Debit/ATM card security based on chaos function and QR code

Conference Paper · April 2014

CITATIONS
0

READS
626

1 author:

Gaurav Agrawal
Inderprastha Engineering College, Ghaziabad
4 PUBLICATIONS **10** CITATIONS

SEE PROFILE

Debit /ATM card security based on chaos function and QR code

Gaurav Agrawal, Akash Singh

***Abstract*—Debit card or ATM card frauds had been a major sector of concern due to which Reserve Bank of India (RBI) has set new guidelines since December 1, 2013. Now you will have to enter your personal identification number (PIN) every time you swipe your card at any merchant outlet. Taking the existing state of affairs into consideration, in this paper the conventional security issues of the use of ATM and debit cards are discussed along with the feasibility of other alternatives. Then, the research paper will propose a model for secure use of the debit cards and ATM cards via Chaos function and QR code (DACQ model) that bolsters both speed and security without confounding the process or making it undesirable to users.**

***Index Terms*—ATM card, Chaos function, Debit card, QR Code.**

I. Introduction

During the last three decades, the use of debit cards have rapidly grown into extensively used payment instrument at the point-of–sale (POS) in India. The rolling increase in the use of debit cards has made it more alluring for various frauds. This in turn is going to affect customers' confidence on the use of debit/ATM cards and eventually they will shift away to other means of payment.

Security requirement of such cards include account verification, user identity verification, information access restriction and prevention of card tampering. Card security should be included at all level of card's life cycle which is during its issuance, personalization, distribution and debit and credit transaction [1]. In this paper we propose a DACQ model to completely eradicate such frauds occurring at the POS. Various approaches for debit transaction can be categorized as follows:

A. Conventional approach of debit card usage:

1. *Contemporary approach*: As per Reserve Bank of India (RBI) guidelines from 1st December, 2013 all the debit card transactions at retail outlets will need to be validated using your existing ATM PIN [2]. However, entering your PIN at POS is vulnerable to threats like shoulder snooping, hidden pinhole camera, etc. Now, all that the culprit needs is to get a glimpse or an image of your debit card that contains your card number, expiry date and CCV number which is not a big deal considering the current technical advancements. It should be noted here, now the customer will be exposed to on-line frauds which requires the above mentioned obstacles [3], [4].

2. *Signature debit:* This approach uses signature as a means of user authentication at the POS [2]. Since, the signature can easily be forged. So, such a technique suffers from debit card theft.

3. *Aadhaar-based biometric authentication:* This provides a secure payment infrastructure but incurs with itself cost of maintaining huge amount of database and is also less time efficient as compared to the contemporary approaches [5].

4. *NFC technology for contactless payments:* A NFC-enabled phone is provisioned with a payment application and payment account information issued by customers' financial institution. The phone uses NFC technology to merchants' contactless payments-capable POS system and the transaction occurs [6]. However, the major concerns for this approach is that, in a developing country like India, it is not possible for everyone to get their mobile replaced by NFC embedded one. This is also prone to theft and other frauds.

5. *Based on the short message service (SMS):* As SMS is a universal source of communication and is available in all mobile phones, pagers or other handsets. However, service providers can try to deliver it but cannot ensure its delivery. Moreover, SMS incurs surplus charges. Thus, it is an infeasible approach and is not necessary a low cost solution [7].

Gaurav Agrawal is Asst. Professor in Department of Computer Science and Engineering at Inderprastha Engineering College, Uttar Pradesh Technical University, Sahibabad, Ghaziabad, U.P.-201010. (phone: +919899987137; e-mail: gaurav.agrawal@ipec.org.in).

Akash Singh, student in Computer Science and Engineering, 4th year (B-Tech), Inderprastha Engineering College, Uttar Pradesh Technical University, Sahibabad, Ghaziabad, U.P.-201010 (phone: 9555582581 e-mail: akashsingh.skyhorn@gmail.com).

