International Journal of Engineering &Technology, 7 (1.7) (2018) 96-99

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

RFID enabled safer cards for new gerneration ATM machines

S. Uma [1]*, R. Bhuvanya [1], K. Vijayalakshmi [1], A. Suresh [2]

[1] Assistant Professor, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India
[2] Professor & Head, Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, T.M.Palayam, Coimbatore-641105, TamilNadu, India
**Corresponding author E-mail: umas@veltechuniv.edu.in*

Abstract

The newer generation of ATM card is introduced for the current ATM machine. Instead of the ATM card, machine can be operated through the RFID tags. These RFID tags put an end to the usage of many number of ATM cards and provides a facility to integrate it into a single card named RFID Safer cards. When the safer card is inserted in the ATM machine the reader unit present in the machine, then the information about the card holder will be sent to the server. Information related to the user such as their account details, photo will be fetched from the server. Meanwhile the camera embedded in the machine will capture the image of the user and it will be compared with the image stored in the server. Hence the enhancement of security will be benefited when compared to the current ATM machine since it offers both the password and biometric capacity. If the particular image matches with the database it requests for the pin number and the transaction processing will be initiated. Otherwise the transaction will be aborted. When the user's image matches with the database the system generated OTP will be sent to the user's mobile. Then the user has to enter the obtained OTP to continue the banking process. Thus by using this system ATM card usage will be completely eliminated and it can be done by the RFID safer card. System malfunction can also be avoided which will make our transaction more secure.

Keywords: *RFID Tags; Newer Generation of ATM; Face Recognition; OTP Generation.*

1. Introduction

In view of getting authentication people will use the traditional password scheme and they can enable One Time Password (OTP) in their mobile. Since the remembering of password is a tedious process people will use the same password for many accounts. And that will lead to a weaker security. As an alternative to the text based password some users are trying with the graphical password that is extremely helpful for easier remembrance. Some password protected sites can present CAPTCHA after some stipulated failed attempts or it may lock out the targeted account temporarily. But the later process will affect the legitimate users if it is done accidentally. Though the CAPTCHA scheme is a reliable process it can be easily attacked by the current artificial intelligence. Also if many valid user ids are known by the attacker then there is a possibility of Bulk Guessing attacks. Now the recent survey reports the security vulnerability is high for the manually generated password by the humans.

1.1. The technology used

RFID standard cover the communication protocols where the data sharing will be done based on the existing Radio Frequency Identification. It allows the two way communication between the peer points. Now the implementation of safer cards can be done in two types. We can implement this Safer Card using two types:

i) Active RFID
ii) Passive RFID

Active RFID size is up to 512Kb and the connectivity range is longer but the Passive RFID size is only 1Kb and the connectivity range is shorter. Since our project needs only a shorter range and size we make use of Passive RFID.

1.2. Possible innovation at a later stage

Using RFID Safer Cards we can not only use this as a replacement for ATM card. But also we can replace this for Identification, Driving License, PAN Card, and Voter ID by implementing these in RFID Safer Cards.

1.3. Scalability

This RFID enabled Safer Cards can be extended for multipurpose. The mode of payment in various places such as shopping malls, restaurants etc. using debit cards and credit cards can be replaced by this Safer Cards.
The market (the size of the market and its growth potential)
As ATM's are widely used, the enhancement using Safer Cards will also have a higher impact in the society.

1.4. Object based password

Still the authentication process is carried out by typing the password manually and by enabling the OTP facility in their mobile. In view of getting better authentication, hints for an image, video or text passage from a web/document can be chosen instead of choosing the text based passwords. Thus the proposal of accessing digital objects came to existence. With that the user will get aware of which standard object to use. Instead of using the standard guidelines and procedures for setting up the password recollecting or searching through the emotionally meaningful content will

become more satisfying. Still to enhance the security the idea can be combined by taking the entropy values of digital objects with the denial of wrong password that is used in traditional schemes, enables ObPwd security. The password obtained can be stored in a secure place and it can be recreated whenever it is needed.
Now a day's ATMs have become very familiar and it reaches the general public for their availability and supports the most powerful user friendly characteristics. And it is available for every few kilometers for the easy usage of public. ATMs are found in various locations such as restaurants, supermarkets, shopping malls, schools, colleges, gas stations, and hotels, work locations, banking centers, airports, entertainment establishments, transportation facilities.

1.5. New generation ATM

ATM machines are available to public for their easy usage and also it provides the capability to do the financial transactions such as withdrawing the amount, transferring the amount from particular account to another, and banking functions such as checking the balance will be done at any time or any day on a week. ATM machine will capture the user's image and compares it with the user image in the server. This paper proposed a system in which users can access the ATM without the usage of ATM cards. Handling this system enables ATM machines to be operated through the safer cards. When the user inserts the RFID card in the reader unit of the machine then the user information will be feed to server from the RFID card. In server we can collect the user information such as their mobile number (i.e.) the users account details, their photo etc. Meanwhile the camera enabled in the ATM machine will capture the image of the user and it will be compared with the one that is present in the database.

