Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2021 SCPE. Volume 22, Issues 2, pp. 273–282, DOI 10.12694:/scpe.v22i2.1920

ENHANCED SECURE ATM AUTHENTICATION USING NFC TECHNOLOGY AND IRIS VERIFICATION

MAHIMA BISWAS, NEER CHOKSI, PARITA OZA AND SMITA AGRAWAL[*]

Abstract. In today's world technology has advanced to such an extent that it is interchangeable with connection and convenience. ATM was one of the major breakthroughs, and over the time it has provided better convenience in fulfilling one's banking needs. Although, there are certain predicaments that such ATM transactions are susceptible too. The conventional PIN based authentication that is presently accustomed in all ATM apparatus is liable to shoulder surfing, hassle in remembering the multiple PIN and the rest. The physical card brings along setbacks in particular, wearing out of the magnetic strip attributable to frequent usage, losing or getting it stolen. Aside from these there are other unlawful activities that are carried upon. The objective of this paper is to present a solution to the above stated problems. In contrast to standard architecture, the proposed solution incorporates NFC enabled smartphones as a substitute for physical card and iris based authentication for PIN.

Key words: Internet of Things, Wearable devices, Security

AMS subject classifications. 68M25

1. Introduction.

When it comes to making banking activities approachable, the role of the ATM cannot be overlooked. Hence, it is crucial to make such activities secure yet convenient [12]. Authentication using PIN (Personal Identification Number) is ubiquitous, but comes with many downsides [15]. First, ATM skimming, skimming devices and small cameras may be fit to steal authentication details. Second, physical cards have magnetic strips which get damaged due to frequent usage and become non-functional. Third, physical cards take users longer to authenticate [8]. Near Field Communication (NFC) is a wireless technology that requires very tiny proximity between two NFC-enabled devices in order to establish a connection [12].

NFC has an array of advantages over Bluetooth, RFID(Radio Frequency Identification) and other such technologies in the aspect of secure transaction [13]. There are several factors that make NFC dominant over other wireless technologies. Unlike Bluetooth and RFID, NFC tag is passive, it is read or written by the powered terminal. Whereas in the case of Bluetooth and RFID, both of these require some power source. As mentioned, small distance between respective devices is a requirement for this technology to work, there is a poor possibility of data to get stolen during communication [15]. NFC, unlike RFID, establishes bidirectional communication, hence can be used for complex interactions such as Peer-to-Peer sharing. NFC has different modes of communication such as peer-to-peer mode, reader/writer mode and card emulation mode, and each of these modes indicates how NFC will behave in respective context. NFC has varied financial applications. One such application is contact less payment, such payments are made through wallets in smartphones, smart watches or tap-to-pay credit and debit cards [12].

One of the examples of smart cards is Visa payWave that uses an embedded computer chip to send payment information to a secure reader at the point of sale. To make payments users may wave their card or device within 2.5-5 cm (1-2 inch) of the reader. This NFC through ATM transaction will transform the way conventional transactions are done, in a more secure manner. Since PIN is the classic approach, multifarious ways have been discovered by the imposters to compromise the system [1, 10]. As opposed to this, biometric technology has a wide range of benefits, from a user's stance bio-metric is greatly convenient and faster [18]. Moreover, as biometric authentication cannot be delegated, no transaction can be made without the consent of the user [5]. The level of security provided by bio-metric is again undeniable.

[*]Department of Computer Science and Engineering, Nirma University, Ahmedabad, India (20bce501@nirmauni.ac.in, 20bce504@nirmauni.ac.in, parita.prajapati@nirmauni.ac.in, smita.agrawal@nirmauni.ac.in)

Refonaa et al. [19] proposed a model to enhance security in ATM account with the help of biometric system. This framework used two security parameters: portable help and biometric. For authentication purpose author used fingerprints. The model consists of various modules such as Registration of use, Enrollment of finureprints, Sending an email, Account Login and Finger print verification.

