Research Journal of Applied Sciences, Engineering and Technology 4(24): 5406-5409, 2012
ISSN: 2040-7467

Submitted: March 18, 2012 Accepted: April 14, 2012 Published: December 15, 2012

Enhanced ATM Security with PII Using Otpip Algorithm

[1]K. Ram Kumar, [2]B. Santhi and [3]N. Janani
Department of Information and Communication Technology, School of Computing,
SASTRA University, India

Abstract: Biometric verification system is the crux of almost every security mechanism these days and failure of a biometric system can lead to grievous issues. The objective of this study is to identify the consequences when biometric verification fails during ATM transaction and hence suggest a novel enhancement mechanism for it. The security of ATM transactions can be further strengthened using the PII (Personal Identification Image) method. The proposed security algorithm is called OTPIP (One Time Password using Image Processing) and involves two phases. The first one is a verification phase which is done using biometric systems. In case of failure of biometrics, code verification is done. This is followed by the PII phase. These two phases ensure two-tier security of ATM machine and thereby introduce a foolproof safety mechanism.

Keywords: ATM security enhancement, biometric in ATM, fingerprint in ATM security, fingerprint verification, image processing in ATM

INTRODUCTION

With the advent of technology, the need for security especially in machines like ATM is also on the rise. Biometric verification systems such as fingerprint verification, iris scanning, facial recognition and voice recognition have been incorporated in ATM machines which have revolutionized the entire security outlook. Biometrics uses unique physical characteristics of an individual to achieve verification of identity. But there are certain loopholes in embedding biometrics in ATM.

LITERATURE REVIEW

Myo (2009) uses model of multi-layers of convex polygon to implement fingerprint verification. Nain *et al*. (2008) suggest a fingerprint verification using Tracing Ridge flow algorithm. Nathan *et al*. (2011) describes extraction of minutae co-ordinate points from biometric templates and application of elliptic curve algorithm. Saropourian (2009) proposes fingerprint verification based on view patterns and groove pattern. Uma Maheswari *et al*. (2007) use neural network data mining techniques to achieve efficient fingerprint image classification and recognition. In Santhi and Ram (2012), a comparison is drawn between the above papers and detailed discussion of the limitations is done. They find that fingerprint verification is the predominant biometric proposed for ATM, but no alternative is suggested if the biometric system fails. There are two most important scenarios to be considered. One, if the biometric system is subjected to forgery, such as creating forged latent fingerprints, forging iris scan by wearing contact lenses with same iris pattern on them or faking voice by mimicry or using recording, then the whole purpose of introducing this security mechanism fails. Secondly, if the biometric verification fails because of a genuine cause at the user's end such as slight variations in facial expressions, injury in finger leading to disfigured fingerprint or cracked voice due to sore throat, then the user faces the brunt as he is unable to access his account for the required transaction. Hence a contingency plan must be introduced to make the system secure and reliable.

A conclusion is drawn that a single biometric verification does not provide security solution of its own. At the same time, using two or more biometric systems makes it more costly and complicated. Hence an algorithm (OTPIP) is proposed which introduced a hybrid technology for security of ATM. This study depicts the implementation process of the proposed algorithm and uses concrete experimentation results to affirm the same.

Algorithm:

Step 1: User inserts ATM Card and gives his/her fingerprint (as input) on the finger scan pad.
Step 2: Fingerprint verified through pattern matching algorithm
Step 3: If Validated

Initialize Counter = 0.
Goto Step 7

Corresponding Author: K. Ram Kumar., Department of Information and Communication Technology, School of Computing, SASTRA University, India

Customer Database

	A	B	C	D	E	F	G	H
1	ATM card NO	CUSTOMER NAME	PHONE NO	PII value	FINGER PRINT ID	SESSION ID	VERIFICATION CODE	BALANCE
2	12201	Ram kumar,K	9994616592	5445	QW90	060220120706CH	0	77560
3	12202	Siva Guru,J	9597961646	0	ER99		0	98834
4	12203	Anjana,S	9944316936	0	TY98		0	3424
5	12204	Janani,N	9626203748	0	UI97		0	25003
6	12205	Yugaveena	9994255960	0	OP96		0	23565
7	12206	Niranjana,B	7708568609	0	AS95		0	67675
8	12207	Ashwin Kumar,S	9003018344	0	DF94		0	10001
9	12208	Hari Prasad,T	9962037240	0	GH93		0	7456
10	12209	Vignesh,V,R	9944856834	0	JK92		0	30054
11	12210	Vinay,G	9629893088	0	LL91		0	420

Fig. 1: Customer database maintained by bank

Else
Generate verification code
Send SMS verification code
to user's mobile number

Step 4: Enter received verification code
Step 5: Comparison of code with database
Step 6: If Validated
Initialize Counter = 0.
Goto Step 7
Else
Abort transaction
STEP 7: PII interface with multiple images on ATM screen
Step 8: User identifies image
Step 9: Calculation of pin according to location of PII
Step 10: If pin validate
Allow transaction
Else
Increment counter
If counter < 3
Goto Step 7
Else
Block account

We have implemented the following algorithm in a virtual ATM atmosphere.

EXPERIMENTAL SETUP

A customer database was created with columns as shown in Fig. 1. The PII value is set to default value 0. For every session, at the beginning of every transaction this value is updated to the location of the PII of the user, from the images that appear on the ATM interface for that transaction.