978-1-4799-3357-0

6. *QR code activated transaction:* In this a QR code is embedded in our mobile devices and all the purchases are made scanning this QR code. If the merchant has a QR code scanner, it can scan the QR code on the mobile device to complete the transaction. If in case the merchant does not have a scanner, a four-digit code pops up on the shopper's phone to be entered on the PIN pad. QR code transactions ensure speedy transactions but it is only applicable to smartphone toting customers [8], [9]. In India where a major section of population don't possess a smartphone, you cannot guarantee such a transaction procedure for common people. This scheme is also liable to theft frauds.

The above mentioned hindrances have evidently restricted the use of debit cards and has ameliorated the fraud cost and trends. Therefore, it is very relevant to devise a solution to the above mentioned problems.

The rest of this paper is organized as fallows. Section II deals with the introduction to DACQ model, section III exemplifies DACQ model using henon map, section IV provides us the speed analysis of this model, section V describes changes required in the conventional approach, section VI describes with its advantages and disadvantages, section VII deals with the possible attacks. Further section VIII takes into consideration its future scope. In section IX we demonstrate our results. Finally, in section X we draw the conclusions.

II. Debit card and ATM card security using Chaos function and QR code (DACQ) Model:

This paper proposes a DACQ model that will address both concerns of security and transaction speed.

This will be another way to eliminate fraud transactions caused by debit card theft or by shoulder snooping others PIN at the POS. The traditional payments via debit card requires at least two tokens which are expected from the customers to prove an authenticated transaction. These two involves the existence of card itself, and the signature or the PIN which is getting more popular at POS than signatures. Both the tokens exist with the customer in different places. The debit card is placed in customers' wallet, while the signature or the ATM PIN usually exist in his brain. Following the same concept, this proposal requires two tokens to verify customers' identity. One is your enhanced debit card which has a QR code on it, while the other is the token supplied to you specifically for any public transaction or to be used at any POS, which is to say that this token will not be same as your ATM PIN.

For the issue of speed of setting a transaction, the transaction initiator must be a merchant [3]. This is because the merchants generally possess a more reliable and continuous connection with the third party involved in the transaction, who could be either a bank or any other service provider. Secondly, since we are using QR code in our debit card, it ensures that we get a large storage capacity, small printout size and a very high speed scan [10], [11]. Also because you are already verifying it via QR code at the merchant store, you can further compensate this time by removing the signature token delivered by the customers at the POS, as signatures can easily be forged and merchants are no experts at judging your identity through a signature and by the time authorities recognizes the criminal's false identity, fraud transactions have already occurred. Further, since there is no handshaking involved between the customer and the third party for transaction confirmation, the processing time is expected to be faster than the traditional approach.

Having discussed both the concerns, we can describe the following scenario. While the customer waits in line for the cashier, on his turn he scans his card to the QR code reader and enters the seed value provided to him by the bank. This step acknowledges the identity of the card holder. On scanning QR code, the card reader takes the stored pattern as input and further asks for a private key. With the help of this private key the card reader machine generates the pattern based on the algorithm provided by different cards. This pattern is further matched with the one scanned by the QR code reader. If they are found to be similar then the user's identity is proved. This will further enable the gateway to the third party or the bank itself for further transaction processing which requires swiping of the card on the card reader. Depending on the card used, customers' bank will transfer the money, or the service provider will carry on the money transfer from the customers' to the merchants' bank [12].