Anothor work in similar domain is presented in [21] by Sangeetha,with an objective to introduce a framework for current ATM system to confirm withdrawal message and to introduce second level authentication framework where there is withdrawal limit.

1.1. Research Contribution. To fulfill banking needs, ATM is one of the chief innovations and is providing well suitability. Despite the success of ATMs, ATM transactions are still vulnerable to safety breaches. The conservative PIN based verification that is presently familiarized in all ATM gadgets is accountable to shoulder surfing. We propose a solution to this problem by incorporating biometric details during the authentication process. The proposed work includes NFC-enabled smartphones as a substitute for a physical card. We also take into account Iris-based authentication for PIN number. Apart from Iris, finger-print, voice, and face are a few other biometrics. In our work, we also have given a comparative analysis of all these biometrics and selected Iris because it has a high level of security as there is no way to forge Iris also it is compatible with contact lenses and spectacles. Iris-based verification confirms that the user will not have to worry about transactions being made without his/her approval. The small proximity need of NFC makes sure a secure transfer of sensitive details. This proposed unification of NFC and Iris authentication can surely boost the security of existing ATM systems.

1.2. Paper Organization. The rest of the paper is structured as follows: Section 2 presents reviews of various biometric technologies. Section 3 presents related work in the domain. Our proposed model is presented in section 4. We have assessed the robustness of the proposed work in section 5. Future direction and opportunities are discussed in section 6. We finally end with a conclusion in section 7. Oranization of ppaer is pictorialy presented in figure 1.1.

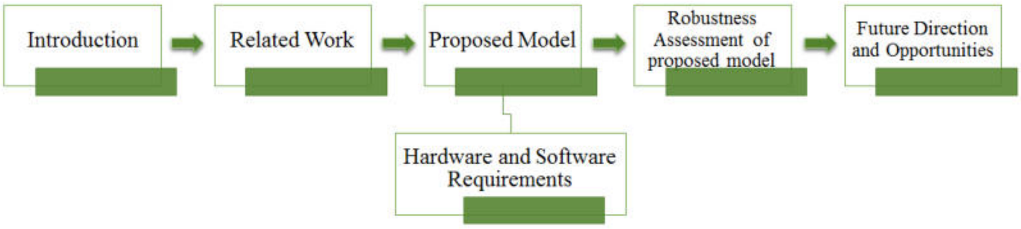
Introduction
Related Work
Proposed Model
Robustness Assessment of proposed model
Future Direction and Opportunities
Hardware and Software Requirements

Fig. 1.1. *Paper Organization*

2. Biometric Technology Review:. Biometric technology has a wide range of benefits, from a user's stance bio-metric is greatly convenient and faster [18].. The Comparative study on various biometric technology presents in this section.

- **Fingerprint** based recognition is one of the oldest approaches used to authenticate and identify a person uniquely. Fingerprints are believed to be never changed throughout the person's life span. Also, the fingerprints on both the fingers of the same individual are different [20]. Fingers have ridges and furrows, those are used to identify a person in fingerprint recognition systems. The two fundamental principles immutability (ridge patterns never change during the lifetime) and uniqueness (distinct ridge patterns on different fingers of the same individual) are used in identification of individual's fingerprint [20].
- **Voice recognition:** Voice recognition biometric is also famously known as Speaker Recognition Biometrics. The voice of a person is a combination of physical and behavioural aspects. The vocal tract, lips, nasal cavity and shape and size of mouth are the physical characteristics and the pronunciation, emphasis, speed of speech, accents are the behavioural characteristics [20]. As a person's voice can be

forged easily, voice recognition is not considered a reliable system. Voice recognition system employs three styles of spoken input as Text dependent, Text prompted and Text independent. [2].

