ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

BI WAY SECURE ATM/VIRTUAL CASH WITHDRAWAL

G. Elavarasi*,G. Nivetha*,K. Sivasathya* ,

Student, Department of CSE, Kalasalingam University.

S.kathirvel+, Assistant Professor , Department of CSE, Kalasalingam University.

s.kathirvel@klu.ac.in

Abstract -In this scenario, as the government is ensuring to take actions in banning certain currency notes, the usage of ATM has increased. This will lead to security risk. The existing system does not coordinate to act against such risk. The idea behind our project will ensure the authorisedaccess using the QR code. As this is a two-way authentication, this system will be safe and secure for access. If a user inserts an ATM card, it will send the QR code to user's mobile number which is linked to that ATM card. We should generate the QR code by using that number, and then we need to show that QR code to the machine. Then it will read it and verifythe same. If it matches, it will send OTP (One Time Password) to user. The user should type that password on the machine; so that the transaction proceeds otherwise it will not. Finally user can enter the pin and continue their transactions. The QR code and the OTP will be generated using the Random number generation algorithm. In which it will generate the numbers randomly and send it to the user for theauthentication.

Key Words – ATM Card, QR code, OTP Verification.

I. INTRODUCTION

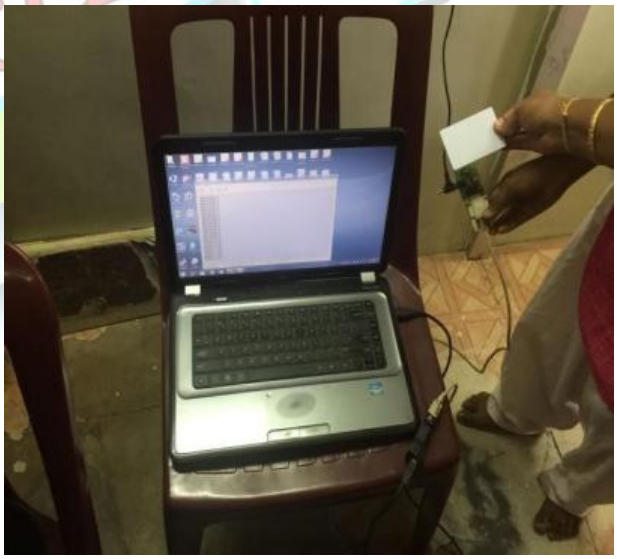
Banking is on eofthe industries most targeted by cyber criminals. Very interesting are the techniques adopted by criminals to steal money with the malicious code or to capture user's PIN directly from the ATMs. There have also been a number of incidents of fraud by Man-in-the-middle attacks, where criminals have attached fake keypads or card readers to existing machines. These have then been used to record customers' PINs and bank card information in order to gain unauthorized access to theiraccounts.

Alternative methods to verify cardholder identities have been tested and deployed in some countries, such as finger and palm vein patterns,[68]iris, and facial recognition technologies. Cheaper mass-produced equipment has been developed and is being installed in machines globally that detect the presence of foreign objects on the front of ATMs, current tests have shown 99% detection success for all types of skimmingdevices.

Carrying 2,000 bytes of data or less. The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card; it provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scannedtoretrievetheidentifyinginformation.

Sample card is the core technology for ubiquitous computing environment implementation, together with USN (Ubiquitous Sensor Network). Currently, there is a new stream, called mobile RFID. It has a small binary coded circuit in it which on energizing either changes from 0 to 1 or vice versa. Depending on application they can manufacture the card with capacity to hold more data. The reader is device which emits EM waves continuously and these waves when touches the card reflects and carries the data back to the reader. This is present in the ATM centre.

2. Read from the card



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

II. CARDAUTHENTICATION

1. *Card*

The acronym refers to small electronic devices that consist ofasmallchipandanantenna.Thechiptypicallyis capableof When an RFID tag passes through the field of the scanning antenna, it detects the activation signal from the antenna. That "wakes up" the RFID chip, and it transmits the information on its microchip to be picked up by the scanning antenna. Like this the card should be shown to the ATM machine, it will read all the details about the card and displays the information .The read time is typically less than 100 milliseconds. Once the card is authenticated it will pass the control to next module or else its terminate the transaction.

III. FIRST AUTHENTICATION (QRCODE)

1. *QRCode*

A machine-readable code consisting of an array of black and white squares, typically used for storing URLs or other information for reading by the camera on a smart phone. Q code is the matrices bar code which was first designed in Japan. QR codes have replaced barcode in many areas because of several advantages like increase in capacity, reduced size, etc. Combined with the diversity and extendibility offered, it makes the use of QR code more appealing than that of the barcodes.

The QR code which was generated using Random number generation Algorithm (AES Algorithm) is sent to the user's mobile phones. Customer will show the received code to the ATM machine, then ATM will verify the code.

IV. SECONDAUTHENTICATION (OTP)

After this verification process is successfully made, we have to verify OTP (One Time Password). The OTP was generated using Random number generation Algorithm. This generated OTP was sent to the user's mobiles. Then user can enter this OTP onto the ATM machine. In ATM machine after the OTP verification was successfully done, then the transaction will be started. When the QR code verification and OTP verification successfully done. Then money transaction can start with an ordinary mode.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

V. ADVANTAGES

1. This system ensures the authorized accessofthe user using the generation of the QR code. Through this wecan avoid the ATM fraud and also to deny the unauthorized access from using ATMaccounts.
2. This can be done using generating the OTP to user. Then only the user can do theirtransaction.
3. This can be done by without using the Internet connection.

VI. CONCLUSION

The idea behind our project will ensure the authorized access using the QR code. Through this project the customer can perform most secure transaction. This project had successfully implemented it will avoid ATM hacks from the malicious criminals.

REFERENCES

1. David PintorMaestreUniversitatOberta de Catalunya08018, "QRP:Animproved secure authenticationmethod using QR codes", Barcelona, June8, 2012.
2. Mrs. S. P. Balwir, Ms. K. Katole, Mr. R. D. Thakare, Mr. N. S.Panchbudhe, Mr. P. K. Balwir, "Secured ATM transaction system using micro-controller", International Journal of Advanced Research in computer science and software engineering, Vol. 4, Issue 4, April 2014.
3. S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy Mag., vol. 1, no.*2, pp. 33–42, 2003.
4. https://www.ieee.org/publications_standards/publications/authors/author_guide_interactive.pdf
5. *B. Batiz-Lazo, T. Karlsson and B. Thodenius.* "The originsofthe cashless society: cash dispensers, direct to accountpayments and the development of on-line real-timenetworks, c. 1965-1985". *Essays in Economic and Business History, 2014 (32). The Economic and Business History Society,2014.*
6. https://www.blackhat.com/docs/us-16-materials/us-16-Hecker-Hacking-Next-Gen-ATMs-From-Capture-To-Cashout.pdf
7. Kravetz, Andy (2009-02-18). *"ATM software aimed atreversing crime - Peoria, IL"*.pjstar.com. *Retrieved 2011- 02-11.*
8. *"ATM Security Issues & ATM Fraud Issues by Geography |ATMSecurity.com ATM Security news ATM Security issuesATM fraud info ATM"*. Atmsecurity.com. 2009-03-04. *Retrieved2011-02-11.*