Introduction: In e-commerce application, the payment steps of the shopping which is made by users, the Credit card, Money Order or Cash on delivery are became very popular. And users preferred these process. These kinds of payment method stored in application database due to its ease of use. Recently, Cyber-attacks have increased at a much higher rate because data leaks are occurring in e-commerce application. For the reason of data leaks, unauthorized transactions are  
occurred by the using of the credit card information of the customers and material losses occur. These kinds of problems are arising from the storage of customer credit cards position a threat to both customers and e-commerce applications. E-commerce applications have the responsibility for securing storage of credit card information in the database. Although the use of SSL(**Secure Sockets Layer** , it is the standard technology for keeping an internet connection secure with any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details) in client-server communication of e-commerce applications which provides communication security but does not provide database security. That’s why data encryption methods are used for ensuring security.

The security of credit cards which is tried to be determined by the Payment  
Card Industry-Data Security Standard (PCI-DSS) standard which is the common security standard for the use, protection, storage, and transmission of credit card data ,recommended by MasterCard and VISA .

An e-payment system should have the following four security features:

1) Authentication: customer and merchant should be authenticated against each other before the transaction takes place.

2) Confidentiality: sensitive data such as credit card number and customer’s PIN (Personal Identification Number) should be inaccessible to any unauthorized user.

3) Data Integrity: data transferred during the transaction should be tamper-proof.

4) Non-repudiation: DoS from any entity during the transaction should not take place.

There is the most difficult part of storing sensitive data is ensuring data security and integrity. For ensuring data security and integrity Data  
Loss Prevention (DLP), intrusion detection (IDS), or prevention systems (IPS) are used .

Recently, blockchain technology which is using cryptographic methods that has been introduced to protect data security and integrity.

A blockchain-based model is used for securing storage of credit card information in e-commerce applications. SHA256 hash algorithm is used for the data integrity of the model. Since the hash is a one-way function which encrypted data that cannot be restored. Therefore, the credit card information is reused by the customer which is encrypted with the AES symmetric algorithm.