- **Face recognition** system identifies a person based on its facial features like size, diameter and location of nose, eyes, lips and other such. Face recognition can be carried out in the following ways [20][2]:
  1. Facial metric: The location and shape of facial attributes are measured. For example, distance between nose to lip or pupil to chin
  2. Eigen faces: The overall face image is analyzed i.e., collection of weights describing the canonical faces.
  3. Skin texture analysis: This is an emerging technique of face recognition along with other visual details of skin. Finding the location of the unique spots, lines and patterns in a person's skin.
- **Iris** recognition systems are used for high levels of security and authentication. Iris of two humans can never be the same, even for twins it is different. Iris recognition offers a very high capability to distinguish between individuals, even between user's left and right eyes[5][20]. Iris is a unique self-generated pattern which remains stable throughout adult life [22]. The characteristics of the iris cannot be changed by the eye surgery or the wearing of glasses and contact lenses.[20]. Hence we can say that iris can be considered as most reliable when it comes to authentication [23] and security [17].

Each biometric has its merits and demerits. Table 2.1 comparatively discusses level of accuracy and security of each biometric along with its working mechanism.

3. Related Work. Lots of work has been done in the domain of secure ATM transactions. This section presents different design facets that have been used by various researchers in the domain.

Ranasinghe et al. [18] has presented a scheme wherein the proposed device design works as RFID or NFC along with fingerprint authentication. Choices are given for selection of input and output of data. After selection, data is exchanged between device and NFC/RFID reader via RF signals but prior to that fingerprint authentication is carried out. Only after validation data exchanging process is proceeded. The RFID/NFC reader device consists of a power button, navigation buttons, fingerprint scanner and display screen.

Hassan et al. [8] has presented a card-less model in which the card is replaced with fingerprint and a shuffling keypad method is used where the proximity sensor mounted upon the terminal senses the finger of the user and changes the layout of the keypad. Different layout for each time a finger of the user is sensed.

A card-less NFC enabled approach was proposed by Mahansaria et al.[12] In this work, the mobile device exchanges required details with a terminal via NFC mounted upon the ATM apparatus. The process starts with the user entering username and PIN. A default PIN is generated at the time of registration. Entered credentials are verified and upon successful authentication, an OTP is generated. OTP and the username is read by the NFC reader, validated by the authentication server, and finally a transaction is granted upon successful validation. The presented idea works in Card Emulation Mode.

Madalapu et al. [13] proposed an NFC enabled solution where an ATM card has to be swiped as an initial step. Subsequently, the user has to tap the NFC enabled phone on the reader fixed upon the terminal. The reader contains an URL which when read will open up the browser within the smartphone and the user will be prompted to enter a pre registered Mobile number. Having this step followed, a consecutive process involves the user entering a Pattern password that was registered during the registration process. The authentication process is completed by the user entering the generated OTP on the ATM screen within a preset time.

Mohanty et al. [15] brought forward an architecture where there are card taps upon the terminal, and upon tapping the NFC enabled cards data from the card is read by machines. PIN generated in the android application is entered and then verified against the data in the database. If authenticated then the user gets logged in and transaction is permitted. The card specific details are prewritten into the NFC memory chip by admin at the time of issuing.

Muley et al. [16] has also proposed a card-less model where the fingerprint is replacing the physical card. The ATM servers will have many samples of users' fingerprints and the system will verify the scanned fingerprint against every sample unless a matching sample is found. This system only works with customers having one account.

