	States HTTP transmits data in plain text without encryption.
1	Identifies HTTPS	States HTTPS is HTTP with added encryption layer (SSL/TLS).
1	Explains confidentiality mechanism	Explains HTTPS encrypts data, preventing interception by attackers.
1	Explains integrity mechanism	States HTTPS uses hashing or digital signatures to ensure data is not altered.
1	Explains authentication mechanism	Describes use of digital certificates to verify server identity.
1	Contrasts HTTPS vs HTTP (confidentiality)	Notes HTTPS protects sensitive data, HTTP exposes it to interception.
1	Contrasts HTTPS vs HTTP (integrity)	Notes HTTPS ensures data remains unmodified, HTTP has no such guarantee.
1	Contextual application to e-commerce	Explains HTTPS ensures customer details remain private and secure in online transactions.

Sample Response

HTTP transmits data in plain text, which means sensitive details such as customer names, addresses, and payment information can be intercepted or modified during transfer. In contrast, HTTPS adds an encryption layer using SSL/TLS.

- Confidentiality: HTTPS encrypts the data using symmetric session keys, preventing third parties from reading customer order details.
- Integrity: HTTPS uses hashing and message authentication codes to detect tampering. If the data is altered in transit, the recipient can verify this.
- Authentication: HTTPS relies on digital certificates issued by trusted Certificate Authorities (CAs) to prove the legitimacy of the server, preventing "man-in-the-middle" attacks.

Thus, HTTPS ensures secure communication between the web server and database system, protecting customer data from interception and modification. HTTP offers no such protections.

Part C

Marks	Criteria	Evidence of achievement
1	Identifies first APP	States APP 5 (Notification of collection).
1	Explains APP 5	Requires informing customers when personal data is collected.
1	Implementation of APP 5	States platform should provide clear privacy notices during checkout.
1	Identifies second APP	States APP 11 (Security of personal information).
1	Explains APP 11	Requires organisations to take reasonable steps to protect personal data.
1	Implementation of APP 11	States platform should use secure storage, access control, and encryption of databases.

Sample Response

Two relevant Australian Privacy Principles (APPs) are:

- APP 5 (Notification of collection): The e-commerce platform must inform customers at checkout that their personal data (name, address, order details) is being collected, why it is needed, and how it will be used. This can be implemented through a clear privacy policy and on-screen notices before data submission.
- APP 11 (Security of personal information): The platform must take reasonable steps to protect customer data from misuse, interference, or unauthorised access. This includes encrypting customer details in the database, using access controls to restrict staff access, and applying regular security updates.

By implementing these APPs, the platform ensures transparency, accountability, and ethical handling of customer information.