III. Working and Configurations

DACQ model uses a QR code and a chaos function to generate a random pattern which is stored to form a string of characters in QR code. In an attempt to enhance the security of such cards this paper uses a chaotic map to generate cypher based crypto system. Chaotic map possess properties like pseudorandom behavior, topological transitivity and sensitive dependence on initial conditions. Due to such properties they have been used to develop various block and stream cipher based cryptosystem [13]. The proposed cryptosystem involves the use of henon map. It is a 2D map which takes a point (x_n, y_n) and maps it to a new point (x_{n+1}, y_{n+1}) [14]. This is expressed as:

$$x_{n+1} = y_{n+1} - ax_n^2$$
$$y_{n+1} = bx_n$$

The map depends on two parameters 'a' and 'b' and also on the initial values of 'x' and 'y'. At different values of 'a' and 'b' the map may be chaotic, intermittent or converge to a periodic orbit. The randomized pattern generated is stored in a QR code.

QR code is a matrix type two dimensional barcode which indicates information with black and white cross stripes. QR code is used in this scheme due to its following properties [10], [11]:

1. Sufficient data capacity:
   Numeric : 7089
   Alphanumeric: 4296

Binary : 2953
Kanji : 1817

2. High speed scan
3. Small printout size
4. Omni-direction readability
5. Error correction capability
   Level L: about 7% or less error can be corrected.
   Level M: about 15% or less error can be corrected.
   Level Q: about 25% or less error can be corrected.
   Level H: about 30% or less errors can be corrected.

- *Algorithm to generate pattern:*

Step1: Perform several iterations with some initial conditions of x and y. Here we have taken number of iterations as 16.

Step2: Generate a chaos matrix by assembling the x and y as alternate elements of the chaos matrix as shown in fig. 1.

X1	Y1	X2	Y2
0.1000	0	0.9860	0.0300
-0.3311	0.2958	1.1423	-0.0993
-0.9263	0.3427	0.1416	-0.2779
0.6941	0.0425	0.3681	0.2082

Fig. 1. Chaos matrix taking initial values as x=0.1 and y=0. Values of constants a=1.40 and b=0.30

Step3: Generate a pattern by appending the matrix elements after ignoring the initial values of x and y. A positive value is denoted by a '0' whereas a negative value is represented by a '1'. The pattern for the chaos matrix shown in fig. 1 is given below,

00986000030010331100295801142310099310926300342700141610277900694100042500368100208 2

The pattern generated will be very different for different values of 'a' and 'b'. To exemplify this let's take a=1.35 and b=0.30. In this case the value of pattern generated is,

00986500030010283800296001187210085110988000356200038510296400701600011500347000210 5

Step4: This pattern is further appended to the end a numeric code which will be used as a token to distinguish between varieties of cards. This numeric code should be of fixed number of digits. In this research paper we have taken two digits to represent the card type. For example, Master card can have code: 32. This 32 will be appended at the beginning of the generated pattern.

32009860000300103311002958011423100993109263003427001416102779006941000425003681002082

Step5: This pattern is further stored in QR code. The generated QR code of the above pattern is shown in fig. 2

Fig. 2. QR code with embedded chaos pattern when a=1.40 and b=0.30.

Step5: Further, this QR code is embedded on your debit cards.

Step6: Key can be generated by directly appending the decimal part of seed value of the chaos function used. For example, if we are using a=1.30 and b=.40 as seed values then we append the decimal values as 3040. This acts as the key for the customer. This can be further ameliorated by using various encryption algorithms but for the simplicity of our proposal we have used a direct approach in this research paper.

IV. Speed Test for DACQ based verification:

In order to test the efficiency of our model, the simulator analysis is done on the computer of 4.0 Giga byte of memory, 64 bit operating system, Intel® Core™ i7-2670QM CPU of 2.20Ghz (8 CPUs), ~2.2GHz processor. The experiment is implemented using MATLAB R2012a software. The analysis is shown in table1:

S. No.	Pattern generation time(sec)->t1	Pattern matching time(sec)->t2	Total time(sec) t=t1+t2	Cumulative t(sec)
1	0.035896	0.000196	0.036092	0.036092
2	0.036972	0.000165	0.037137	0.073229
3	0.035247	0.000268	0.035515	0.108744
4	0.035393	0.000164	0.035557	0.144301
5	0.037549	0.000166	0.037715	0.182016