Table 3.1
Comparative study among different bio-metrics

Bio-metrics	**Working**	**Accuracy**	**Level of Security**
Finger-print	When the finger is placed on sensor surface, the ridges of the finger touches the surface, hollow distance between the ridges can also be observed, these distances is calculated by the sensor and later used while authenticating user	Medium level accuracy can be achieved as a person might get a cut on the finger which can result into nonrecognition of that person, moreover wet fingers may also lead to the same	Medium level security as many ways have been discovered to forge person's fingerprint
Voice	Firstly, the biometric software registers the voice sample of a person. Then a statistical methodafter recording and analysing the voice of many distinctive characteristics creates a voice print or biometric model, this model is then encrypted and stored in a secure database. So, when the person interacts with the system, the system compares the respective person's voice sample with one stored in the database.	There is a low level of accuracy here as the voice of a person is physical and behaviour dependent. In addition to this, it is non-viable for a person to speak at the same pace and frequency consistently.	Low level since it is immensely susceptible to forgery
Face	A picture of a person is captured first by software, then key factors of face geometry are identified like distance between an eye, or distance from forehead to chin and several other parameters. For authentication such parameters are recognized and compared with parameters stored in the database.	Medium level accuracy as it works on principle of analysing several facial geometric parameters, and at times there can be changes in a person's facial appearance due to makeover, age, surgery or any injury which can lead to the system showing in- appropriate results.	Medium level as facial traits change / vary over time.
Iris	The camera, in iris recognition, locates the centre of a person's pupil, edge of iris, eyelids, and eyelashes. The iris scanner software analyzes and translates to the iris template. This data is then compared to authenticate the user.	High level accuracy as it is compatible with contact lenses and even eyeglasses and can be used by blind people too, as long as they have an iris.	High level security because there is no way a person's iris can be forged or duplicated.

Table 3.2
Different communication and authentication technologies availed by the researchers in their work

Ref	Communication Technologies				Authentication Technologies				
No	NFC	RFID	Card less	Card based	Face	Finger-print	Voice	Iris	OTP/ PIN
[18]	Yes	Yes	Yes	No	No	Yes	No	No	No
[8]	No	No	Yes	No	No	Yes	No	No	Yes
[12]	Yes	No	Yes	No	No	No	No	No	Yes
[13]	Yes	No	No	Yes	No	No	No	No	Yes
[15]	Yes	No	No	Yes	No	No	No	No	Yes
[16]	No	No	Yes	No	No	Yes	No	No	No
[24]	No	No	Yes	No	No	Yes	No	No	Yes
[25]	No	No	Yes	No	No	Yes	No	Yes	No
[19]	No	No	Yes	No	No	Yes	No	No	Yes
[21]	No	No	Yes	No	No	Yes	No	No	Yes
[14]	No	No	Yes	No	Yes	Yes	No	No	Yes
[9]	No	No	Yes	No	No	Yes	No	No	Yes
[6]	No	Yes	No	Yes	No	Yes	No	No	No
[7]	No	No	Yes	No	No	Yes	No	Yes	Yes
[4]	No	Yes	No	Yes	No	Yes	No	No	Yes
[11]	No	No	Yes	No	Yes	No	No	No	Yes
[3]	No	No	No	Yes	Yes	Yes	No	No	No

In this work as proposed by Taralekar et al. [24] substitutes physical cards with fingerprints and incorporates GSM modules for OTP generation. The databases are stored on cloud and using web services access to all bank accounts linked to the user are given. First step of authentication requires a fingerprint to get validated. Upon successful validation UID is given and using this UID all the details from the bank database are fetched. Furthermore, the user selects the bank account to make transactions displayed on the screen from all the accounts that the user holds. After selection of bank account and before transaction OTP generated using GSM module sent to user's registered mobile has to be entered and then transaction is granted.

Tyagi et al. [25] here a bimodal biometric system has been brought forward. First the user enters the amount to be withdrawn. If the amount is less than 10,000 then the user has to go through a single authentication process which requires only a fingerprint to be scanned. However, if the amount is more than 10,000 then two authentication processes are involved, which is iris recognition and digital signature. In iris recognition, the iris pattern is scanned and verified against the sample available in the database, if valid then the user is allowed to proceed with the second level of authentication where a digital signature is asked to provide to complete the verification process. If the provided digital signature is valid then the transaction is granted.

