DESIGN AND DEVELOPMENT OF E-COMMERCE SECURITY USING RSA CRYPTOSYSTEM FOR ONLINE TRANSACTION

[1]Megha Bane,[2]Sweety Fernandes,[3]Nilam Gavkar ,[4]Amol Khadapkar, [5]Omkar Krishna Karle
[1]Assistant professor,[2]student,[3]student, [4]student,[5]student
[1]Electronics and telecommunication department,
[1]S.S.P.M's college of engineering kankavli ,Kankavli,India

Abstract : E-commerce has given a new way of doing transactions all over the world using internet. Over the years the rate at which e-commerce sensitive information is sent over the internet and network has increased rapidly. There is affluent growth in the areas of credit card fraud and identity theft because the internet is a public network with millions of users. Amongst users are crackers or hackers that carry out the credit card fraud and identity theft in many ways facilitated by poor internet security; a concern regarding the exchange of money securely over the internet increases. E-commerce industry is slowly addressing security issues on their internal networks but security protection for the consumers is still in its early stage, thus causing a barrier to the development of e-commerce. There is an increasing need for technological solutions to globally secure e-commerce transaction information by using appropriate data security technology. The technology solution suggested for solving this security problem is the RSA cryptosystem. So our project focuses on securing e-commerce information sent through the computer network and internet using RSA cryptography. It sort out the implementation of RSA algorithm and shows that e-commerce security powered with RSA cryptography is very important in e-commerce transaction. While many attacks exist, the system has proven to be very secure and reliable.

IndexTerms **- E-commerce security, Cryptography, RSA algorithm.**

I. INTRODUCTION

E-commerce is trading in product or services conducted via computer networks such as the internet. It is considered to be the sales aspect of e-business consisting of the rollover of data to facilitate the financing, payment and security of business transactions. E-commerce refers to a large range of online business activities for products and services. High degree of assurance needed in authenticity and privacy of such transactions can be difficult to maintain where they are exchanged over an unsecured network such as the Internet. E-commerce also refers to online business transaction in which the parties interact electronically rather than by physical exchanges. A security objective is the contribution to security that a system is well- intentioned to achieve. Security has merged as an increasingly most significant issue in the development and success of a commerce organization. Gaining access to sensitive information and replay are some common threats that attackers impose to e-commerce systems. Trojan horse programs launched against customer systems pose the largest threat because they can bypass authentication and authorization mechanisms. Privacy is most important for users with the rise of identity theft and impersonation. Any concern for users must be treated as a major concern for e-commerce providers. E-commerce security has burden and is one of the highest known security components. E-commerce shares security concerns with different technologies in the field. Security is one of the principal and continuing concerns that restrict users and organizations engaged with e-commerce. The e-commerce industry is very slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks present for the e-commerce systems personnel to read and implement. Educating the consumer on security issues is still in the early stage but will prove to be the most critical element of the e-commerce security architecture.

1.1 Problem definition

E-commerce refers to a large range of online business activities for products and services. High degree of assurance needed in authenticity and privacy of such transactions can be difficult to maintain where they are exchanged over an unsecured network such as Internet .

1.2 Objective

Designing of secure e-commerce transaction by using RSA cryptosystem to avoid security threats to online transaction and securing e-commerce information sent through the computer network and internet.

II. LITERATURE REVIEW

The review is focused on providing the information associated with technology based services of banks and the security techniques adapted worldwide. Online banking now a days plays a crucial role at each level on day to day transactions. [1]Cryptography is a technique which is developed solely for the purpose of data security and integrity in the process of communication. An important element which determines the type of cryptography is key distribution. Based on the type of key

distribution, cryptography is broadly classified as symmetric and asymmetric. Both Symmetric and Asymmetric Key algorithms are highly competent in securing the transferred data over any communication channel. Symmetric cryptography utilizes a single key to achieve encryption and decryption which could increase security issues. On the other hand, Asymmetric Key Cryptography uses two different keys to prevent any unethical access to the data. One key remains private while the other is available in the public key repository. The latter provides more security than the former. Still symmetric cryptographic techniques are preferred for their simpler description and less requirement of resources. In future, for resourceful and protected data transmission, cryptography is an ultimate solution. Various applications can be built using symmetric and asymmetric algorithms for enhancing the protection.. The higher the security of the system, lesser are the chances of breaking into it. Prasithsangaree and his college Krishnamurthy have analyzed the Energy Consumption of RSA and AES Algorithms in Wireless LANs in the year 2003.They have evaluated the performance of RSA and AES encryption algorithms in [3]. The performance metrics were encryption throughput, CPU work load, energy cost and key size variation. Experiments show that the RSA is fast and energy efficient for encryption of large packets. However, AES was more efficient than RSA for a smaller packet size. The tradeoffs with security are not completely clear In the Comparative Analysis of AES and RSA Algorithms for Better Utilization as in [4], the performance metrics were throughput, CPU process time, memory utilization, encryption and decryption time and key size variation. Experiments show that the RSA is fast and energy efficient for encryption and decryption. Based on the analysis done as part of the research, RSA is better than AES. We compare the encryption time of AES and RSA algorithm over different packet size. RSA takes less time to encrypt files with respect to AES. The large prime number is difficult to factorized. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly represented the algorithm in 1977. RSA is very widely used for secure Internet communication (browsers, S/MIME, SSL, S/WAN, PGP, and Microsoft Outlook), operating systems (Sun, Microsoft, Apple,Novell) and hardware (cell phones, ATM machines, wireless Ethernet cards, Mondex smart cards). It is used in many of software products and can be used for key exchange, digital signatures or encryption of small blocks of data. RSA uses a variable size encryption block and key. The key-pair is derived from a very large number n, that is the product of two large prime numbers chosen according to special rules; these primes must be 300 or more than 300 digits in length each. The public key information consist n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n from this information alone and that is what makes the RSA algorithm so secure. Asymmetric key distribution is an algorithm to ensure that the keys generated for such a scenario will not be symmetric and that authoritative power will remain in the hands of one Special Server. In order to provide such authority to the Special Server, it is to be ensured that even if all the share servers were to cheat and try to sign a request illegitimately; they will not be able to do so by virtue of their shares. Their shares, under no circumstances will be able to reproduce the Special Server's share. In other words, the servers are no longer peers; the share distribution scheme is no longer symmetric. In order to provide such authority to the Special Server, it is to be ensured that even if all the share servers were to cheat and try to sign a request illegitimately; they will not be able to do so by virtue of their shares. Their shares, under no circumstances will be able to reproduce the Special Server's share. In other words, the servers are no longer peers; the share distribution scheme is no longer symmetric.

III. METHODOLOGY

This chapter contains the methodology of design and development of e-commerce security using RSA cryptosystem for online transaction. It is illustrated in the points given below.

3.1 Block diagram of system

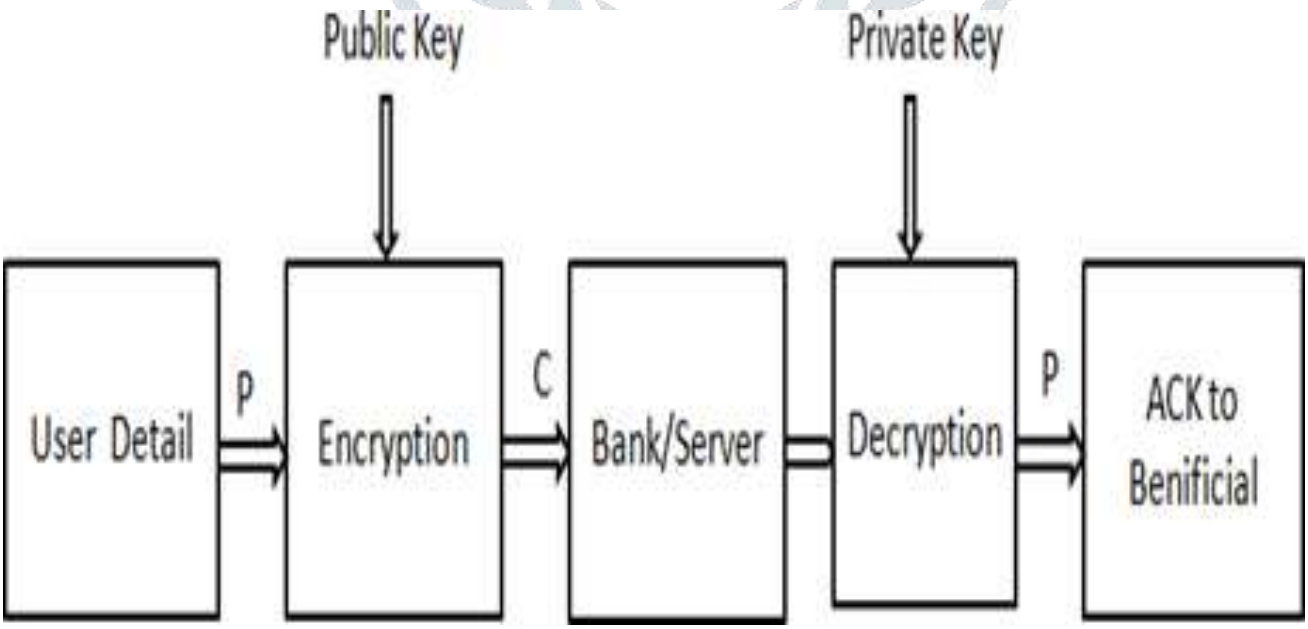

Figure3.1: Block Diagram of System

3.2 Flowchart of system

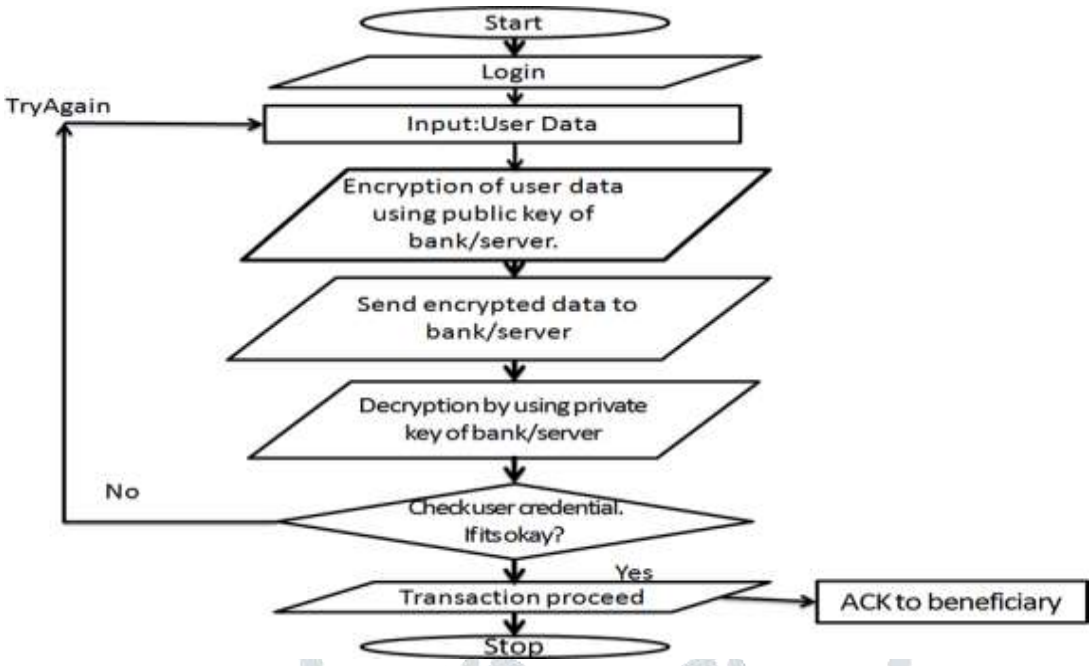

Figure3.1: Flowchart of project

3.3 Project overview

The transmission of the data during e-commerce transactions, we need to keep secret our confidential data from different users. Due to this reason we use encryption algorithms to encrypt our data. Encryption is the process of using algorithm to transform plain text data into a non-readable form called cipher-text. A key is required to decrypt the data and return it to its original plain text format. In this project we are using the Asymmetric key cryptography. In which asymmetric encryption uses two different keys, each has a specific function. A public key encrypts the information, while a private key decrypts the information.

The RSA algorithm is the more secure asymmetric algorithm in asymmetric type cryptography. Two type of keys are used: Public Key and private key. In a payment method, the public key can be distributed to a merchant , and that device can store the key in hardware or software. Even if that key is found by someone who should not have rights to it, all that the person can do is encrypt data with the key; he can't decrypt anything. On the other hand, the private key where the decryption occurs must be controlled very securely. Hence in a public key cryptosystem, the sender encrypts the information using the public key of the receiver and uses an encryption algorithm that is also decided by the receiver and the receiver sends only the encryption algorithm with encryption key. But by using the public key, information can only be encrypted but not decrypted, and the information is only decrypted by the private key that only the receiver have. So no one can hack our text. The RSA cryptosystem is based on the difficult to find a two factor of large prime numbers . The RSA algorithm consist of three steps: key generation, encryption and decryption. The need for the sender and receiver to share secret information is terminated, as all communications involve only public keys. Anyone can send a confidential message using the public key but the information can only be decrypted using the private key, which is in the only one possession of the intended recipient (RSA, 2000). An presentation of a public key system is a safe with a slot at the top, anyone can put items into the safe, but only the person who knows the combination can get the items out.

