1. To preserve the confidentiality of customer’s credit card information, there are two scenarios that need to be consider according to the question
2. Store of credential :- since the customer might want to save the card information for future transactions, it make sense that the information can’t be stored as is. It has to be secured. Thus strong encryption techniques need to be implemented to store confidential data in encrypted form
3. Security of data in transit :- During a transaction, the credit card information is in transit in between networks. Thus, it is exposed to the risks in a network. Thus strong network layer protocols must be used such as SSL (Secure Socket Layer) and TLS (Transport Layer Security) to preserve and protect the data from potential attackers during a transaction
4. Since the company is processing credit card information, it need to comply with payment cards industry data security standard (PCI - DSS)

This is so because any organization processing credit card information hast to be compliant with this standard as it is a legally mandatory. This standard enlists security measures that need to be taken by organization to safeguard protected information of customers. Under this standard, following this are covered

1. Security of data while storage in order to ensure privacy
2. Security of data in transit in order to prevent data theft
3. Code audits in order to make code better and free from loopholes