SNRU Journal of Science and Technology 14(2) May – August (2022) 245396
DOI: https://doi.org/10.55674/snrujst.v14i2.245396

SNRU Journal of Science and Technology

Journal home page: snrujst.snru.ac.th

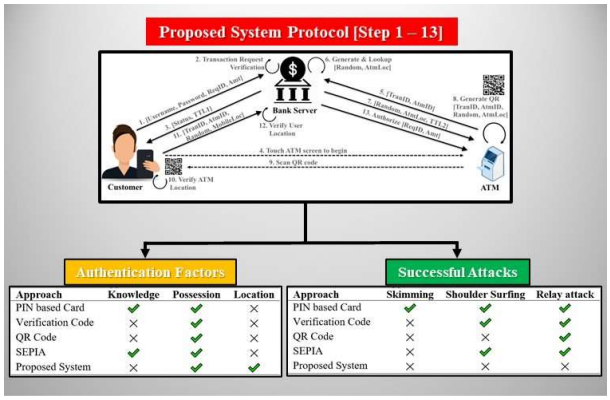
Mutual authentication for cardless ATM withdrawal using location factor

Wilawan Rukpakavong*, Kannikar Subsomboon, Sirikunya Nilpanich
Department of Computer Science, Thammasat University, Pathumthani, 12120 Thailand
*Corresponding Author: wilawan@cs.tu.ac.th

Received: 6 September 2021; **Revised:** 7 February 2022; **Accepted:** 8 February 2022; **Available online:** 1 May 2022

Abstract

Many banks offer cardless ATMs, using a mobile banking application on the smartphone to overcome the high risk of attack with traditional PIN-based cards. Several pieces of research into cardless ATMs have focused on security strengthening, while others have focused on improving usability. Extra hardware devices may be required to increase both security and usability. This paper presents a location-based mutual authentication scheme. This technique combines both security and usability to achieve usable security without requiring additional hardware at the ATM machine. In addition, this paper analyses and discusses the security and usability issues of the proposed scheme, comparing with other systems using a simulation study. The results show that the proposed system has higher security levels with an equivalent standard of usability.



Approach	Knowledge	Possession	Location
PIN based Card	✔	✔	×
Verification Code	×	✔	×
QR Code	×	✔	×
SEPIA	✔	✔	×
Proposed System	×	✔	✔

Approach	Skimming	Shoulder Surfing	Relay attack
PIN based Card	✔	✔	✔
Verification Code	×	✔	✔
QR Code	×	×	✔
SEPIA	×	✔	✔
Proposed System	×	×	×

Keywords: Mutual Authentication; Cardless ATM withdrawal; Location Factor

©2022 Sakon Nakhon Rajabhat University reserved

1. Introduction

Authentication is one of the most important security features, especially for banking transaction systems. Three commonly used factors for authentication are ownership (something you possess), knowledge (something you know), and inherence (something you are). Besides, there are some additional factors for improvements and one of these alternatives is the location. Many systems utilise location information to provide authentication solutions [1]. To increase the security, it is very common to combine multiple authentication factors. For traditional card-based transactions, the Automated Teller Machine (ATM) system uses two-factor authentication, in which each customer must possess an ATM card and must know the PIN number in order to issue an ATM transaction [2].

With the widespread use of ATMs, frauds are also increasing significantly. Card skimming and PIN capturing are the main security problems in using card and PIN-based ATM authentication. Shoulder-surfing, fake machines or fake PIN pads are the most common methods used by adversaries to capture a PIN from victims [3]. Therefore, customers have to be careful whenever they are entering the PIN numbers to save their PIN from being captured. To overcome this problem, cardless access technology is proposed as the solution, with no card and PIN required. During 2012, the NCR Corporation, a leader in banking and commerce solutions, introduced a new technique for withdrawing cash from ATMs using smartphones, and thereafter many banks offered cardless

ATMs to allow customers to get money without inserting their card into a card reader [4].

The works of various researchers focus on the security and enhanced facilities of ATMs in order to improve the system. They can be categorised by technique usage; for example, Near Field Communication (NFC), biometric, one-time verification code and QR code. NFC and biometric implementations seem to be expensive, because ATM machines require large investments in hardware and software. Many Thai banks widely deploy either a verification code or QR code method, due to their inexpensive and easy implementation. The scope of this paper will mainly focus on the existing systems in Thailand, and on research works including security issues and improvement based on these two methods.