Table1: Statistical analysis of time consumption

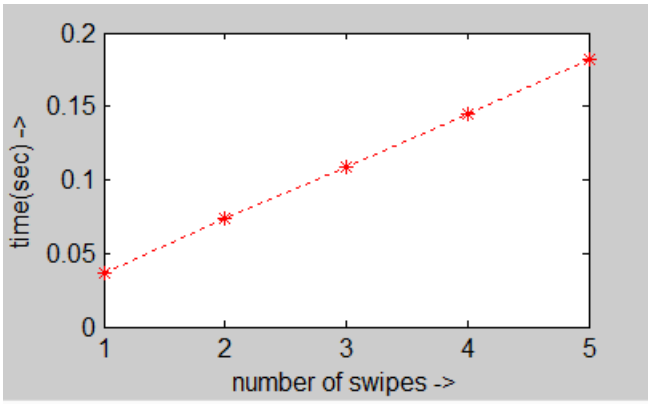

Fig. 3. Total Pattern generation time with increasing card swipes.

QR code takes around 1 sec to get scanned whereas PIN based approach requires a handshaking between bank or any other third party and the merchant and also a signature to verify customers' authenticity. Also, the time spent for processing for five customers is nearly equivalent to 0.2 seconds by which we can infer that for a thousand transactions the net time spent will be 200 seconds, which can be easily neglected for enhancing the security at POS, no matter whether the bank continues its signature policies or not.

V. PRELIMINARIES

A. The Card manufacturers:

The card manufacturers ensure that the following things are present on the debit cards distributed by them to the customers. The following steps are required to make enhance the existing debit cards:

1. Generate a chaos pattern using a suitable chaos function. To exemplify this, Hanon map is used in this research paper.
2. A unique pattern gets generated at different initial values or different constant values. These initial values are converted in the form a private key before distributing it to the customers as a token for their authenticity.
3. The pattern values are stored to form a pattern of characters in QR code.
4. Place this QR code on the conventional Debit cards.

B. At the Point-of –sale (POS):

The following steps have to be followed in the defined order:

1. Card holder hands over his debit card to the merchant.
2. The merchant uses a QR code reader to take the random pattern as input from the customers debit card.
3. Then the customer is asked to enter his private key in the swiping machine. Not to forget that this key is not your ATM PIN.
4. Based on the key a cipher is produced which is converted into the pattern and is further matched with input pattern of customers' debit card.
5. If the pattern matches with the input pattern then normal procedure for the transaction is carried out which involves swapping the magnetic strip on the swapping machine and further making the transaction.
6. If the pattern does not match which implies that the customer is not an authenticated user of the debit card and he is given 2 more attempts before the card gets blocked.

C. The debit card machine manufacturers:

1. Embed the algorithm provided by different card manufacturers on the card reader.
2. Enhance the existing card readers by affixing a QR code reader which acts as a source of input to the above mentioned algorithm.
3. Don't open the gateway to bank's processor until the authenticity of user is verified via above mentioned algorithm.

   Note: Access to card agent should be disabled unless the client's authenticity is verified through QR code

VI. ADVANTAGES AND DISADVANTAGES

Advantages of this method:

1. The actual decryption key is neither stored in the card nor in the card reader. This protects the system from direct key recovery attacks.
2. Each card has its own private key.
3. Authentication procedure requires mutual collaboration of both card and the card reader. So, to compromise with the system, the culprit requires access to not only the card of the victim but also the algorithm stored in the card reader. However this alone will not suffice the culprit's requirements, he will further need the private key which again is only available in victim's brain. Hence the procedure becomes almost impossible to crack.
4. It ensures that the users don't have to use their ATM PIN publically which in turn secures them from fraud internet purchase or any other transactions, as all culprit needs for any e-purchase is the victim's card number, CCV number, his name and his ATM PIN. Card number and CCV number can be easily acquired as it is directly displayed on the victim's card itself and his name is his public identity which makes it easily available. The only thing that avoid fraud e-transactions by the culprit is the victim's ATM PIN. This procedure completely avoids this risk.
5. This approach requires no change in the business logic at the bank's processor and no extra database handling is required.