Manish et al. [14] introduced a bimodal biometric system. The system involves enrolling the customer data into the database. Secondly, there is the Login Phase where registered users can login by providing their fingerprint, scanning their face and then completing the process by receiving an OTP pin. After successful verification of all these three inputs , a transaction is granted.

Researchers of this domain have incorporated many different technologies in their proposed design. Table 3.2 presents various communication and authentication technologies that have been put to use in the domain by different researchers.

4. Proposed Model. Since the use of smartphones is pervasive, and every individual has a unique iris pattern. designing a card-less unimodal biometric system that replaces the traditional ATM card with the user's NFC enabled smartphone and Iris recognition based authentication instead of PIN. Model proposed incorporates Host Card Emulation mode. All the sensitive details will get stored into the server of respective banks. As and when the authentication process is initiated by the user via the application, required details are

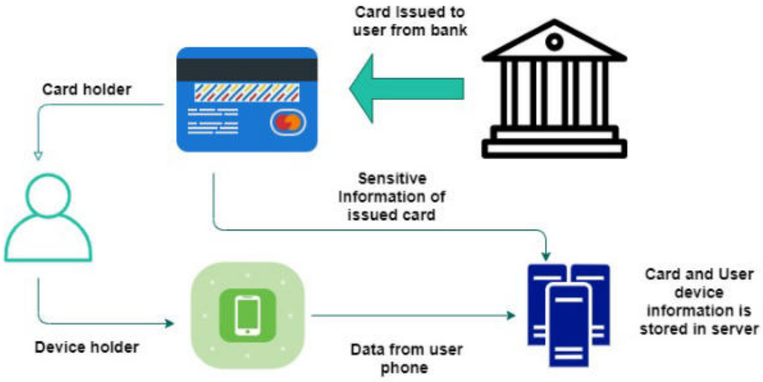
Card issued to user from bank
Card holder
Sensitive Information of issued card
Card and User device information is stored in server
Device holder
Data from user phone

Fig. 4.1. *Registration Stage*

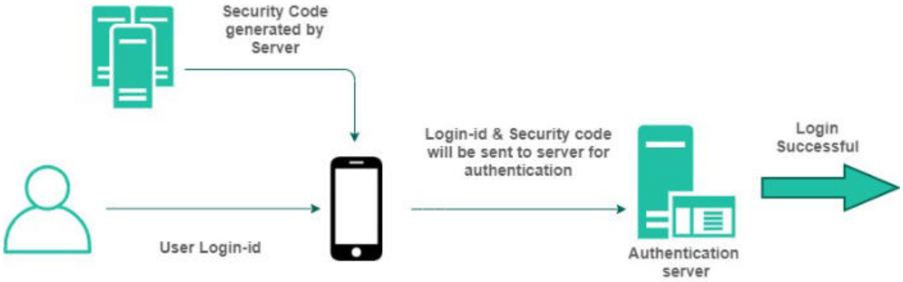
Security Code generated by Server
Login-id & Security code will be sent to server for authentication
Login Successful
User Login-id
Authentication server

Fig. 4.2. *Login Stage*

sent from the server to the user's smartphone. Each bank will have its own custom application.

As mentioned in Fig 4.1, when a card is issued to the user, the card will get registered into the bank's server. All the sensitive details associated with the card will get stored into the server by the issuer at the time of issuing. When a card is issued to the user, the card will get registered into the bank's server. All the sensitive details associated with the card will get stored into the server by the issuer at the time of issuing.

As mentioned in Fig 4.2, after registration, the user will have to log in into the custom application with a user id and security code. User id will be unique and provided from the bank, and the security code will be dynamic. For each login, there will be different security code, generated by the server and sent to the registered mobile. For users having different accounts, will be provided with different user id associated with each account.