Siam Commercial Bank (SCB) [5] has deployed the verification code based cardless withdrawal technology. With this technology, the customer opens up the mobile banking application on the smartphone, indicates the account, and selects the amount of cash to withdraw. The banking server will generate a unique, one-time verification code, called a withdrawal code, and send it to the mobile application. After that, the customer has to go to the nearby ATM machine and enters the registered mobile number linked to the bank account, along with the withdrawal code recently received. The withdrawal code cannot be reused after transaction completion and generally expires within 15 minutes. The process flow of verification code-based on cardless ATM transactions is shown in Fig. 1.

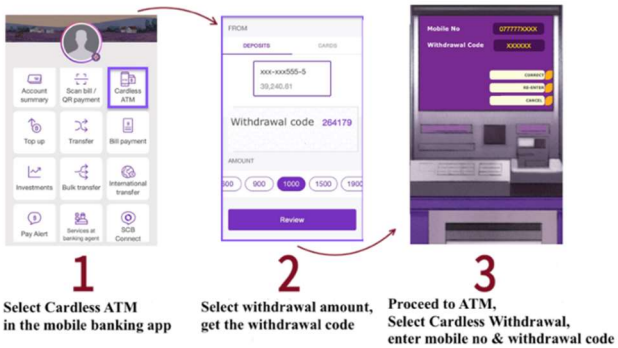


Fig. 1 Verification code-based ATM transaction flow.

The verification code-based technique seems to represent lower authentication security than traditional card and PIN based ATM technology, because only one factor (code via mobile phone) is used for authentication, instead of both card and PIN [6]. It is easy in shoulder surfing on smartphones in the similar way as on ATM keypads. An attacker can obtain the verification code displayed on the victim's mobile by directly looking over the victim's shoulder, which means verifying the ownership factor is eliminated. After gathering knowledge about the verification code (or withdrawal code), an attacker owns all the necessary information to act as the customer and has complete access to the money at the ATM. It is assumed that mobile number is already known by the attacker via open resources, such as contact information on social media. Moreover, a relay attack is possible against this technique in the similar way as the attack on card and PIN-based technology [7].

Kasikorn Bank (KBank) [8] implemented another way, called QR (Quick Response) based technology. The customer starts using the mobile banking application on the smartphone, indicates the account, and selects the amount of cash to withdraw. After the request is created, the customer has to go to the ATM within 24 hours, and the process gets initiated when the customer touches the screen of the ATM machine. This in turn is transmitted to the bank server as a request transaction. Later, the server transmits transaction data to the ATM machine as a response. The ATM generates a QR code and displays it on the screen. After that, the customer uses his/her mobile banking application to scan this QR code for identity verification. Once the identity is verified, the withdrawal transaction is completed, as shown in Fig. 2.

The QR code method provides better ownership factor verification, since a QR code has to be scanned within the mobile banking application. This is to confirm the ownership through a mobile device (or mobile application). However, a relay attack is also possible on the system.

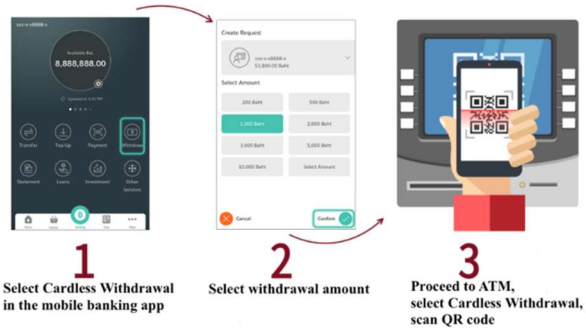


Fig. 2 QR code-based ATM transaction flow.

An attacker may choose a target ATM and capture the displayed QR code on that machine for relaying to the fake ATM machine. If some victims visit the fake one, they are not able to check that the displayed QR code refers to the real ATM, which they are not standing in front of. After they have scanned that QR, cash is dispensed on the real ATM in front of the attacker, as shown in Fig. 3.

