As days are passing online payments is getting popular and for this people uses various modes of payment like Debit card, Credit Card, electronic wallet, e-banking etc. People purchase products over the internet and also pay the bill online, which is easy to implement and also saves the time. But the only question that comes in the mind of every person is about the security of data which has been shared by the person while online payment

When it comes to the communication of sensitive data security has always been an important topic. With hardware advances allowing users the advantage of accessibility used in mobile devices, individuals are now spending more and more time on these devices. Additionally, with the viral popularity of social media applications and single sign-on, users do not always take as many precautions as needed with their information. Multi-factor authentication creates more and varied walls to block out the wrong people from seeing your information

Basically now-a-days mobiles comprises of the basic authentication required which can be treated as the first factor authentication and the other two factors need to be implemented as follows,

The process of authentication is essential for allowing users to enter credentials and if they matches with the existing one then user is authenticated user and is allowed to login to the system otherwise not. This is the initial factor authentication which also gives control access to system by verifying each user and giving access to only verified ones. Now Addition of other factor authentication is a security mechanism which uses two of the three factors of credentials for authentication. The two-factor authentication works with two separate security mechanisms. Typically one is a physical validation token, and one is a logical code or password. Both must be validated before accessing a secured service or product. Now coming to the multiple factor authentication is a mobile authentication/ financial transaction System using a unique mobile identification code and method thereof, where in mobile authentication and/or financial transaction are carried out without replacing a mobile communication terminal in Such a way that various authentication and/or financial transaction are performed based on the unique mobile identification code received from a mobile communication terminal according to a Standardized mobile communication protocol

And the flow of implementation will be as follows, The merchant will first register a source of funds and a payer device with a unique ID with the payment server. Then once a merchant and the payer have agreed on a financial transaction amount, the merchant requests a transaction ID from the payment server for that amount. The payment server sends the merchant a transaction ID, which the merchant then communicates to the payer. The payer in turn relays this transaction ID to the server, which validates the transaction using the payer device. The server then releases funds to the merchant. The server can preserve all records for auditing purposes, but security is enhanced because the merchant never gets direct access to the customer's financial account information

Therefore we consider 4 phases in the transaction flow of the system as follows,

1. Firstly, the basic login i.e validating the credentials of user/payer

2. Performing of Two factor authentication

3. Now validating of the Transaction Identification Code (TIC).

4. SMS Confirmation.

In an alternative approach that is used by some mobile payment services providers, for example Ericsson IPX, to purchase online goods, the payer (i.e. customer) provides a mobile phone number to merchant, which then presents the phone number to the Ericcson payment system. The payment system in-turn provides the payer with a short passcode number (PIN). The payer gives this PIN to the merchant. Upon receiving this PIN, the merchant then releases the on-line goods. The payment funds ultimately come from the payer's mobile phone bill.

The drawback of this approach is payer needs to share his personal information, for example phone number with the merchant site. Separately this process is bit inconvenient for the payer since he has to first enter information on the payee site and then read PIN from his cell phone, and then enter PIN into merchant’s online site

An alternate method of payment that utilizes a temporary and usually a one-time use transaction “identifier” or code (transaction ID). This transaction ID does allow a payment to be tied to a customer's (payers) financial information, but does not require that the payer's sensitive financial information be transmitted to a potentially insecure merchant (payee) or other provider of goods and services .The invention is further based, in part, on the idea that this transaction ID should preferably be short enough to be easily communicated by humans (e.g. a 10 character or less code, rather than a large 30+ character code). As previously discussed this transaction ID should often be good for only a single transaction, and/or be valid for only a relatively limited period of time. Such as a week, day, hour, or even minute. Here the shorter the period of time in which the transaction ID is valid, the fewer the number of unique transactions that be supported by this particular transaction ID. This can result in improved convenience for the payer, but of course overly short time periods can also result in inconvenience and an occasional need to repeat valid transactions. This short period can be adjusted to achieve a good trade-off between security and convenience.

Encryption algorithm plays very important role in communication security, On a survey the performance of existing encryption techniques like AES, DES and RSA algorithms is as follows ,Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption and RSA consume longest encryption time . From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm.