International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Securing Online Transactions with Cryptography and Secured Authentication Methods

A. Aruna, Devansh Sharma, Manikanta Elluru, Subha Sarkar

Abstract: ***Cyber attacks are the common thing which is happening very frequently due to increase in online transactions. Millions of transaction takes place everyday and with increase in the numbers of it ,Stealing user credentials and using it with unauthorized access to do fraud transaction is increasing rapidly. One of the major frauds and stealing of user credential is done during credit card and debit card transactions. We are introducing multi-step authentication and secured algorithm to secure the confidential data. When credit card or debit card is swiped in POS machine or at any counter where the magnetic strip of card is used then automatically machine reads the card details and sends it to the merchant for further completing the transaction. When card details are sent to the are shared between merchant and bank of both the parties then there are several chances of stealing the information of card's confidential details during the process. Further , There is very weak security at the user end as without user consent , transaction can be carried out. Inorder to secure the transaction at initial stage when the card will be swiped in any machine or any cards data will be used ,Card owner have to enter the 4 digit code in bank app to approve the transaction.Then secondly when the card data will be shared between merchant and bank then it will be secured by AES algorithm so that in between process, details can't be misused by any cyber hack. Finally eight digit OTP generated will be the final step to complete the process. These three steps will secure the card transactions which will result in less cyber crimes.***

Index Terms: Cyber Attacks, AES algorithm, Authentication , Cryptography,Online Transactions

I. INTRODUCTION

In present time,credit and debit cards are used at large scale for online payments.Nowadays cashless transaction are highly promoted to make the fianancial system more transparent on mundane level.Credit card and debit card companies and bank offers various schemes and offers to increase the user database.Banks and companies are making huge profits with online payment system.The major concern with increase in card transaction is security of data shared on servers to complete the transaction process.With increase in online transactions ,cyber crime is also increasing at a high rate.Different kind of attacks on companies and banks effects the finance. The security of the confidential data is also compromised. In past records,Banks and finance companies are hugely effected by cyber attacks and in return attackers demands huge compensation money to not disclose confidential data and which result in financial loss for the victim company.Successful cyber attacks on the companies leads to lose of interest and trust of the investors and the customers which again results in financial loss.

Cards payment are the most common method of payment and majority of transactions takes place online.There are different types of threat to card holders.All types of cards have essential information required to make a purchase.Card numbers,Security code ,card expiration date can be easily copied.Misuse and wrong handling of cards during shopping or handling the cards to unknown can leads to various transaction frauds and million of users are effected due to this.Many transaction process and merchant involves only one factor authentication to complete the payment and An expert cyber attacker can break the security which can result in loss of money and bank confidentials.

On server side ,there are many flaws and loopholes while the transactions takes place between merchant and the retailer.During the process when the data of card is send via server then it can be compromised in between if data transfer between the merchant and the retailer is not secured via secured algorithms.There are many algorithms to secure the data and with advancement in algorithm ,It is very necessary to update and replace the security system in active transaction system.Different kind of algorithms include level of steps to secure the encryption and decryption of the data.AES algorithm is most advanced algorithm which can be easily applied and can secure the transmission of data.

AES algorithm is used to secure the transfer of card details and maintain the confidentiality of card during online transaction process.AES algorithm protects the data from unauthorised access and secure it with various encrypted key lengths,AES-128,AES-192,AES-256.These three key lengths provides user an option to choose according to the level of speed and security.

AES algorithm generates 10 128-bit keys from the 128-bit key.These keys are stored in 4 x 4 tables.The plaintext is also divided into 4 x 4 tables in 128 bit .Each of the 128-bit plain text blocks are processed in a 10-round process (10 rounds on 128-bit keys, 11 on 192, 13 on 256).

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Ms. A. Aruna*, CSE (Asst. Prof.), SRM Institute of Science and Technology, Chennai, India.
Devansh Sharma, CSE, SRM Institute of Science and Technology, Chennai, India.
Manikanta Elluru, CSE, SRM Institute of Science and Technology, Chennai, India.
Subha Sarkar, CSE, SRM Institute of Science and Technology, Chennai, India.

It includes various steps like key expansion ,Adding roundkey,Substituting bytes,Shifting rows ,mixing columns and adding round key again.This process is repeated several times.The implementation of the algorithm is very easy and it needs only one key to decrypt and encrypt the data.AES algorithm is the most secured algorithm to ensure the security of the data.AES algorithm is an efficient algorithm which provides speed in both hardware and software.AES algorithm is very difficult to crack and it's the most secured algorithm till now.

Many a times,Card details are stolen by using unethical cyber practices or due to lack of knowledge about the securities,users shares their details with unauthorized bodies which leads to stealing money from the bank accounts via card transactions.In addition to securing the data on the server side , It's a adequate step to secure the whole process on initial level so that from the beginning of the transaction card owner will be aware of the transaction, and without user consent ,transaction can't proceed.

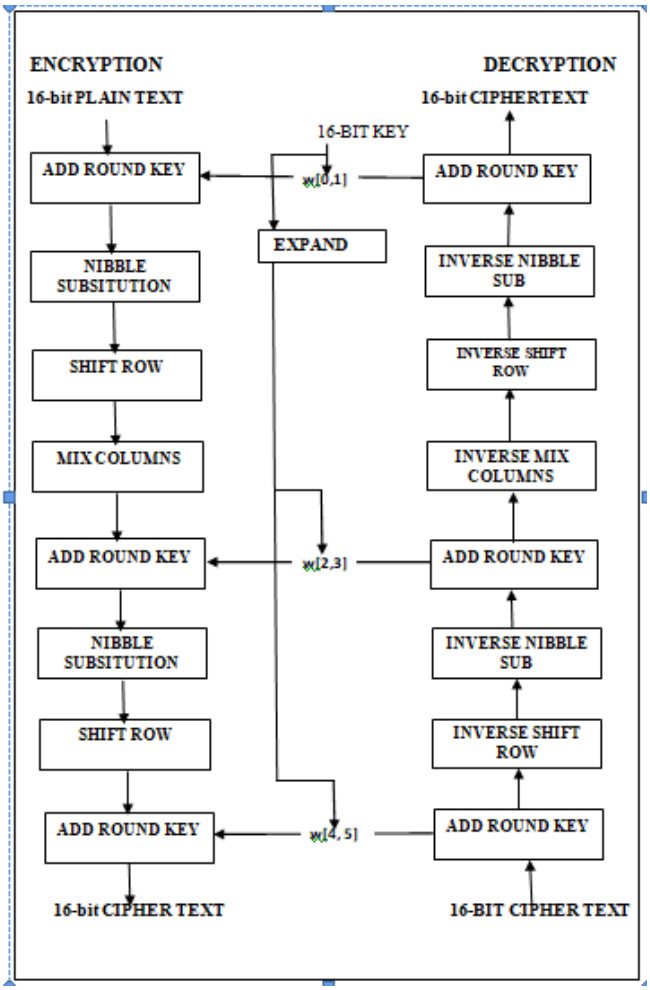

Fig 1:Working of AES algorithm

II. RELATED WORK

Five phase authentication system is proposed in [1].It uses various steps of authentication.First userid and user password is created then user unique id is created.The key step of the paper is to match UID with the QR code of user and finally with one time password the transaction gets completed.This paper includes RSA algorithm and MD5 algorithm to secure the data shared on server and the merchant carrying the transaction.Use of these algorithms ensures features like privacy and secrecy authentication,non-repudation and integrity.

In [2] Visual cryptography is used with QR code to secure the online process of transaction.This system of transaction includes initial steps of generating user Id and password then password is sent to the merchant and its is matched with the database of bank servers. As soon as details match ,Bank generates OTP which is converted into QR code.QR code is converted into two shares. One hare is sent to client via email and other share is sent to the merchant.When share 1 matches with share 2 the transaction gets completed.This method of converting OTP into two shares secures the transaction from user end and merchants end.Without permission and knowledge of client , Transaction can't take place.

In [3],Public key infrastructure is used to secure the data send on server.It proposes three steps process which includes Authentication, Securing connection and then encrypting the message.Firstly in the process of authentication certificate authority is used to authenticate the server.Then password authentication method is followed to identify client to server and finally all the messages and details which are sent over server are encrypted by AES algorithm.

Triple DES algorithm is used in [4] which is more secured than DES algorithm. In this paper , Firstly user credentials are identified and then only valid users are allowed to further proceed. Details are encrypted and then decrypted again at bank end.Data send across the server is secured by TDES which is directly applying DES algorithm three times on same process. But now a days , breaking this algorithm is also possible and data sent on server can be decrypted in between by experts.It is also less efficient as there will be more load on processor and which can decrease the all over speed of the work.

In [5] two layer authentication method is used.When the user proceeds to make payment in the application,the user is asked to enter a sequence number to confirm theauthenticity of the transaction and then transaction process forwards to the next level of security.In next step images are displayed as OTP. The user enters a code which is generated by the algorithm which is then sent to user's mail for verification. If the entered code is verified as true, the user is redirected to the page where an OTP image is displayed which is formed by the stacking. The user has to input the code in the image within the given limited time. If the entered OTP code matches with the original pre-verified value, then the transaction is successful and payment process is completed.

Fraud Resistant technique is used in [6].As normally 16 digit card number is shown on cards which can be used in unethical way but the author has proposed a modal which replaces the last 8 digit numbers of cards with alphanumeric characters. The eight-digit number is used to identify the issuer and the card type while the eight alphanumerical characters are used to verify the cardholder's identity. Generally, Many users save their passwords in browser which can lead to unauthorized access as any other person can log into the computer and easily execute the transaction.In[7],

QR code and watermark method is used to increase the security.Bank will generate a alphanumeric string code will be embedded in the QR code with watermark.User have to verify the code code by scanning which will be sent to the user's email id.After decoding the code string and matching with bank database,Transaction will take place.

III. METHODOLOGY

In proposed system,multiple steps for securing the online systems are introduced as shown in fig[2].There are multiple layers applied to make the transaction more secure from server side and user side.When the user's credit or debit card will be in use,then first step on the initial stage will be to take permission of card holder to validate the transaction via the application.Then the card details will be processed between the merchant bank and retailer bank with the help of trusted card network which will act as bridge between the banksThe whole process of sending card credentials to the banks involved will be secured by AES algorithm and finally card owner will get an eight digit code on the registered mobile number with the bank .As soon as eight digit code will be entered,transaction will complete and database will be updated .

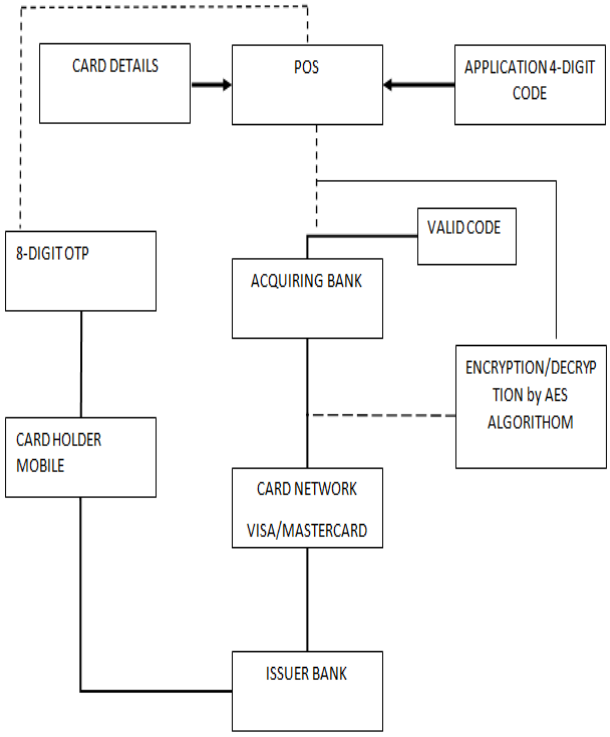

Fig 2: Architecture diagram of proposed modal

A. VALIDATION FROM THE CARD OWNER

A verification system via an application is used is here.The bank who have issued the card will provide an application for verification step.When an transaction process will start,At first,Card will be swiped or details will be entered in POS.As soon as card details are entered in the system, Card owner will get an notification in the application with transaction details.Card owner have to enter the 4 digit common password which will pass the authenticated message to the server and transaction will take over from that step. 4 digit numeric code used in the application will be common and it will be fixed one time in database to authenticate all the transactions which are going to be executed so that card owner knows about the transaction.

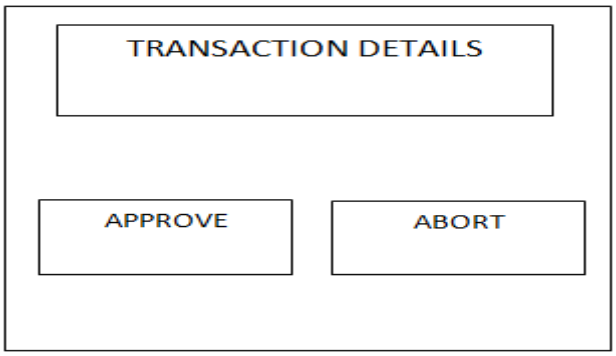

Fig 3:Notification in application interface

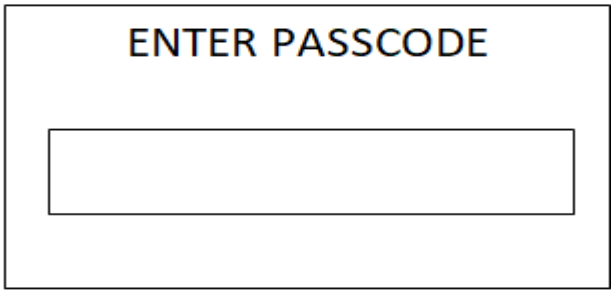

Fig 4:Application screen to enter passcode

B. APPLICATION INTERFACE

Application interface will include user details,Bank details and History of transactions as shown in fig[5].Initially,User will be given an option to set one time 4 digit code to proceed all transactions.