As mentioned in Fig 4.3, for initiating the authentication process, first the security mechanism of the smartphone will have to be bypassed. It could be either in pass-code or pattern or biometric. Following that, the server will send a token number instead of the original account number which will be sent and stored within the smartphone. The sent token number will be dynamic in nature and will have no relevance to the original card data and only be valid for 10 minutes. Once the time period gets exhausted that token will no longer be in use. Once the token is received the user will be asked to swipe the smartphone before the NFC enabled ATM terminal. The token will be read by the reader and the user will be prompted to get his/her Iris scanned by the scanner mounted upon the terminal.

As mentioned in Fig 4.4, the scanned Iris data and the token number will be sent to the host processor, the host processor will map the token number with the original account number and match the iris data with the existing iris sample.

Having verification done successfully, an OTP will be sent in the user's registered number which is to be entered in the ATM terminal. After validating the entered OTP, the transaction will be granted for 20 minutes. Once the given time limit is passed. The user will have to re-authenticate.

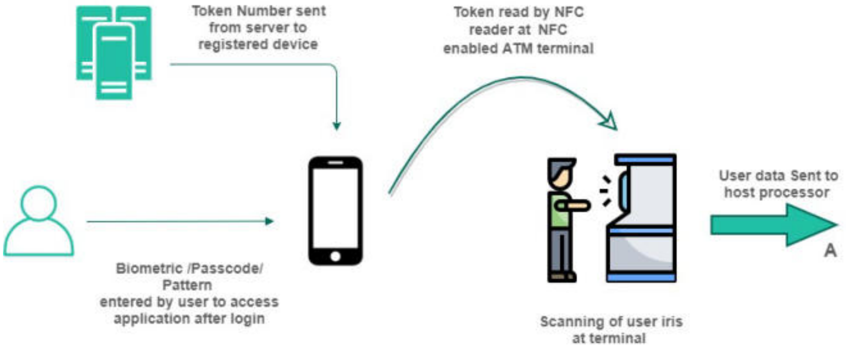
Token Number sent from server to registered device
Token read by NFC reader at NFC enabled ATM terminal
User data Sent to host processor
A
Biometric /Passcode/ Pattern entered by user to access application after login
Scanning of user iris at terminal

FIG. 4.3. *Authentication Stage*

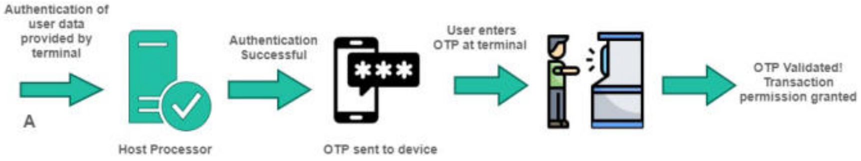
Authentication of user data provided by terminal
A
Host Processor
Authentication Successful
OTP sent to device
User enters OTP at terminal
OTP Validated! Transaction permission granted

FIG. 4.4. *Acknowledgment of verified details with an OTP*

TABLE 4.1
Hardware and Software Requirements

Software Requirements	
Modules	**Description**
Login Page	This module is used to get user-id and password.
Entry lock	This module will authenticate user biometric/pin/password to let user use the application.
Inquiry module	this module will allow the user to view his account user.
History module	This module will help users to know their transaction history.
NEFT/Fund Transfer module	This module is required in order to let users transfer money online.
Change password	this module is used to change login-password
Report Transaction/Concern	this module is used to help user report any concerns or transactions not committed by them
Hardware Requirements	
Component	**Description**
NFC enabled device	A NFC incorporated mobile device is required for communication with the terminal.
ATM terminal	A NFC reader incorporated an ATM terminal.
Iris Scanner	Iris scanner for user identification which will be mounted on the ATM terminal itself.
Authentication server	Used to send Token to user device and verify token number as well as verify user iris sample sent by terminal to server
Database server	Used to store information of card issued to user along with their device and iris data which is later used to authenticate user for transaction.

4.1. Hardware and Software Requirements. In order to implement the proposed model, basic hardware and software modules are listed out in Table 4.1.