3.4 RSA Algorithm

The RSA cryptosystem, invented by Ron Rivest, Adi Shamir, and Len Adleman, was first publicized in the August 1977. The cryptosystem is most commonly used for providing privacy and ensuring authenticity of digital data. These days RSA is deployed in many commercial systems. It is used by web servers and browsers to secure web trac, it is used to ensure privacy and authenticity of Email, it is used to secure remote login sessions, and it is at the heart of electronic credit-card payment systems. In short , RSA is frequently used in applications where security of digital data is a concern.

3.4.1 How RSA is used

The RSA is a block cipher whereby the plaintext and cipher text are integers between 0 and n-1, for some n. A typical size for n is 1024 bits. In the RSA algorithm, one party uses a public key and the other party uses a secret key, known as the private key. Each station randomly and independently choose two large primes p and q number, and multiplies the m to produce n=pq. This is the modulus used in the arithmetic calculations of the RSA algorithm.

The RSA algorithm methods are described below:

1. Select two prime numbers, that is, p and q.
2. Calculate n=pq
3. Calculate z=(n)= (p-1)(p-1).
4. Select integer e, gcd((n),e)=1; 1<e<(n).
5. Calculate d, e.d=1 mod(n).
6. For encryption, Ciphertext C=Me mod n.
7. For Decryption, Plaintext M=Cd mod n.

3.4.2 Flowcharts of RSA

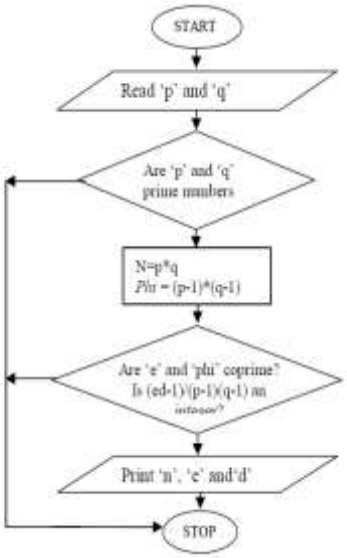

Figure3.4.1: flowchart of key generation

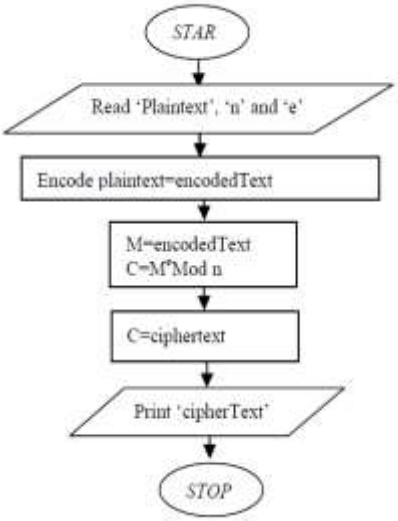

Figure3.4.2: flowchart of encryption

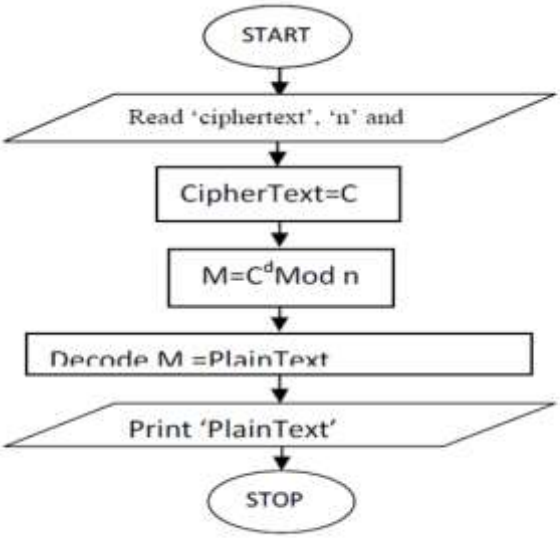

Figure3.4.3: flowchart of decryption

3.4.3 Numerical Study of RSA Algorithm

Example: 1

1. Select two prime numbers, p=17 and q=11
2. Calculate n=pq=17*11=187
3. Calculate phi(n)=(p-1)(q-1)=(17-1)(11-1)=16*10=160

