1.

a. Security attacks essentially occur when a third party enters the picture and attacks or edits the data, resulting in a data breach. This information might also be misused. The various security threats that specifically apply for this e-commerce operator are:

- It is vulnerable from an attack launched from within a system or organization's perimeter, either by an unfriendly party or one of its own employees. It is risky because internal attackers often already know how the system is set up and are aware of its vulnerabilities, whereas external attackers must first get past the firewall by breaking into the network before they can access the system.
- The computers and mobile devices of the e-commerce operator are capable of stealing the private and sensitive information of the users. Hackers can access your system by visiting infected websites, downloading suspicious files, or opening links or attachments in emails.
- It has a threat from someone who could steal another person's payment information without their consent in order to make purchases or withdraw money.
- It has a threat from Cyber attacks. The objective of a cyberattack would be targeting directly at the e-commerce providers to interfere with their networks' or operators' regular operations. This could be accomplished by continuously burdening the server or network with traffic.
- A cyber criminal would access or steal the user's or the company's sensitive or vital data or information without the system's consent.

b. How would I design usability studies for building such platform:

- Choosing the participant base: A good selection of study participants is essential to guaranteeing that the results appropriately reflect the target population. As a result, the study population's selection ensures accurate data collection. We can also consider engaging UX professionals to help identify potential problems.
- Tasks: defining what they will actually be doing during a usability test. They should be given a task to complete. It needs to be brief enough to cut down on participant commitments.
  • Synchronizing events to communicate tasks: Establishing a hypothetical situation in the real world based on the website, its functions, and its aim. Scenarios give some illustrative background information.
- Finding Participants: Once you've found the correct participants, it will be simple to repeat the scenario-playing and feedback-gathering process. It's critical to choose sources that best reflect the experience and education of the intended audience.
- • Carrying out the study: Now that everything is set up, it's time to conduct the test. Introduce yourself and the study at the beginning. After then, you can continue with the tasks and inquire further about each one as you do it. Once all the tasks have been done, you can move on to the main questionnaire, where you'll be asking about their overall impression of the platform.
- Examining data: The results of the usability testing need to be examined to find any areas that could use improvement. It's crucial to take thorough notes while conducting the test in order to achieve this.

● Enumerate useful feedback: We develop ever-better models as we get knowledge of what individuals require by testing and analyzing the outcomes. Yet because we're learning, we constantly test and adjust what we're doing.

c. Designing a usable data sharing protocol with built in security mechanisms to prevent data theft and mechanisms would work for this specific scenario as:

- Inform all staff members of information security guidelines and provide them with guidance on how to handle issues as they emerge.
- If your platform is still running an outdated version of Windows, request an update from the IT team.

- Employ agreed or specified protocols to communicate across the web securely and effectively.
- Download a trustworthy ransomware blocker right away.
- Configure access control, a security measure that can be used to limit who or what can access network resources.
- Always make a backup of your data, encrypt it online, and if at all possible, save it offline.
- Use security technology to keep an eye on and examine database activity that runs outside of the DMS.
- To find and address any flaws in your security framework, do frequent security audits and security testing.
- Employ encryption to protect data so that it is hidden from the public eye and only accessible to the people we want to see it.
- To provide an additional layer of security, enable multi factor authentication on all application endpoints throughout your networks.

This would work for this specific scenario as it has strong security measures that are intended to guard against data theft and manipulation. Additionally, it makes sure that personally identifiable information is deleted or anonymized to preserve the privacy of the customers and that the data can only be accessed by authorized workers who need it to carry out their job duties. Ultimately, the data is always kept private and secure because of the implementation of frequent security evaluations and legal responsibilities.

d. Guarantees the protocols described in (C) provide for data confidentiality and integrity:

• Confidentiality: Giving information only to those who have the proper authorization to access the particular sensitive material; otherwise, the data would be encrypted during its transfer and storage, protecting it from being accessed by unauthorized parties.

• Integrity: Data must remain consistent in its general completeness, correctness, and consistency throughout its entire lifecycle, and measures must be taken to prevent unauthorized parties from altering the data while it is in the stage of Transfer.