Table 4.2
Robustness analysis of the model

Ref.	Issues	Issues addressed by proposed model
[8]	In this paper, the proposed card less approach involves fingerprint as security mechanism which as discussed in sec 1, is not often secure and is subjected to fingerprint forgery. In addition to that, it is PIN based which is again susceptible shoulder surfing	· This model is free from PIN based authentication that is less secure and susceptible to shoulder surfing attack. ·The biometric chosen for authentication is iris which has poor possibility to get forged. ·The level of accuracy is high as iris detection can be done through glasses or contact lens too ·User only needs to carry his/her smartphone from which the authentication is to be done. · There is no need of carrying different cards for different accounts as the smartphone is the one step platform for authentication of all accounts. ·This model ensures that the sensitive details of the user are still safe in case the smartphone gets compromised as locally on the smartphone no data linking to the user's account gets stored. ·In the authentication process, the involvement of iris verification makes certain that even if the smartphone is not under user's possession, the authentication process stays unfulfilled and hence, transaction and any other activity is not granted.
[13]	The researchers of this paper proposed an NFC enabled solution which incorporates two devices, a physical NFC card as well as the user's smartphone. For security, there is pattern-based authentication which needs to be remembered and can also get stolen.	
[15]	This model proposed in this paper is card based and is susceptible to many predicaments associated with physical cards discussed in the paper The data specific to one account is pre-written at the time of issuing which makes user to carry multiple cards for multiple bank accounts	
[16]	The researchers of this paper have proposed a design that works for users having one bank accounts	
[24]	The system that has been proposed in this paper involves a GSM module which is susceptible to electromagnetic interference and leads to substantial amount of latency	
[18]	In this paper the device that the researchers have proposed is based on fingerprint verification which has low accuracy. Moreover, here it is required for the users to carry an additional device for inputting required details.	
[12]	The researchers have proposed a model that is completely card less. However, it is PIN based and comes with many downsides of PIN based systems.	

5. Robustness Assessment of proposed model. Different researchers have presented different models for enhancing the authentication process, making it more secure and robust . However, there are some issues in their proposed designs. In Table 5.1 the issues in the different design facets that have been discussed in sec 2 are taken into consideration and addressed by the model proposed in this paper.

6. Future Direction and Opportunities. Near Field Communication is the latest emerging technology which can be used to solve issues of many current technologies used like RFID. NFC in the upcoming future will be used in many sectors, one of the sectors related to banking is covered in this paper. In future, sclera vasculature biometric technique can be used for high level security authentication. Additional things for further research in NFC [26]:

1. Development of required NFC standards from policy, regulations and legal points of view.
2. The economic performance of NFC developments
3. Potential NFC-enabled applications that are operating in peer-to-peer mode, adoption issues
4. Possible implications of cultural differences on adoption of NFC technologies
5. Impacts of NFC technologies on companies, organizations and business models

7. Conclusion. In this day and age, security of ATM systems has become paramount as multifarious ways have been discovered to compromise the system. There are many pitfalls in the existing system such as they are prone to security breach due to simple PIN based authentication. Moreover, remembering PIN for different accounts is also a impediment. The usage of physical card also carries along obstacles particularly, getting it stolen. This paper proposes a model alternative to the existing system, that uses NFC technology and biometric for authenticating users. We have compared various biometrics and choose to work with Iris due its inherent advantages. Iris based authentication makes certain that the user will no longer have to be concerned about transactions being made without the user's consent, PIN theft, remembering multiple pins, etc. Tiny proximity requirements of NFC ensure secure transfer of sensitive details. Hence, the amalgamation of NFC and Iris verification enhances security of existing ATM systems.

REFERENCES

[1] S. Bharadwaj, M. Vatsa, and R. Singh, *Biometric quality: a review of fingerprint, iris, and face*, EURASIP journal on Image and Video Processing, 2014 (2014), pp. 1–28.