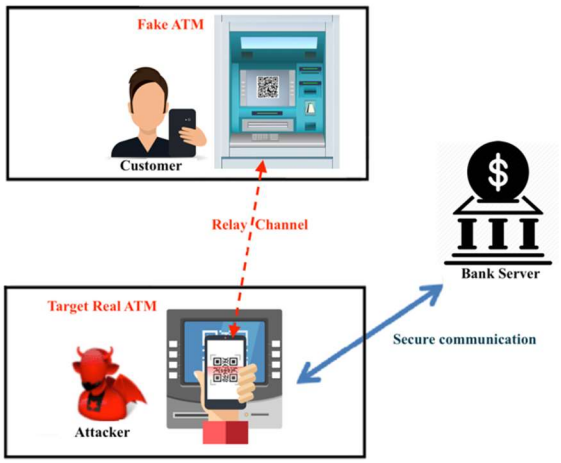


Fig. 3 Relay attack on QR code based ATM.

Rasib Khan *et al.* [9] developed a framework in which secure PIN authentication could be provided, as a service called SEPIA. This system consists of three major entities, namely SEPIA server, ATM and customer of the system. For this system, all customers must have a smartphone for connecting to the SEPIA server. They may use wearable devices, such as Google glass, for protection against shoulder surfing. The protocol involves mutual interaction between all three entities. The withdrawal process is started by the customer touching the ATM screen. Then, the ATM sends a request message to the SEPIA server with request ID and location ID. After the server receives the request from the ATM, it generates an ID and PIN template for the transaction. Next, it sends those generated data to the ATM attached with a short time period of validity. Once an ATM has received the response from the server, it will extract the transaction ID and generate a QR (Quick Response) code combining request ID and location ID. At this step, the customer can see the QR code on the ATM screen and he/she will use the wearable or mobile device to scan the QR code via the SEPIA application. After that, the transaction request message is sent to the SEPIA server from the application. This message contains location ID, request ID and transaction ID, username, and password. When the SEPIA server receives that request message, it will verify and respond to the customer's device. The response message contains a PIN number. To complete the withdrawal transaction, the customer has to enter a PIN number to the ATM for final verification.

SEPIA is more resistant to the shoulder surfing attack. However, customers have to use wearable devices to protect the PIN number from shoulder surfing. These wearable devices are not common tools and cannot be afforded by most people. Moreover, there is the possibility of a relay attack, which is similar to the existing QR code method. In addition, customers have to complete many steps, and go back and forth between the ATM and their mobile devices. This will decrease customer satisfaction, since many customers prefer withdrawal transactions that involve minimal interaction with the system.

The research of Imran *et al.* [4] and Hegde *et al.* [10] focused on ease and convenience of use for customers. They proposed approaches which do not involve too many formalities and restrictions. Every customer will have a mobile phone number registered with the bank account. Cardless cash withdrawal can be accomplished using OTP via SMS. These two approaches are similar to the verification code-based technique. Therefore, it would be possible for a shoulder surfing attack, as well as a relay attack.

To increase the security level for the money withdrawal process, several approaches have been presented. However, a high level of security degrades usability, and leads to inconvenience and frustration for customers, resulting in many operational mistakes. Therefore, the system should be user-friendly and easy to use. Moreover, it should not require any additional devices for reasonable and practical deployment. Hence, it is interesting to integrate security, usability and practical deployment into the requirements and design process. This paper proposes a new scheme of using location as an additional factor to increase the authentication security and provide two-way (or mutual) authentication for cardless ATM transactions. It requires a lower number of interactions compared to SEPIA and provides higher security levels than other systems.

2. Materials and Methods

The proposed system is a modified existing QR code scheme for relay attack resistance. From the customer's point of view, all the steps are the same as the existing QR-based ATM flow. There are three parties: customer (mobile banking application), the ATM terminal, and the bank server. Each party interacts with others over secure communication channels through the protocol shown in Fig. 4.

Step 1 [Mobile Application Usage]: The customer logs on to the mobile banking application and selects "Cardless Withdrawal" to perform a request. Then, the mobile application sends a MOBILE_REQ message to the bank server. The structure of the message is defined as:

$$\text{MOBILE\_REQ} \Rightarrow [\text{Username, Password, ReqID, Amt}]$$

The username and password are in the customer account and have been registered for using a mobile banking application. The ReqID is a request identifier which is generated by the mobile application for this withdrawal request and amount. In practice, there would be more factors for mobile app authentication. This study focuses on the interaction between the ATM and its customers.

Step 2 [Mobile Request Verification]: Upon receiving the MOBILE_REQ message, the bank server verifies this request by checking customer account information, such as username, password, account status, funds, etc.