Specific scenarios where they fail are:
● The computers and mobile devices of the e-commerce operator are capable of stealing the private and sensitive information of the users. Hackers can access your system by visiting infected websites, downloading suspicious files, or opening links or attachments in emails. This may harm confidentiality.

- An attacker may gain access to sensitive data if they can persuade and read the thoughts of an authorized user into disclosing their login information.
- Itis vulnerable from an attack launched from within a system or organization's perimeter, either by an unfriendly party or one of its own employees. It is risky because internal attackers often already know how the system is set up and are aware of its vulnerabilities, whereas external attackers must first get past the firewall by breaking into the network before they can access the system.
- The security measures might not work if a new vulnerability is found and used by attackers before it is fixed.

2.
a.
As a security architect, I would design and employ usable encryption mechanisms that would prevent MITM based security breaches:

- A method known as "certificate pinning" links a server's public key to a particular certificate. By confirming that the client is connecting with the intended server and not a faked one, this helps avoid MITM attacks.

● Inform users of the dangers of MITM attacks and how to protect themselves. This entails staying away from public Wi-Fi hotspots, looking for active SSL/TLS certificates, and creating strong passwords.

- A popular encryption technology called SSL/TLS may encrypt data traveling between clients and servers. By encrypting sensitive data in transit, this helps to avoid MITM attacks.
- Develop secure and difficult-to-crack encryption techniques.
- The best defense against MITM is provided by VPN services which provide secure communication channels. Even if you access HTTP websites, these services will encrypt your connection to shield you from MITM assaults.

● Ensure that only individuals with permission can access sensitiv data by using access control technologies like Role-Based Access Control (RBAC).
● Determine the resources that require protection and potential attack scenarios. A threat model assists in your understanding of the security precautions required to reduce potential dangers.
● By requesting two different forms of identity from users before granting access to a system, 2FA offers an extra layer of security. By guaranteeing that only authorized users have access to sensitive data, this helps avoid MITM attacks.

- Software and systems should be updated often to keep them secure against known vulnerabilities.

b. Key management protocol are:

● Key Generation: Either the key distribution center, a specific user, or sender will provide the key. They will be encrypted, and depending on the level of security, the size and difficulty should be chosen.

- Key Storage: To avoid illegal access, modification, or theft, keys must be kept safely. The keys can be protected from numerous attacks using both logical and physical security techniques.
- Key Distribution: A key must be securely transmitted to the appropriate users when it has been generated. Using a secure communication route may be necessary for this.
- Key usage: The key will encrypt and decrypt data while it is being transmitted.
- Key deregistration: The key will be deregistered by the authorized authenticated third party after session is timed out or we can say session is completed, which is when data has been delivered by the sender and received by the receiver.

Few scenarios where protocol may fail are:

- Users who might attempt to steal patents or sensitive data when they depart the company. Sometimes IT administrators will attempt to hurt the company or steal data. They may remove files that destroy infrastructure or even create accounts throughout the company that will allow them to return and reclaim data.
- The keys run the risk of being seized, stolen, or used improperly ifthey are shared with unauthorized individuals or through an unsecured channel. This can occur when the SSL or VPN connection is exploited, the CA is unreliable, or the keys are distributed among several users or programmes.
- The keys could be vulnerable to physical or logical attacks if they are kept in an unsecure area or if the appropriate encryption, passwords, or access controls are not used. This may occur ifthe keys are kept on a hard drive that is not encrypted, ifthe passwords are insecure or shared, or ifthe access controls are set up improperly.
- The generated keys may be weak and vulnerable to brute-force attacks if the key generator was defective, biased, or predictable. This may occur if the key-generation algorithm is incorrect or the random number generator is not genuinely random.

C. More comprehensive solutions for such situations are:

- Do regular security risk analyses and penetration tests to find and fix any network security flaws.
- Safeguards you against threats like viruses, ransomware, and malware. Watches for malicious activity and then deploys a protection mechanism in response.
- Establishing networks inside networks, or subnets within subnets. Segmentation reduces the number of broadcast domains and eliminates extraneous network traffic, allowing for more effective use of resources. By decreasing an organization's attack surface, it improves security.
- Watch out for any strange activity in the network traffic that can point to an ongoing MITM assault.
- To ensure that only permitted individuals can access the network, use strong authentication mechanisms like two-factor authentication.