1.6. Replacement of ATM card

Only when the user image matches with the database then the transaction will be initiated by asking for the pin number and the transaction will be initiated. Otherwise the process is terminated. Hence the introduction of this system eliminates the usage of ATM cards and it is replaced by the RFID cards. Malfunctions
can be avoided by introducing this system which will make the transaction more secure. To help the visually impaired person voice enunciator can be added to make their financial transaction easy. In all the existing methods the usage of keyboards plays a vital role while the introduction of this voice enunciator will encourage the blind people to carry out their transaction independently.

2. Related work

2.1. User study, analysis, and usable security of passwords based on digital objects

R.Biddle emphasize that the usage of strong password have faced some failure. Here an alternative approach of object based password (ObPwd) is introduced instead of the users creating and maintaining the high quality password. User selected digital objects will be converted to high entropy text passwords in Obpwd. Since the remembrance of password in image will be comparatively good than memorizing the exact passwords. Variants, usability and security analysis of Obpwd is presented for the above mentioned methodology and the report will be generated based on the user study of 32 participants. Finally the proposed work proved that it can provide good usability and promising password selection strategy. [1]

2.2. SSMS - a secure sms messaging protocol for the m-payment systems

S. Chiasson enhanced the Short Message Service (SMS) by integrating GSM network's global availability. Here the secure application protocol is embedded and it becomes SSMS which embed the desired security attributes that will act as a security check. This method will be extremely useful when it comes for m-payment systems. Through the proposed work confidentiality, authentication, integrity and non repudiation can be achieved. Elliptic curve based methodology is adopted here for sharing the secret keys among large number of participants. It makes use of the SMS applications efficiently and well suited for the e-payment applications where the security lies as a top preference. [2]

2.3. Multiple password interference in text passwords and click-based graphical passwords

D.Davis proposed the method of remembering graphical based password instead of text based passwords. If the password is enabled as a text then there is a probability that the people may choose the same text for different circumstance. Hence the author claims the graphical password can be retrieved by multiple clicks. When it comes for the analysis part the graphical password significantly works better than the text based password. Even if the user tries to login after the stipulated period of time he/she can easily remember the graphical password which in turn reduces the error by increasing the success rates from the existing methods. Since the user may face some recall error while dealing with text passwords. [3]

3. Implementation

3.1. Existing system

Now the people are working with the Existing ATMs which typically provide instructions on an ATM display screen that are read by andto do the financial/banking transactions. Having read the display screen instructions, the user is able to use and operate the ATM via data and information entered on a keypad. However the drawback in the existing system is that the user should carry their ATM card without fail. But in many cases we forget it. So this system helps us to use the ATM machine without the ATM card.

3.1.1. Disadvantages of existing system

- Multiple ATM Cards are needed To transfer the amount
- Not Easy to remember All Passwords
- Less Security only for Four Digit Password

3.2. Proposed system

Here the new generation ATM card is designed in such a way that it can be operated in an ATM machine without the existing ATM card. RFID card is introduced here that can be operated through the RFID reader. When the user inserts the RFID card in the reader unit of the machine then the user information will be feed to server via the RFID card. User account details such as mobile number and Account details can be collected from the server. The camera enabled in the ATM machine will capture the image of the user and it will be compared against the database.
If the presented image is matched with the database then the user will be prompted for the pin no which initiates the further processing. Hence the usage of this method will completely eliminates the need of carrying all the ATM cards. Thus the machine can be operated by using a single card itself which in turn secure our transaction. In order to encourage the visually impaired person to carry out their transaction independently, voice enunciator can be supported which provides convenient method for doing their financial and banking process.

Advantages

- No Need To Maintain ATM Card
- Very Easy to Transferring Amount
- Cost Efficiency
- High Security

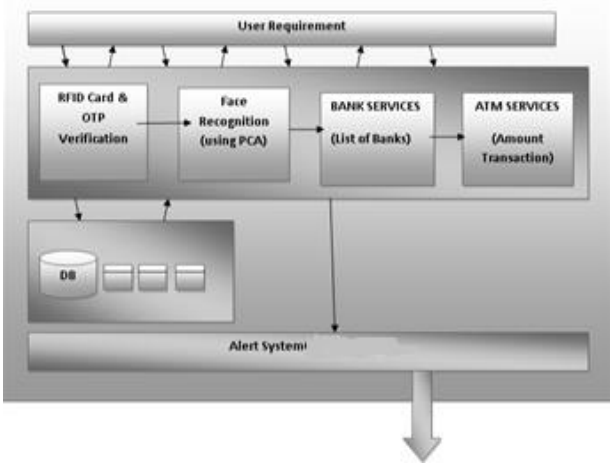

Fig. 1: System Structure Diagram.