Step 3 [Customer Request Response]: The bank server then sends the request verification result back to the customer attached to an expiry time, TTL1 (e.g., 30 minutes)

Step 4 [Find Nearby ATM]: If the return result is a failed status, the process is terminated. Otherwise, the customer has to go to the nearby ATM within TTL1 time and select "Cardless Withdrawal" at the ATM machine.

Step 5 [ATM Transaction Request]: At this point, the ATM sends an ATM_TRAN_REQ message to the bank server. The structure of the message is defined as:

$$\text{ATM\_TRAN\_REQ} \Rightarrow [\text{TranID, AtmID}]$$

Here, the TranID is a transaction identifier which is generated by the ATM for this current transaction. The AtmID is the unique and verified identifier for the particular ATM point-of-service assigned by the bank.

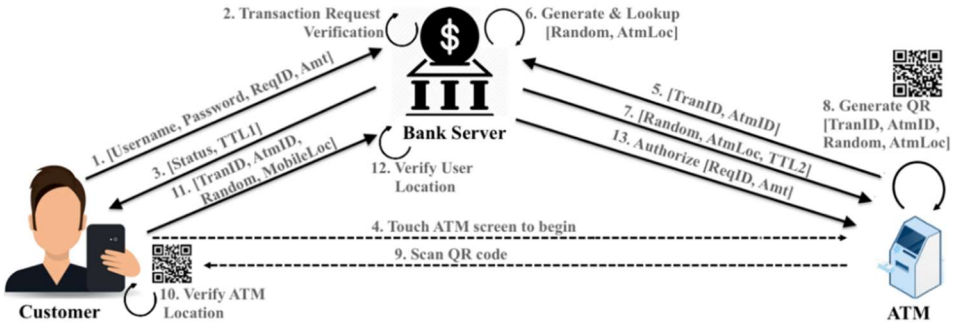


Fig. 4 Proposed System Protocol.

Step 6 [Random Number Generation]: After receiving the ATM_TRAN_REQ message from the ATM, the bank server generates a random number for this particular ATM transaction request. The bank server also finds the ATM location identified by AtmID from the database.

Step 7 [ATM Request Response]: An ATM_REQ_RES message is transmitted from the bank server to the ATM. This message consists of a random number and ATM location, attached to an expiry time, TTL2 (e.g., 30 seconds)

Step 8 [QR Code Generation]: Once the ATM receives the ATM_TRAN_RES message, it extracts all the data and generates a quick response (QR) code. The QR code is generated from the encrypted of following context:

$$\text{QR Code} \Rightarrow [\text{TranID, AtmID, Random, AtmLoc}]$$

Here, the TranID, AtmID, Random and AtmLoc are the transaction identifiers, ATM identification number, random number and ATM location, respectively. The QR code is then displayed on the ATM screen.

Step 9 [QR Code Scan]: At this point, the customer then uses their mobile, running the bank application to scan the QR code. After successfully scanning the QR code, all encrypted data are transferred to the customer's mobile.

Step 10 [ATM Location Verification]: In this step, the mobile application running on the customer's mobile decrypts all the data and then verifies the location. Location verification utilises two location coordinates (Latitudes, Longitudes) of the ATM machine and the current mobile position. These two location coordinates are then compared to see if the ATM standing in front of the customer is the same location as identified in the QR code (ATM location data from the bank server). Therefore, this step is designed to resist relay attack. Normally, smartphones are equipped with Global Positioning System (GPS) chips, which can accurately determine the location of the mobile within a few metres of its actual location [1, 11 – 14]. This accuracy value can be set as the threshold distance.

Step 11 [Customer Transaction Request]: After successfully checking the ATM location, the mobile application sends a CUS_TRAN_REQ message to the bank server. The structure of this message is as follows:

$$\text{CUS\_TRAN\_REQ} \Rightarrow [\text{TranID, AtmID, Random, MobileLoc}]$$

In this message, the TranID, AtmID, and Random have been obtained from the QR scan, and the MobileLoc is the current location of the mobile device. This is to check that the customer with the mobile device is standing in front of the ATM machine.

Step 12 [Customer Location Verification]: After receiving a CUS_TRAN_REQ message from the mobile application, the bank server compares the location of the customer (MobileLoc) with the location of the ATM machine in a similar way to Step 10.

Step 13 [Customer Request Authorisation]: If the location checking is successful, an authorisation message is sent to the ATM for dispensing cash.