- Use end-to-end encryption on all channels of communication to stop hackers from snooping on and reading private data.
- For remote access, a VPN can be used to secure the communication paths.
- Use intruder detection as well as preventative systems and firewalls to track and stop illegal access attempts.
- To encrypt communication and verify identity, employ digital certificates and a public key infrastructure.
- Configure access restrictions to provide only authorized personnel an access to sensitive data.
- To inform staff members of the dangers of MITM attacks and how to spot and report unusual activity, hold regular security awareness training sessions.
- Create a security incident response plan that describes what has to be done in the event when an MITM attack is successful.

Bonus. If certificate-based scheme is not allowed, key management protocols can still be implemented:

- Key Generation: Either the key distribution center, a specific user, or sender will provide the key. They will be encrypted, and depending on the level of security, the size and difficulty should be chosen.
- Key Distribution: A key must be securely transmitted to the appropriate users when it has been generated. Using a secure communication route may be necessary for this.
- Key usage: The key will encrypt and decrypt data while it is being transmitted.
- Key deregistration: The key will be deregistered by the authorized authenticated third party after session is timed out or we can say session is completed, which is when data has been delivered by the sender and received by the receiver.
- Key Storage: To avoid illegal access, modification, or theft, keys must be kept safely. The keys can be protected from numerous attacks using both logical and physical security techniques.

Few scenarios where key management protocol may fail are:

- Users who might attempt to steal patents or sensitive data when they depart the company. Sometimes IT administrators will attempt to hurt the company or steal data. They may remove files that destroy infrastructure or even create accounts throughout the company that will allow them to return and reclaim data.
- The keys run the risk of being seized, stolen, or used improperly if they are shared with unauthorized individuals or through an unsecured channel. This can occur when the SSL or VPN connection is exploited, the CA is unreliable, or the keys are distributed among several users or programmes.
- The keys could be vulnerable to physical or logical attacks if they are kept in an unsecure area or if the appropriate encryption, passwords, or access controls are not used. This may occur if the keys are kept on a hard drive that is not encrypted, if the passwords are insecure or shared, or if the access controls are set up improperly.

- The generated keys may be weak and vulnerable to brute-force attacks if the key generator was defective, biased, or predictable. This may occur if the key-generation algorithm is incorrect or the random number generator is not genuinely random.

3.

a.

To convince Bob of her hypothesis, she needs to:

- Get an alternative to Bob's original dataset that was used to train the model and is indicative of the road environment.
- On the new dataset, build the RL-MDP model.
- Record the model's correctness and safety protocols after analyzing its performance on the new dataset.
- Drive the vehicle on the new road environment using the RL-MDP model, and note any risky or unexpected behavior.
- To find any recurring patterns or the model's failure modes, analyze the recorded data.
- Determine the model's sensitivity to environmental influences by changing the weather and illumination during the test.
- Dynamic barriers should be included to evaluate the model's adaptability to unforeseen circumstances. Change the road's texture and signs to give the model additional obstacles to overcome.
- To test the model's ability to react quickly and make decisions, raise the car's speed.
- Check the model's capacity to handle foreseeable circumstances.
- Test the model's resistance to attacks using an aggressive attack to alter the input data.
- Use the model to drive on a wholly distinct road network to evaluate its capacity to generalize to new contexts.
- Report the findings in detail, highlighting the model's shortcomings, failure mechanisms, and recommendations for enhancement.

b. Two different solutions for improving the robustness of his RL-MDP based model are:

- Use a strategy to enhance the performance of AI models. The model's robustness can also be increased using it, in a similar manner. By adding several forms of modifications to the training photos, such as brightness, contrast, rotation, and translation, Bob can improve the data sets. The model can learn to generalize to new contexts more effectively by being trained on a varied set of training data. He can also add randomness to the training procedure to mimic the uncertainty seen in the actual world.
- Using regularization techniques during training is another option to increase the robustness of the model. By punishing excessive weights and bias values, regularization techniques like L1 and L2 regularization can assist reduce overfitting and enhance the model's generalization performance. Bob can also lessen co-adaptation between the models by using strategies like dropouts and early pausing to increase their robustness. These methods can assist the model in learning more broad properties that apply to a variety of road situations rather than memorizing specific examples from the training

data.