Disadvantages of this method:

1. The card holder has to get his card enhanced.
2. This approach requires new card readers.

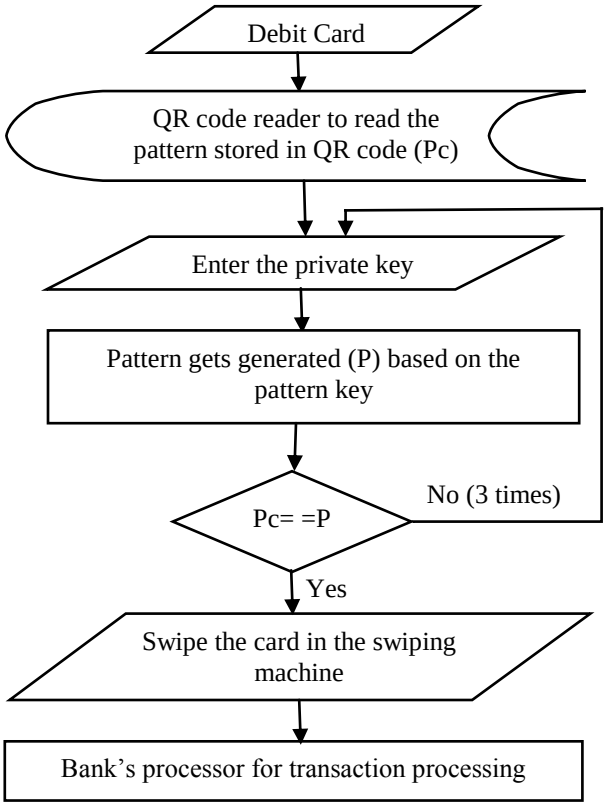

Fig. 3. Flowchart to demonstrate the working of DACQ model

VII. ATTACKS

1. *Card theft:* Debit/ATM card theft is no more a matter of concern as it is not the only token required for transactions at the POS, you will also need the private key of the victim. By the time you plan to get his private key, the user will get sufficient time to report it to authorities and disable his bank account until a new card is issued to him [15].
2. *Card tampering:* Once the QR code is embedded on the card, write access to it gets disabled which further protects it against accidental or intentional accidents.
3. *Card forgery:* Each card is personalized with a specific PIN for ATM machines or for any internet based transactions and a special private key used for QR code based authentication at the POS [16].
4. *Private Key guessing approach:* This technique will not work because the private key used here is quite different from the seed value of the chaos function and also you need other tokens to get yourself authenticated which obviously becomes a impossible combination [16].

VIII. FUTURE SCOPE

You can see QR code everywhere on marketing materials. Newspapers, on receipts, posters, etc. It is an easy way to gain information at a quick snap of your camera phone. Conventionally when we want to know our balance, either we have to visit some ATM machine or we have to make a call to the customer care of our bank and then after taking us to several different options we finally have to enter our 16 digit card number which itself makes it a time consuming process.

This procedure can further be enhanced to resolve the above mentioned issue. The idea is very simple and all you have to do is to scan the QR code and you can easily retrieve the information that you want. To ameliorate it further, it can also be utilized to find the closest ATM.

All that needs to be done is, just make an application freely available to the customers which is capable of scanning QR code and which transfers your scanned data to the respective bank for information regarding your account. The customer on the other side will download the application and can easily use it like any other QR code scanner.

This will not only enhance customers' satisfaction but also reduce the number of phone calls that the bank receives on daily basis [17]. Further, this reduced time spent no receiving calls will payoff for the money spent on implementing this procedure. The bank capable of implementing this much can be an innovator which might fulfill their dream of placing their cards on top of everyone's wallet.