4. Modules

- Face Detection
- Face recognition
- Account Management
- Customer FundTransfer

Face detection

The proposed method follows the strategy of image recognition when the user appears in front of that ATM camera. For the image recognition, Principal Component Analysis (PCA) can be chosen which falls under the cover of factor analysis. The main goal of PCA is to reduce the huge dimensionality of the data space to the little dimensionality of feature space which in turn helps to describe the data more economically.

Through the proper utilization of PCA, image prediction, extracting feature from the image, compression of image can be done easily. Since it is a classical technique under the category of linear domain it is well suited for signal processing and image processing. Face recognition is further sub grouped into face identification followed by the face classification and gender prediction.

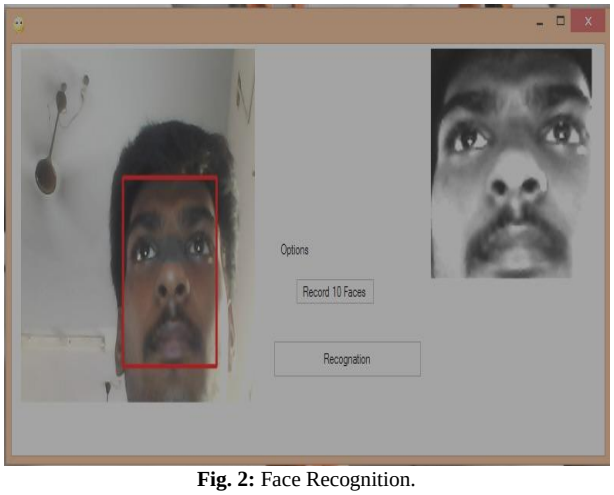

Fig. 2: Face Recognition.

Face recognition

Face recognition system is done using the Principal Component Analysis (PCA). Since the automatic face recognition system is used it helps to check the identity of a given face image. Training set will be assigned to simulate the memory of face recognizer. Training set stores the extracted features from the well known face images of various persons. Thus the goal of the face recognizer is to identify the most familiar feature from the sample test image among the trained set data. Here it is easy to recognize a particular person when an image is presented to the system. And the Principal Component Analysis is applied here for extracting the feature.

Account management

A customer can hold more than one account. But a single account in a bank is chosen here to apply several transactions. ATM allows customers to perform their own transactions using cash cards as identification. The ATM machine will interact with the user to gather information about transaction and validates the information from the central server. After the validation the cash will be dispensed to the particular user. From this we can conclude that an ATM will not operate independently of the network. Usually a bank may have its own internal network of computers to process accounts but here we are dealing with the one that interacts with the Network.

Fig. 3: Adding New Customer Information.

Customer fundtransfer

Customers can select a bank according to their fund availability. As the card contains banking details of the entire bank, it is easy to complete their banking in a single ATM Center. Cash Withdrawal, Fund Transfer etc are possible.

Fig. 4: Generate OTP.

Fig. 5: Bank Selection.

Fig. 6: Transaction.

5. Conclusion

Introducing the new generation ATM cards helps the users to defend against unauthorized access and replay attacks in an ATM machine. Since all the account details of a customer is incorporated in a single card this will facilitates the users to perform the transaction with the destined bank easily. Enabling of face recognition method helps the ATM machine to automatically reject the unidentified face and the OTP generation justifies whether the intended person is working with the ATM or not

Acknowledgement

I would like to thank all my colleagues and students who assisted and helped me to completedmy work.

References

[1] R. Biddle, S. Chiasson, and P. van Oorschot, “Graphical passwords: Learning from the first twelve years,” ACM Computing Surveys, to be published. https://doi.org/10.1145/2333112.2333114.

[2] W. E. Burr, D. F. Dodson, and W. T. Polk, Electronic authentication guidelines NIST Special Publication 800-63, Apr. 2006 [Online]. Availa-ble:http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

[3] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, “Multiple password interference in text and click-based graphical passwords,” in Proc. ACM Computer and Communications Security (CCS’09), Chicago, IL, Nov. 2009. https://doi.org/10.1145/1653662.1653722.

[4] S. Chiasson, P. van Oorschot, and R. Biddle, “A usability study and critique of two password managers,” in Proc. USENIX Security Symp., Vancouver, Canada, Aug. 2006.

[5] D. Davis, F. Monrose, and M. K. Reiter, “On user choice in graphical password schemes,” in Proc. USENIX Security Symp., SanDiego, CA, Aug. 2004.

[6] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, “A comprehensive study of frequency, interference, and training of multiple graphical passwords,” in Proc. Conf. Human Factors in Computing Syst.(CHI’09), Boston, MA, Apr. 2009. https://doi.org/10.1145/1518701.1518837.