ATM Attack Methods and Simulation

The evaluation of the proposed concept is compared with several methods, namely traditional PIN based card, verification code, QR code, and SEPIA. It is assumed that the customer's mobile number has already known. Three factors have been used in ATM authentication described as follows:

Knowledge: This factor includes all things which customers must know for verification, such as personal identification number (PIN).

Possession: This factor includes anything that customers must have in their possession for verification, such as an ATM card or a withdrawal code from the mobile application.

Location: This factor includes anything that can be used to find the location, such as GPS coordinates, MAC address or customer's cell tower location.

This research focuses on the potential attacks on ATM usage involving four parties: the attacker, the customer, the real ATM and the fake ATM. Two persons act as the attacker and

the customer. One desktop computer acts as the fake ATM. The attacker stands in the front of the real ATM machine, while the customer stays at home in front of the fake ATM. There is an IP camera installed behind the customer. The simulation attacks are as follows:

Skimming: The attacker has installed a skimming device on the ATM machine to get hold of the customer information [10]. It is assumed that the attacker has already cloned the customer's ATM card.

Shoulder surfing: This is the criminal practice of spying on someone's personal or private information through direct observation from behind and looking over the victim's shoulder when he/she enters a PIN number at the ATM or receives a PIN/OTP on his/her mobile device [10]. This is simulated by capturing both the customer's mobile screen and a fake machine screen using the IP camera.

Relay attack: An imitation ATM terminal relays information to the attacker. Customers are tricked into thinking that this terminal is a valid one, and then perform ATM activities [10]. This event is simulated by developing simple software for sending and receiving data between the fake machine and the attacker's mobile through the Internet.

In this simulation, an SCB ATM is used as the real ATM for both PIN based card and the verification code techniques, while a KBank ATM is used as the real ATM for both the QR code and the proposed methods. To simulate the SEPIA method, another computer acts as the real ATM running the SEPIA algorithm. To simulate location checking for the proposed technique, the real ATM location has been pre-configured and displayed with QR code on the fake machine. The customer must run a location checking application to verify the distance before starting a transaction. Overall average position accuracy of the GPS-enabled smartphones is 10 metres [11 – 14]. Therefore, this value is used as a threshold for location checking algorithm.

3. Results and Discussion

Table 1 shows factors used in each approach and Table 2 shows successful attacks for each approach.

For withdrawal authentication at the ATM terminal, the verification code and QR code methods use only one factor, while the others use two factors. In general, two-factor authentication (2FA) is more secure than single-factor authentication. However, it is only better if those two factors are independent and each of them is very well protected at all stages. Cloning the

Table 1 Authentication Factors for Each Approach.

Approach	Knowledge	Possession	Location
PIN based Card	✔	✔	×
Verification Code	×	✔	×
QR Code	×	✔	×
SEPIA	✔	✔	×
Proposed System	×	✔	✔

Table 2 Successful Attacks for Each Approach.

Approach	Skimming	Shoulder Surfing	Relay attack
PIN based Card	✔	✔	✔
Verification Code	×	✔	✔
QR Code	×	×	✔
SEPIA	×	✔	✔
Proposed System	×	×	×

ATM card via skimming or capturing the PIN/OTP through shoulder surfing, render the 2FA ineffective. Therefore, the proposed system is better in archiving the objective of 2FA than others. Moreover, the simulation demonstrates successful relay attacks on all approaches except the proposed one. The proposed method provides mutual authentication in which both the ATM machine and the customer authenticate each other. As a result, it is resistant to relay attack.

In terms of usability, scanning QR code is more usable than entering PIN/OTP to the ATM machine [15 – 17]. SEPIA uses both scanning QR and entering PIN number for security improvement. However, this decreases the usability level. Both the QR code technique and the proposed system use only QR scanning, while the other two approaches use entering PIN/Code. Accordingly, both QR code and the proposed methods provide better usability than the other three approaches. From a deployment point of view, none of the approaches require additional hardware or devices for the ATM machine. Therefore, they are applicable, low-cost and easy for large-scale deployments.

4. Conclusion

Many financial institutions offer cardless ATMs to improve customers' experience by eliminating the need to carry and replace cards, which can easily be lost or compromised, as well as to reduce the cost to the institution to replace them. However, the current cardless ATM withdrawal systems are vulnerable to several attacks. This paper describes and simulates the adversarial models for the possible attacks, such as shoulder surfing and relay. Moreover, this paper proposes a mutual authentication scheme by using location factor, which is a modified model to solve those possible problems. For this proposed system, customers still perform the same process and get the same transaction facilities for withdrawal transactions as presently exist. In addition, this paper analyses and discusses the security and usability of the proposed scheme, comparing it with other systems.

