Continuous and Transparent User Identity for Secure ATM Services

D. Dhayalan[1] and S. Namita[2]

[1] Master of computer applications/Vel Tech high tech DR RR DR SR Engineering College/Anna University, Chennai-62
[1]dhayalan@velhightech.com
[2] Master of computer applications/ Vel Tech high tech DR RR DR SR Engineering College/ Anna University, Chennai-62
[2]snamita34@yahoo.in

ABSTRACT

ATM refers as Any Time Money, Which helps us to easy our process of cash withdrawing, balance enquiry, etc., with our ATM Cards. It helps us to tension free and save our valuable time without going to bank to refer our accounts. Though the process is easy, time saving and very helpful in our hard situation to draw our amounts there is also disadvantages are like inserting duplicate card, misuse of pin code and collection of account details etc. To recover all these above said problems, here our paper has brought an advanced technology of biometric user identity image capturing for secure ATM service through session managements. The function of protocol used in given as mat lab for extra activity to processing easy in ATM services. User enter ATM pin number (correct or wrong) at that time the biometric minutiae image is verified, if the matches are similar the next step is executed and if it mismatch the image is send to admin (bank manager) and authorized user(card holder). The bank manager sends the image and message to card holder. Finally the ATM services are made safe and secure using biometric facial reorganization.

Keywords — ATM, Wrong Pin, correct pin, Admin (Bank Manager) and Authorized User (Customer), unauthorised user and helper or family member.

1. INTRODUCTION

Now a day's each and everybody carrying ATM cards instead of money because of make their life style easy and safety of their own money from thefts. At present ATM's are working under surveillance of security cameras, where the all photographs and videos got saved in DVR (Data Video Recording).In this particular system there is no information about ATM misuse's (who use to enter the wrong or write 4 - Digit Pin).

To overtake first problems, here we are using **Continuous and Transparent User Identity for ATM Transactions When User Entered Wrong pin.** This will help us to identify the UN – user who enters the wrong pin while using the ATM card. The biometric image is captured and sent to bank manager and authorised user.

To overtake 2nd problems, here we are using **Continuous and Transparent User Identity for ATM Transactions When User entered correct pin.** There are three activities performed. They are authorised user, unauthorised user and family member.

I. **Authorised user**

The authorised user has three options given. They are: 1. Add, 2. Accept, 3. Reject and 4. Ignore, the person in the list and new person enter is all base on the accepting and rejecting option given by the authorised user to use his account.

II. **Unauthorised user**

When the unauthorised user enters the correct pin biometric scan the image then the user is rejected. The message is displayed on the screen your transaction has been rejected.

III. **Helper or family member**

The family member and helper is accessing the account then bio-scan of image is done then the cash is withdrawn from ATM machine.

2. EXISTING SYSTEM

The ATM service includes the following accessories which is included in the ATM (OS). The biometric function work at the time of user enters the wrong 4-digit pin no and correct pin no. The image is captured and saved in the database of the operating system. Then the image and message is sent as e-mail or message to admin (bank manager) and authorised user (client). The biometric image is scanned with the help of CASHMA scan session management analyse and sent to the authorized user as e-mail, so the user is not regular to his e-mail login in many situations. So the bank manager sends the message to the authorized user. An unauthorised user cannot run the personal account of authorised user. The new user image has been added in the data base and then later checked by authorised user and only the accepting and rejecting option is given to the authorised user, weather he/she can is again allowed to cash withdraw from ATM account and particular card holder's account.

2.1 Disadvantages

I. Everyone may be not receiving the picture message. (Depends on the advancement of the phone they use).
II. It takes little extra time than the before.
III. If there is more facial change scan cannot be clear.
IV. When the face is covered it cannot be scanned.

3. PROPOSED SYSTEM

This system can also be used in laptops, iPod, mobile phones etc. The owner can withdraw the funds from the ATM without entering the pin by scanning their face.

3.1 Advantages

I. Time can be saved when the owner withdraw the money.
II. Owner can be rejecting the person who he doesn't want to use their card.

4. ARCHITECTURE

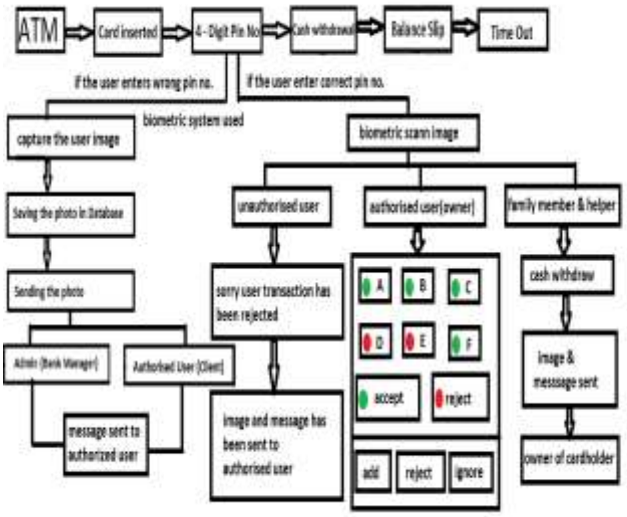

Fig.1 The main function work of the whole ATM service

5. MODULES

5.1 ATM NETWORK FOR EMAIL PROCESS

Networking used in ATM for the purpose of sending messages from Bank Manager to the Authorized user. (Cash Holder). Local area network and broad bands, wireless system are used in ATM for the purpose of sending message.