When a transaction will start, application will be notified with complete details of transaction , user have to click on approve transaction or abort transaction option as shown in fig [3].If user accepts the transaction proceeds with approve option then,a interface screen will appear which will prompt the user to enter the 4 digit pass code as shown in fig[4.]If user enter the correct passcode then the transaction will further proceed and approval message will be sent to the server to continue the transaction.The code can be changed anytime by the user at anytime in application interface if in any condition ,code privacy is compromised.

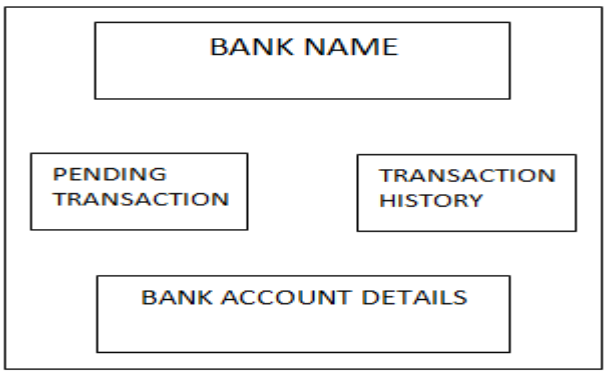

Fig 5: Home screen of application

C. SECURING THE TRANSACTION PROCESS

After getting validation from application interface from the cardholder, Card details will be sent from POS to merchant bank.When card details will be shared with the merchant bank then the inbetween process will be secured by AES algorithm at first stage.Card information will be encrypted and will be converted into cipher text so that attackers can't access the data. At acquiring bank end,Key will be decrypted to ensure the validity of transaction which includes ensuring the availability of transaction amount, authenticity of card.The acquiring bank captures all the information and then it directs the transaction to the appropriate card network. Before routing the transaction to the card network , card Information will be encrypted again to ensure the security.Card network will again decrypt the information and it will send the transaction details to the Issuer's bank for approval.Issuer Bank will send one-time 8 digit password to the registered mobile number with bank to the card holder and as soon as OTP will be entered in the POS interface , Transaction will be completed.Card pin will not be used to authenticate the transaction as card pin is not dynamic and it can be stolen easily. Generated OTP is dynamic and expires in 15 minutes so it provides better security layer as compared to the card pin.

IV. FUTURE WORK

In our system different layers of authentication are used to ensure the secure process and maintain the security of confidential data.In future works, Enhanced application security should be the focus to make it more secure and bugs free.AES algorithm is the most secured algorithm till date but it is possible that ,with new techniques it can be compromised.So making the algorithm more secure or updating the system with latest cryptographic algorithm should is necessary. POS machine technology should be advanced ,so that communication between bank and merchant can be more secure and authenticated. Adding more features to the POS which ensure the security of card details can be added.

V. CONCLUSION

In this study,Multiple security layers are added to maintain the security level in online cards transactions.In initial step itself,Authentication via application is added where card owner will be acknowledged about the complete details of the transaction.Four digit code must be entered to further proceed with transaction.Then whole transaction process is secured by AES algorithm to avoid data stealing .Every information on bank end and merchant end will be encrypted and decrypted simultaneously. Finally, Transaction will be completed by entering eight digit code which will be sent to the card owner registered mobile phone.First step of the modal makes the transaction more secure as card owner will have complete details and information about the transaction and without user's consent transaction will not take place.Also Card pin is not used as card pin can be compromised easily.This whole system makes the transaction more secure and card owner will be fully involved in the transaction process.

REFERENCES

1. Neha Sharma,Brahmdutt Bohra,"Enhancing online banking transaction using hybrid cryptographic method" ,IEEE-CICT 2017
2. Shubhangi Khairnair,Reena Kharat,"Online Fraud transaction prevention system using extended visual cryptography and QR code",Pimpri Chinchwad college of engineering.DOI:10.1109/ICCUBEA.2016.7860061,IEEE-ICCUBEA 2016
3. Isil Karabey,Gamze Akman,"A cryptographic approach for secure client server Chat application using public key infrastructure",ICITST 2016
4. S.Aishwarya,K Devika Rani Dhivya,"Online payment Fraud transaction using cryptographic algorithm TDES",IJCMC,Vol.4,Issue.4,April 2015
5. Kukatlapalli Pradeep Kumar,Dr Ravindranath C Cherukuri"Secured Electronic Transactions using Visual Encryption: An E-Commerce Instance" ICIRCA 2018.
6. Chin-Ming Hsu,Hui-Mei Chao "An Online Fraud-Resistant Technology for Credit Card E-Transactions"Kao Yuan university, DOI: 10.1109/TENCON.2007.4428988, TENCON 2007 - 2007 IEEE Region 10 Conference
7. Aayushi Mishra,Manish Mathuria,"Multilevel Security Feature for Online Transaction using QRCode & Digital Watermarking"ICECA 2017