A separate database for fingerprints was collected. Every fingerprint is given an ID. The fingerprint ID in customer database corresponds to the ID stored in fingerprint database. Every user must have a unique fingerprint ID. Session ID is updated at the start of every session. Verification code is set to default value 0. This value is updated whenever code is generated and sent via

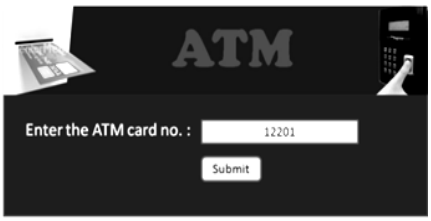

Fig. 2: Virtual ATM interface where user enters ATM card number

Fig. 3: Verification code sent to user's mobile number

SMS gateway through a SMS API, in case fingerprint verification fails.

In an ATM machine, a user inserts his ATM card and the machine reads his card details from the magnetic stripe. For experimental purpose we have made a virtual ATM interface (Fig. 2) where user has to enter his account number manually. User identification is done in this way.

Next step is to authenticate the user. The user puts his fingerprint impression on the scan pad. The system now compares this fingerprint impression with the one stored in customer database. In this case the user with card number 12201 is mapped to fingerprint ID QW90.

If the authentication is done, user enters the PII process and if it fails user has to be verified before he enters PII process.

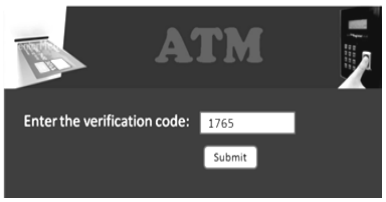

Fig. 4: Received SMS verification code keyed in for authentication

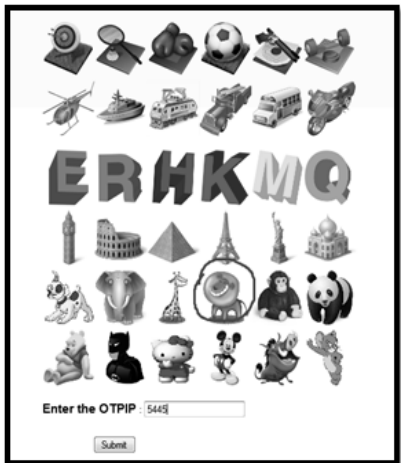

Fig. 5: Interface with multiple images including user's PII. PII location entered in the space provided

Fig. 6: Images reordered for every transaction

A verification code will be generated and it will be messaged to the user via SMS gateway as shown in Fig. 3. The same code will be updated in Database for verification. User has to be verified with this verification code (Fig. 4).

This user is next confronted with the PII interface as shown in Fig. 5 where OTPIP (One Time Password using Image Processing) is used and this creates a new level of security. In our example the user (12201) has LION as his PII and the OTPIP for this transaction will be 5445(5^{th} row 4^{th} column).

The PII process shuffles the row and the column randomly for next transaction as shown in Fig. 6. Now the same user enters another transaction and the PII code for this transaction will be 1221. The PII code will be reset to zero in the customer database when the user quits.

RESULTS AND DISCUSSION

The proposed algorithm works effectively for the two scenarios discussed earlier in the study:

- In the first case, where an intruder or impostor tries doing the transaction, two situations might occur:
  - He fails in the fingerprint verification stage itself. Then he is directed to the code verification stage. But unless he possesses the mobile number or SIM of the person in whose account he is breaking into, he will never have knowledge of the new verification code sent by the system. The probability of him entering the right code by trial and error is very negligible. Under such circumstances where he is able to crack this stage also, he now faces the PII stage. Again the probability of him identifying the right image by trial and error is considerably less. A maximum of three trials are allowed and upon failure, the account gets blocked for 24 h.
  - The intruder is able to forge the fingerprint due to which he gets past the first stage. He next encounters the PII phase. Unless he knows the image and the way to calculate the pin using image location, it is hard for him to break into the account.

This shows that the intruder is bound to fail in one or the other phases. Hence security is immensely strengthened by this two-tier security:

- The user is a genuine one but he fails in the biometric stage due to reasons mentioned earlier in this study. Then he is authenticated through the code verification stage and further by the PII phase. This way the user is able to access his account and do transactions even under conditions of biometric failure. Hence this increases the reliability of the system.

CONCLUSION

The proposed method lays the foundation for a two-tier security mechanism during ATM transaction. It works effectively even when fingerprint verification fails. The concept of PII as a backup methodology enriches the security. Remembering an image (PII) in visual format is

comparatively easier than remembering a number (PIN). In future, the security can still be increased by having first two digits as the position of image followed by PIN. e.g., X-Y-7-1 will be your code where X and Y will be your PII code using OTPIP and 71 will be PIN. So that even if someone tracks your image, he can't proceed further. This PII and PIN combination can enrich the security mechanism. The user has to remember his PII else he will be left in middle of nowhere.

REFERENCES

Myo, N., 2009. Fingerprint identification based on the model of the outer layers of polygon subtraction. International Conference on Education Technology and Computer, pp: 201-204.

Nain, N., B. Bhadviya, B. Gautam, D. Kumar and B.M. Deepak, 2008. A fast fingerprint classification algorithm by tracing ridge-flow patterns. IEEE International Conference on Signal Image Technology and Internet Based Systems, pp: 235-238.

Nathan, B.T., R. Meenakumari and S. Usha, 2011. Formation of elliptic curve using finger print for network security. International Conference on Process Automation, Control and Computing, pp: 1-5.

Santhi, B. and K.K. Ram, 2012. Novel hybrid technology in ATM security using biometrics in JATIT. J. Theoretical Appl. Inform. Technol., 37(2).

Saropourian, B., 2009. A new approach of finger-print recognition based on neural network. 2nd IEEE International Conference on Computer Science and Information Technology, pp: 158-161.

Uma Maheswari, K., S. Sumathi, S.N. Sivanandam and K.K.N. Anburajan, 2007. Efficient finger print image classification and recognition using neural network data mining signal processing. International Conference on Communications and Networking, pp: 426-432.