User network interface makes easy access of data to appropriate service node. This site of networking system is used to connect Satellite with ATM which creates MAC layers. The wireless ATM work and mobile protocol on the following way as shown in the figure below.

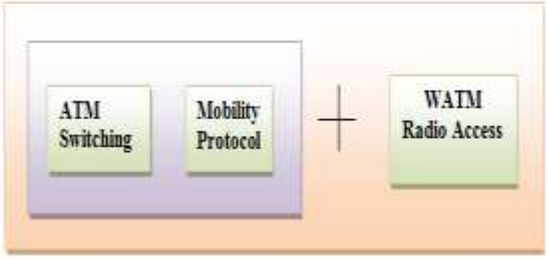

Fig 2. Modular Protocol Architecture of WATM System.

First it its handle by MAC layers Faming Structure then further this handled by adaptive error connections schema. This error correction used to analyze Biometric image frame set. This frames or then checked by authorized user whether to accept the image of the new user currently accessing the account. This is how the networking function works in our secure ATM Service.

The work of wireless ATM service is based on the activity performance done by the protocol function and the stack up-link and low-link. The lower and upper link is otherwise known as up-link and low-link.

Up-link: the up-link is connected with the satellite. This is assigns fixed resource with that of the roaming of mobile MCR connectivity.

Low-link: Base station connectivity link between the bank managers to the authorised user account mobile device. The email image is transferred with that of the message as text to the client.

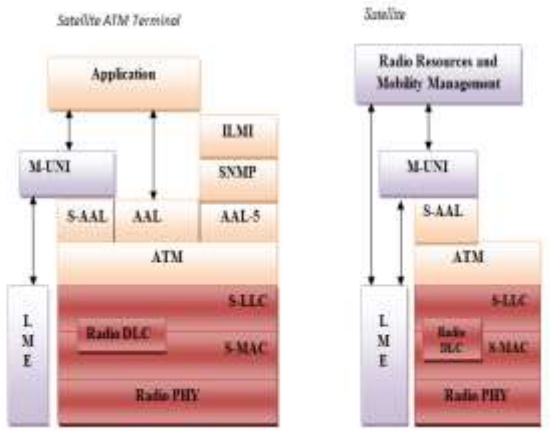

Fig 3. ATM- Sat Protocol Stack

The ATM stack protocol is used for the control of free space in the particular system session management. Also store the data required for the authorised user and the bank manager. To reduce the free space and the extra unwanted images the given sat protocol stack manages. Over load and unwanted data can also cause system problem. So to overcome the protocol system is used in the particular ATM service. It also help system not to get hanged often and make better use of ATM machine.

5.2 MAC FRAMING STRUCTURE

The MAC frame work is used for upper and lower link to access which is used for addition and rejection of the particular image or to ignore the new user or unauthorized user. The MAC frame work is used to clear the traffic problem accrued in the ATM service.

Accepting, rejecting and ignoring function is done by the authorised user with the help of MAC layer. MAC scheme of help the authorized user and ATM Checker to access transaction easily. MAC package includes large number of coding the sending image messages is easy to Bank Manager and Authorized user.

Additional frames work or extra space in the ATM device can be detected or deleted by MAC schema from the storage device automatically. The MAC protocol is also used from scanning the minute change in the face of user and that particular detect image is saved in data storage of the device.

5.3 FACE RECOGNITION

The Bio-Metric face is recognized then the authorized user access is account. The authorized user has given options to accept when the new user or helper or family member uses is account. The new user face is recognize and saved in the device.

Unauthorized user face is also deducted but he cannot accept by the system, because he/she is not included in the list by the authorized user.

The helper and the family members message is send to authorized user but they can access the account transaction is possible, as they are accepted by the authorized user.

The user face recognized is automatically uploaded to the current image by the MAC scheme, for this reason there may be a chance of false in deducting image.

To overcome this problem we are using the following:

I. **Physical changes**

Facial expression change, Aging, Personal appearance Make-up, Glasses, Facial hair, Hairstyle, Disguise.

II. **Acquisition geometry changes**

Change in scale, location and in-plane rotation of the face (facing the camera) as well as rotation in depth (facing the camera obliquely, or presentation of a profile, not full-frontal face).

III. **Image changes:**

Lighting variation, Camera variations, Channel Characteristic, Especially in broadcast and compressed images.

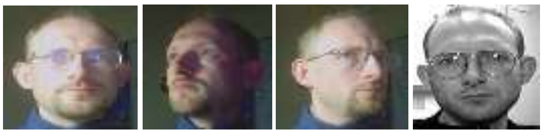

Fig 4. Sample scan image of a single face in different actions performed by user.