5. Suggestions

The accuracy of GPS location is beyond the scope of this paper. Future work involves improving the accuracy of GPS location or distance calculation. Moreover, the proposed idea may be applied to other application fields, such as access point authentication, a door opening system and an employee attendance system.

6. Acknowledgement

The authors gratefully acknowledge the financial support provided by Thammasat University under the TU Research Scholar, Contract No. TUGI 1/2562.

7. References

[1] F. Zhang, A. Kondoro, S. Muftic, Location-based authentication and authorization using smart phones, IEEE International, Conference on Trust Security and Privacy in Computing and Communications 2012, Liverpool UK. 25 – 27 June 2012, 1285 – 1292.

[2] F. Aloul, S. Zahidi, W. El-Hajj, Two factor authentication using mobile phones, IEEE/ACS International Conference on Computer Systems and Applications 2009, Rabat Morocco. 10 – 13 May 2009, 641 – 644.

[3] J. Kim, G. Sharma, I.S. Cardenas, D.Y. Kim, N. Prabakar, S. S. Iyengar, Dynamic PIN: A novel approach towards secure ATM authentication, International Conference on Computational Science and Computational Intelligence 2017, Las Vegas USA. 14 – 16 December 2017, 68 – 73.

[4] M.A. Imran, M.F. Mridha, M.K. Nur, OTP based cardless transaction using ATM, International Conference on Robotics, Electrical and Signal Processing Techniques 2019, Dhaka Bangladesh. 10 – 12 January 2019, 511 – 516.

[5] Cardless Withdrawal, at http://scb.co.th/th/personal-banking/digital-banking/scb-easy/how-to/cardless.html, 18 January 2021.

[6] K. NurL, M. Firoz Mridha, OTP based cardless transction using ATM, International Conference on Robotics,

Electrical and Signal Processing Techniques (ICREST) 2019, Bangladesh. 10 – 12 January 2019, 511 – 516.

[7] L. Sportiello, Internet of smart cards: a pocket attacks scenario, Int. J. Crit. Infrastruct. Prot. 26 (2019) 1 – 15.

[8] Cardless Withdrawal, at http://kasikornbank.com/en/personal/digital-banking/kplus/function/cardless-withdrawal/Pages/index.html, 18 January 2021.

[9] R. Khan, R. Hasan, J. Xu, SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using mobile and wearable devices, IEEE International Conference on Mobile Cloud Computing Services and Engineering 2015, San Francisco USA. 30 March – 3 April 2015, 41 – 50.

[10] N. Hegde, K.R Sharath, Cardless ATM cash withdrawal: a simple and alternate approach, Int. J. Comput. Sci. Inf. Technol. 7(1) (2016) 126 – 128.

[11] S.V. Watzdorf, F. Michahelles, Accuracy of positioning data on smartphones, ACM Press, New York, 2010.

[12] F. Nisar, Location based authentication service using 4G/5G Devices, International Conference on Communication Technologies 2019, Military College of Signals Pakistan. 20 – 21 March 2019, 120 – 126.

[13] A. KwangJong, J. Cho, The simple location-based authentication method using multi-layer display in Korea, J. Bus. Retail. Manag. Res. 13(4) (2019) 256 – 264.

[14] L. Fridman, S. Weber, R. Greenstadt, M. Kam, Active authentication on mobile devices via stylometry application usage web browsing and GPS location, IEEE Syst J. 11(2) (2017) 513 – 521.

[15] T. Maqua, R. Neff, M. Wbbeling, Improve ATM withdrawal security and usability with your smartphone, Computer Science Conference for University of Bonn Students 2016, University of Bonn. 25 May 2016, 86 – 97.

[16] J. Aguirre, A. Moquillaza, F. Paz, A user-centered framework for the design of usable atm interfaces, in: Wang W. (Eds), Lecture Notes in Computer Science, Springer Publishing, New York, 2019, pp. 163 – 178.

[17] N. Mathew, M. Jacob, R.M. Jose, S. Siby, N. Sekhar, QR based card-less ATM Transactions, Int. J. Sci. Res. Dev. 2(2) (2016) 81 – 83.