4. Select e such that e is relatively prime to phi(n)-160. So, we select e=7
5. Determine d such that e*d=1 mod phi(n) 7d=1 mod 160 7*23=1 mod 160161=1 mod 160 (d is calculated using extended Euclid's Algorithm) Here, Public key PU(e, n)=7, 187 Private key PR(d, n)=23, 187 Suppose, the Plaintext value (M) is 88 then,
6. For Encryption, Ciphertext C = Me mod n C=(88)7 mod 187 C = 888832 mod 187 C=11
7. For Decryption, Plaintext P = Cd mod n
   P = 1123 mod 187
   P = 79720245 mod 187
   P = 88

IV. RESULTS AND DISCUSSION

In our project that is design and development of e-commerce security using RSA cryptosystem for online transaction , we provide security for bank details in e-business. In this project we have used RSA cryptosystem that is safe and secure for its users through the use of complex mathematics. RSA algorithm is difficult to crack since it involves factorization of large prime numbers which are hard to factorize. A detailed implementation of 1024-bit RSA encryption and decryption algorithm is presented for use in securing e-commerce payment information. The RSA algorithm is a secure scheme for sending encrypted messages for almost 40 years. RSA is asymmetric type of cryptography. Hence no need of sharing keys ,so there is no possibility of losing the keys. The designing of this system is very easy and convenient to use for any transaction . E-commerce is very convenient compared to traditional payment methods such as cash or check. Since you can pay for goods and services online at any time , from any part of the world, so users don't have to spend time in a line and waiting for their turn to transaction. Hence this system makes sure that it provides confidentiality to the users that it is safe.

There is account detail page where user can fill their information like account number, cvv number etc as shown in fig.6.1. Information fill by user is private and therefore it is responsibility of system to maintain privacy.Here RSA work.RSA encryption algorithm used to encrypt the data and this encrypted data is stored at server side database as shown in fig.6.2. This encrypted data is also called as scrambled data. When user wants to make transaction then he/she needs to enter their information in sender detail page like account number, cvv number which is registered already. When user enter the data in sender details and press encrypt and send button then information is matched with the database which is first decrypted by using RSA decryption algorithm. If the information is not matched then transaction is fail as shown in fig 6.3. and if information is perfectly matched then transaction is SUCCESSFUL as shown in fig. 6.4.