IX. RESULT

The result demonstrates that DACQ approach fulfills both security and speed issues and also makes it more reliable and easy for the customers to get used to it.

X. CONCLUSION

DACQ approach is a very feasible method to fight against Debit/ATM card based frauds. This research paper is the first to propose the chaos base QR code verification at the POS which not only eliminates the usage of the PIN verification table, but also is a very cost effective way to eliminate such frauds.

REFERENCES

[1] Attoh-Okine, N. O. and Shen, L. D., "Security Issues of Emerging Smart Cards Fare Collection Application in Mass Transit," Pacific Rim *TransTech Conference*, pp. 523-526, 1995.

[2] Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card operations of banks, www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=8087 [online], R.B.I., pp. 17-18, 2013.

[3] Martin Emms, Budi Arief, Nicholas Little, and Aad van Moorsel," Risk of Offline Verify PIN on Contactless Cards," Financial Cryptography and Data Security Lecture Notes in Computer Science, vol. 7859, pp. 313-321, 2013

[4] Malcolm Reay, Siemens Insight Consulting," Chip and PIN, a new challenge for data security," Computer Fraud and Security, vol. 2006, pp. 4-5, 2006.

[5] S. Dharanya, and A. Umamakeswari," Embedded Based Conveyance Authentication and Notification System," International Journal of Engineering and Technology(IJET), vol. 5 no. 1, pp. 410, 2013.

[6] Harvey Glickenstein (Senior Editor),"Contactless Payments Debuts on London's Buses New and Improved Railways Around the World," Vehicular Technology Magazine, vol. 8, pp. 19-25, 2013.

[7] Kuan-Chieh Liao, Min-Hsuan Sung, Wei-Hsun Lee, Ting-Ching Lin,"A one-time password scheme with QR code on mobile phone," INC, IMS and IDC.Fifth International Joint Conference, pp. 2069-2071, 2009.

[8] Sana Nseir, Nael Hizrallah and Musbah Aqel, " A Secure Mobile Payment System using QR code," 5th International Conference on Computer Science and Information Technology (CSIT),pp 111-114, 2013.

[9] Young-Gon Kim and Moon-Seog Jun," Design of user authentication System using QR code Identification Method," 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), pp. 31-35, 2011.

[10] Phaisarn Sutheebanjard and Wichian Premchaiswadi,"QR-Code Generator," eighth International conference on ICT and knowledge engineering, pp. 89-92, 2010.

[11] Satrid Vongpradhip," Use Multiplexing to increase information in QR code," The 8th International Conference on Computer Science and Education (ICCSE), pp. 361-364, 2013.

[12] Fumiko Hayashi, Richard Sullivan, and Stuart E. Weiner,"A guide to the ATM and Debit Card Industry", Federal Reserve Bank of Kansas City, pp. 17-68, 2003.

[13] Ljupco Kocarev, "Chaos based Cryptography: a brief overview," Circuits and Systems, IEEE, vol. 1, pp. 6-21, 2001.

[14] Nidhi Taneja, Balasubramanian Raman and Indra Gupta, "Chaos based cryptosystem for still visual data," Multimedia Tools and Applications, vol. 61, no. 2, pp. 281-298, 2012.

[15] Jose M. Pavia, Ernesto J. Veres-Ferrer, Gabriel Foix-Escura, "Credit card incidents and control systems," International Journal of Information Management, vol. 32, pp. 501-503, 2012.

[16] C. Brzuska, N.P. Smart, B. Warinschi, and G.J. Watson,"An analysis of the EMV Channel Establishment Protocol," ACM SIGSAC conference on Computer & communications security, pp. 373-386, 2013.

[17] Reghunathan Sukumara Pillai, and Santhy Sreedhar,"Infosys Finacle-Banking in India: evolution in technology,"2012.