5.4. CASHMA TECHNOLOGY INLUDED IN BIOMETRIC

Cashma authentication service used for accessing the biometric image recognition with the identification and use of Cashma formula and it also used in Bio-metric for the session time management. The timely deduction misused of ATM service and Malicious replaced authorized one is continuously done by the system. The analyses and the image identity framing serial wise arrangement are done, in given formula is used for framing the Biometric face.

$$m(Sk, t0) = 1 - FMR(Sk) \ldots\ldots\ldots.(1)$$

The captured biometric CASHMA image is formatted as trusted text message sent to the bank manager and the authorized user. Then the given image is analyzed, biometric face recognition is taken, stored in the data storage device and also send to the user and Bank Manager simultaneously for further verification requirement. The connectivity of system to mobile is done easily with the help of the required formula given below:

$$m(Sk, ti) = m(Sk, ti\text{-}1) \cdot e\text{-}x\cdot h \ldots\ldots\ldots.(2)$$

The working activity performed in the CASHMA is shown in the given CASHMA architecture. The work done by each communication channel is clearly identical in structure. The web service are made multi linked service and the authorized user included his/her processing work on the bases of the given option selected in the system. An overall view made is shown in the figure below.

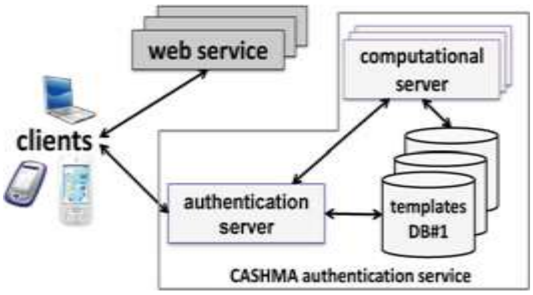

Fig 5. Overall view of the CASHMA architecture.

In the step the face is compared with the main image and fuse image with the help of cashma face reorganization. In this step the time out of sessions is also included in the trusted threshold gmin the time out session is calculated by the given formula Ti = Δ ti = ti +1 – ti. The cashma service is dynamically done by session time out based on the present globe trusted level.

$$Ti = \begin{cases} \tan\left(\frac{gmin\ (\arctan(-s.k) - \frac{\pi}{2}}{trust\ (t_i)} + \frac{\pi}{2}\right) \cdot \frac{1}{k} + s\ , \\ 0 \qquad\qquad \text{if } Ti > 0 \ldots\ldots\ldots (3) \end{cases}$$

Thee length ti of the time out the value is calculated in the gmin it is shown in the authorized user and the bank checker.

The biometric system contains cashma as a part to identify the particular user image and calculate the image on the bases of authorised user access is account. The CASHMA is connecting with channels and linked with the channel node to node makes the message pass captured image to other device as e-mail.

The Bank Manager checks the detail of the authorized user and sends the message to the cash holder. The attackers cannot process the particular account easily. It is very difficult task of using cashma in biometric system and making work of it in ATM mechanism. But the given has been made work successfully the project proposed.

6. CONCLUSION

Thus the biometric facial recognition cashma system is successfully brought in continuous and transparent user identity for secure ATM Services. The protocol time of section also based on the trusted activity performed by the user. The protocol perform checks in facial recognition is consider for the verification and deduction of the user. When the third party enters pin number the bio metric recognition data code strongly depend on the surroundings. The main objective of the designing a protocol is based on quality of the image recognizes, this processed happen in cashma of recognizing biometric face of the user.

The function proposed for us session time out is base reorganization of the image of authorized user, new user and unauthorized user. The similarities are based on acceptance, addition, ignorance and rejection is based on the authorized user. These analyses done for the purpose of secured the particular user details and money.

Hence the given continuous and transparent user identify for secure ATM Service is made secure with the help of Biometric Facial Recognition is proved in our paper and successfully ATM Services is made Secure.

REFERENCES

[1] D. Raychaudhuri and N. Wilson, "Multimedia Personal Communication Networks- System Design Issues", in Proc.3rd.

[2] R. R. Bhat and K. Rauhala, "Draft Baseline Text for Wireless ATM Capability Set 1 Specification", BTD WATM-01, ATM Forum. Dec. 1998.

[3] Damian Gilmurray, Alan Jones, Oliver Mason, John Naylon and John Porter, "Wireless ATM Radio Access Layer Requirements", ATM Forum/96-1057/WATM., Aug. 1996.

[4] Y. Matsumoto and A. Zelinsky, "An Algorithm for Real-time Stereo Vision Implementation of Head Pose and Gaze Direction Measurement", In IEEE International Conference on Face and Gesture, p. 499.

[5] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biomet rics for User Authent icat ion", Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, p. 2019-2040.

[6] Omaima N. A. AL-Allaf, "Review Of Face Detect ion Systems Based Artificial Neural Networks Algorithms", The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.1, Feb. 2014.

[7] Arwa Alsultan and Kevin Warwick, "Keyst roke Dynamics Authentication: A Survey of Free-text Methods", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, Jul. 2013.

[8] M. Cinque, D. Cotroneo, R. Natella, and A. Pecchia, "Assessing and Improving the Effectiveness of Logs for the Analysis of Software faults," Proc. Int'l Conf. Dependable Systems and Networks (DSN), p. 457-466.