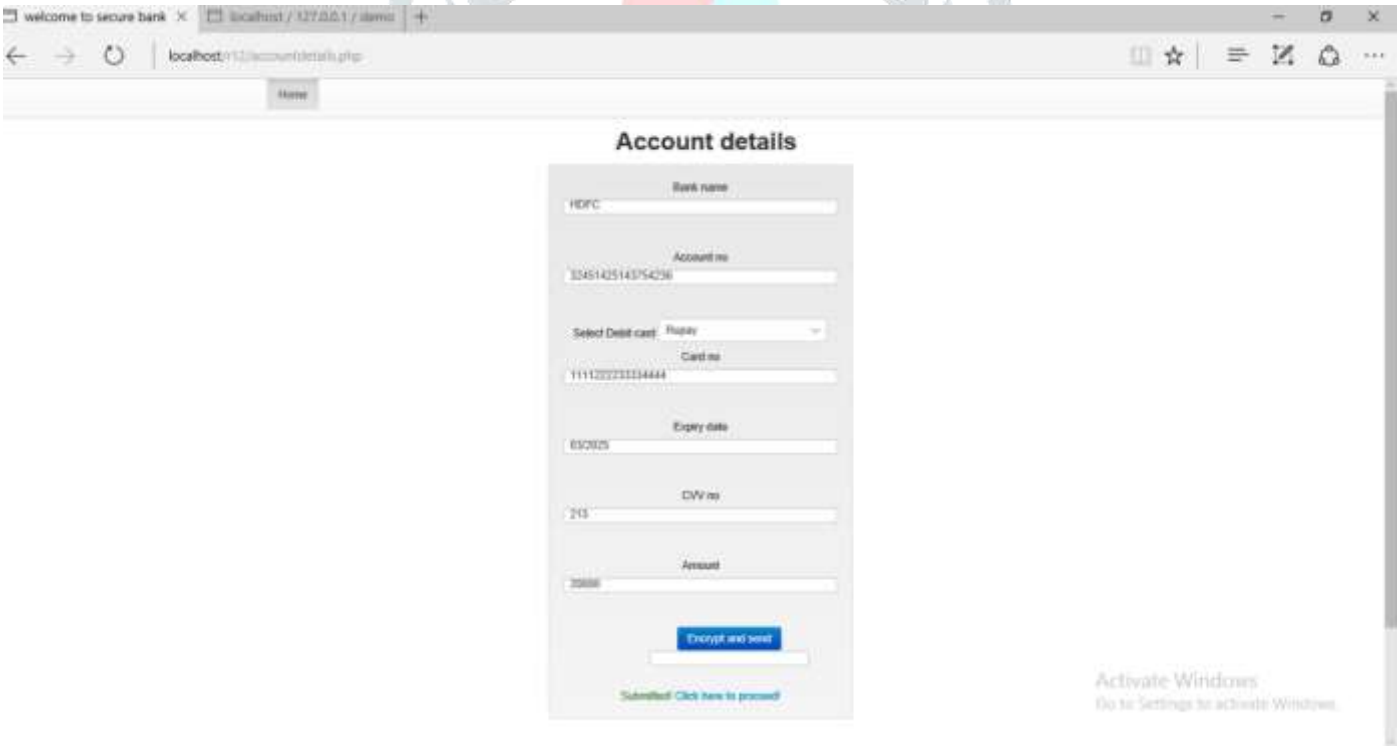

Figure 4.1: Account Details

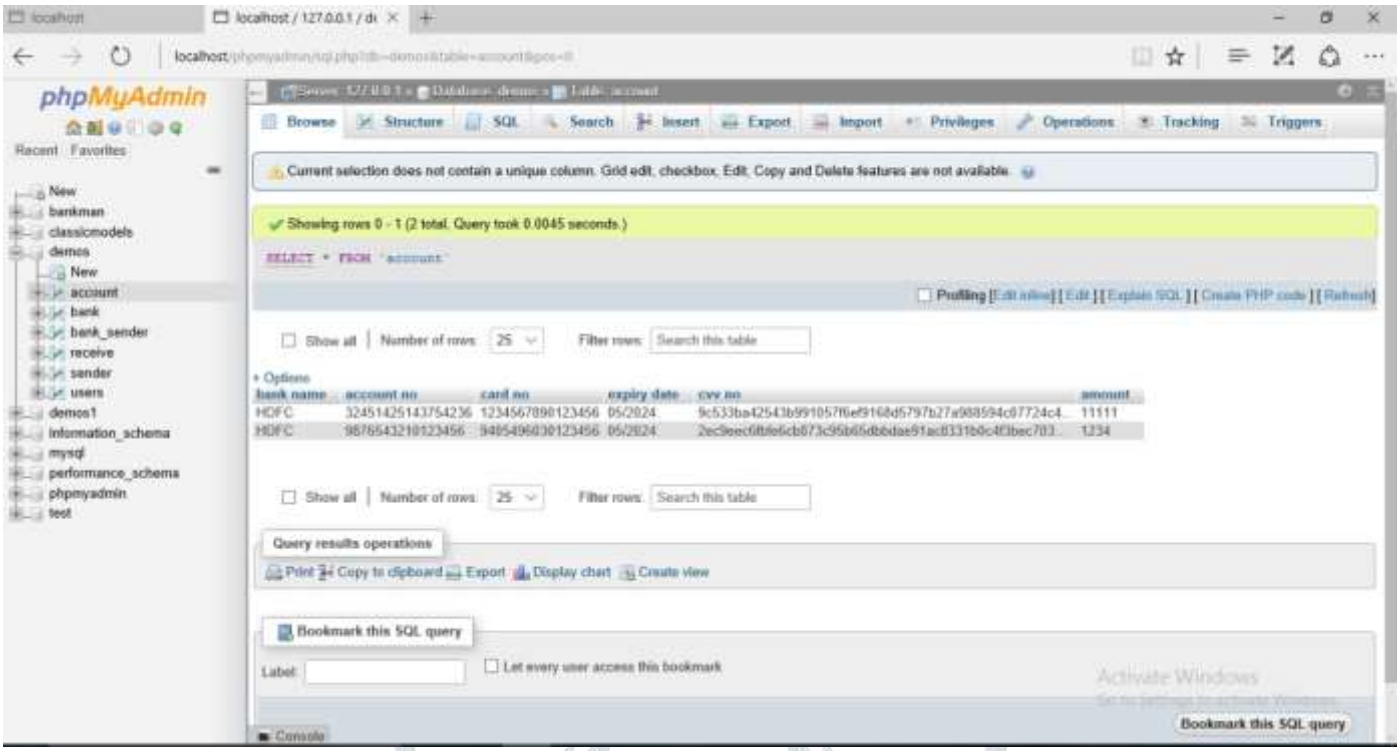

Figure 4.2: Encrypted Database

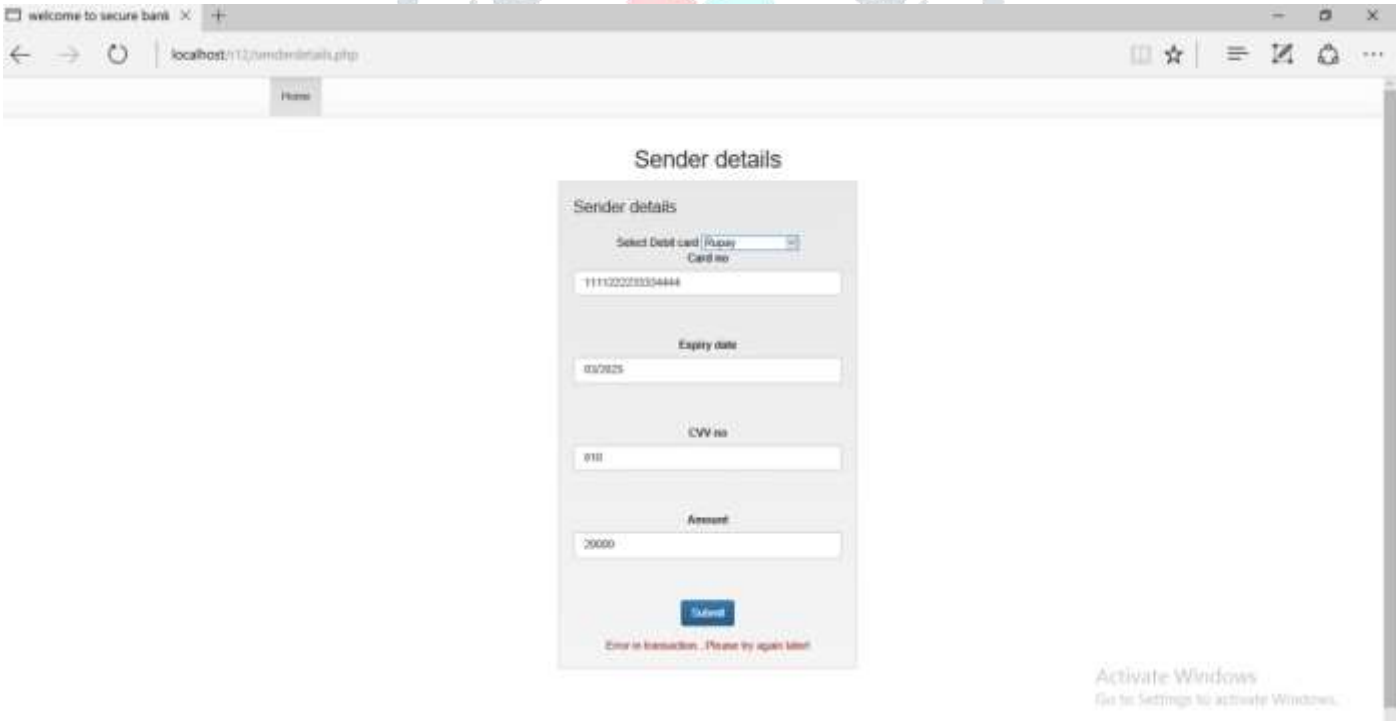

Figure 4.3: error in transaction

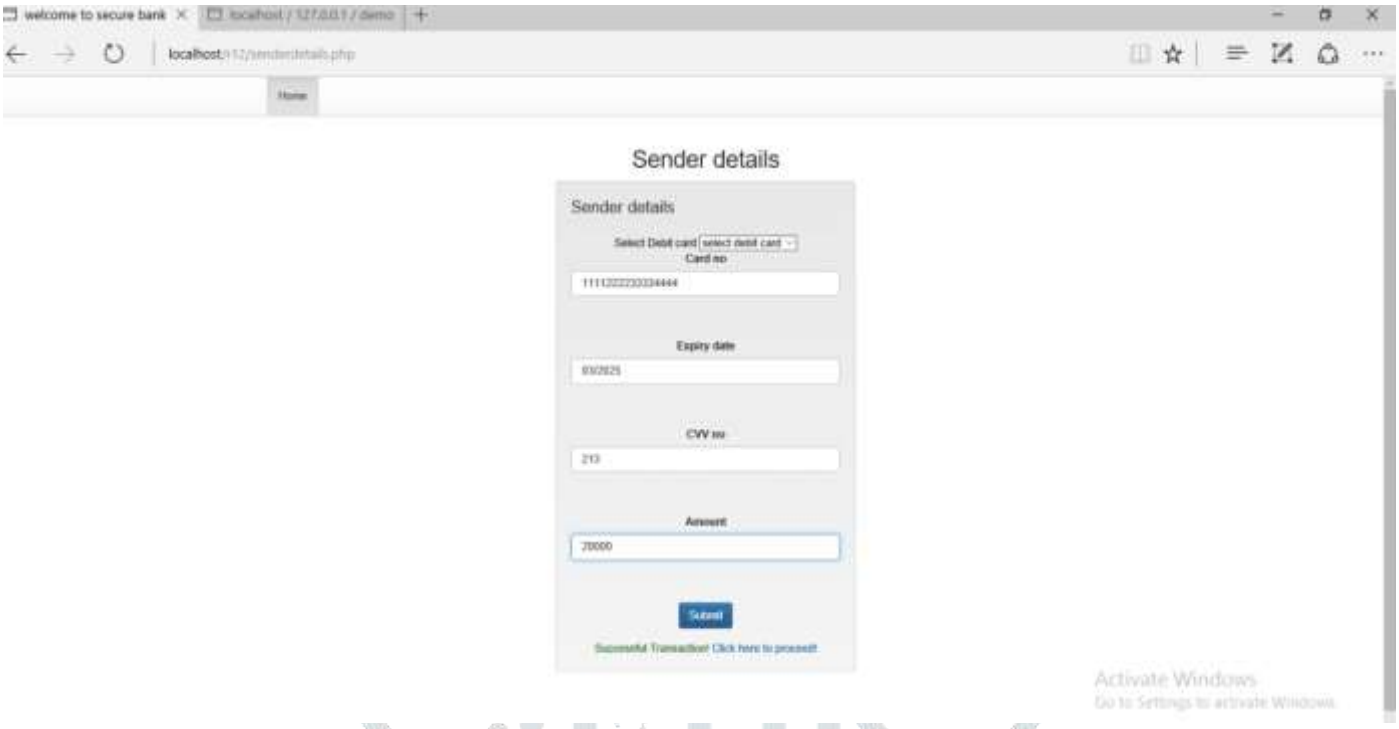

Figure 4.4: successful transaction

V. SCOPE

The future enhancement of the proposed encryption method involves securing online transaction in a cloud environment, wired environment, wireless environment and virtual network environment. The proposed encryption technique is also helpful in Mobile Banking and E- Banking. In virtual environment, data can be shared at two levels, such as Internet and Intranet. The proposed research work is used for sharing the secure data from one to others within the organization of the web server or virtual server at cloud environment. In Local Area Network, the proposed encryption mechanism may be customized for transferring the sensitive data from work station to host based applications. In web based applications, the proposed mechanism enables the transfer of sensitive data from user to user, from user to server and from server to server which are located outside of the organization. In a cloud environment, more number of people are accessing the web server locally or globally to share the sensitive data. The proposed encryption technique is very helpful to enhance the security for web based transactions in future.

VI. CONCLUSION

We have successfully applied the concept of RSA algorithm for providing security to online transaction .In this project we have used RSA algorithm which is asymmetric in nature means it has two keys, public and private which enhances security level. These two different keys are used for encryption and decryption respectively. Hence we avoided need of complex methods of key distribution. Here we have used 1024 bit key length, which is hard to crack so that it can't be broken by brute-force attack. This system is useful for companies to be confident that their electronic transactions can be carried out securely. Also it provides improvements in authentication, integrity, access control and confidentiality for users.

REFERENCES

[1] A. ElShafee and K. A. Hamed, "Design and development of e-commerce security using rsa cryptosystem," IJIRIS Journal division, 2015.
[2] D. M. Ann Murphy, "The role of cryptography in security of electronics comers:," The ITB journal l, vol. 2, 2001.
[3] M. N. . Diffie, W.; Hellman, "A review of some popular encryption techniques," International Journal of Advanced Research in Computer Science and Software Engineering Research, 2014.
[4] E. P. S. U. B. D. Mohammad Nabil Almunawar, Faculty of Business, "Securing electronic transactions to support e-commerce," International Journal of Advanced Research in Computer Science and Software Engineering, 2013.
[5] M. Cozzens and S. J. Miller, "A survey for performance analysis various cryptography techniques digital contents," International Journal of Computer Science and Mobile Computing, 2012.
[6] M. N. M. Preetha, "A study and performance analysis of rsa algorithm," International Journal of Computer Science and Mobile Computing, 2013.