[2] D. Bhattacharyya, R. Ranjan, F. Alisherov, M. Choi, et al., *Biometric authentication: A review*, International Journal of u-and e-Service, Science and Technology, 2 (2009), pp. 13–28.

[3] P. Choudhary, A. Tripathi, A. K. Singh, and P. C. Vashist, *Implementation of integrated security system by using biometric function in atm machine*, in Intelligent Computing in Engineering, Springer, 2020, pp. 33–42.

[4] V. Devika and C. Ankitha, *Multi account embedded system with enhanced security*, (2020).

[5] M. Faundez-Zanuy, *Biometric security technology*, IEEE Aerospace and Electronic Systems Magazine, 21 (2006), pp. 15–26.

[6] S. Gokul, S. Kukan, K. Meenakshi, S. V. Priyan, J. R. Gini, and M. Harikumar, *Biometric based smart atm using rfid*, in 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE, 2020, pp. 406–411.

[7] M. HARINE, K. PADMAVATHI, and M. L. V. KUMAR, *Fingerprint and iris biometric controlled smart banking machine embedded with gsm technology for otp*, (2020).

[8] A. Hassan, A. George, L. Varghese, M. Antony, and K. Sherly, *The biometric cardless transaction with shuffling keypad using proximity sensor*, in 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), IEEE, 2020, pp. 505–508.

[9] M. Y. Imam, N. Jannat, and G. S. Khan, *Multi-banking automatic teller machine transaction system by utilizing gsm and biometric identification with one single touch*, (2020).

[10] A. Joy et al., *A systematic review comparing different security measures adopted in automated teller machine*, Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12 (2021), pp. 388–393.

[11] O. Lala, H. Aworinde, and S. Ekpe, *Towards a secured financial transaction: A multi-factor authentication model.*

[12] D. Mahansaria and U. K. Roy, *Secure authentication for atm transactions using nfc technology*, in 2019 International Carnahan Conference on Security Technology (ICCST), IEEE, 2019, pp. 1–5.

[13] A. Mandalapu, D. Deepa, L. D. Raj, et al., *An nfc featured three level authentication system for tenable transaction and abridgment of atm card blocking intricacies*, in 2015 International Conference and Workshop on Computing and Communication (IEMCON), IEEE, 2015, pp. 1–6.

[14] C. Manish, N. Chirag, H. Praveen, M. Darshan, and D. K. Vali, *Card-less atm transaction using biometric and face recognition–a review.*

[15] A. Mohanty, P. Giria, S. Pal, V. K. Acharya, and R. Hegde, *Nfc featured triple tier atm protection*, in 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT), IEEE, 2018, pp. 482–487.

[16] A. Muley and V. Kute, *Prospective solution to bank card system using fingerprint*, in 2018 2nd International Conference on Inventive Systems and Control (ICISC), IEEE, 2018, pp. 898–902.

[17] N. Patel, P. Oza, and S. Agrawal, *Homomorphic cryptography and its applications in various domains*, in International Conference on Innovative Computing and Communications, Springer, 2019, pp. 269–278.

[18] R. N. D. Ranasinghe and G. Z. Yu, *Rfid/nfc device with embedded fingerprint authentication system*, in 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), IEEE, 2017, pp. 266–269.

[19] J. Refonaa, S. J. Shabu, S. Dhamodaran, L. J. Grace, et al., *To enhance security mechanism in atm account using biometric system*, in Journal of Physics: Conference Series, vol. 1770, IOP Publishing, 2021, p. 012017.

[20] T. Sabhanayagam, V. P. Venkatesan, and K. Senthamaraikannan, *A comprehensive survey on various biometric systems*, International Journal of Applied Engineering Research, 13 (2018), pp. 2276–2297.

[21] T. Sangeetha, M. Kumaraguru, S. Akshay, and M. Kanishka, *Biometric based fingerprint verification system for atm machines*, in Journal of Physics: Conference Series, vol. 1916, IOP Publishing, 2021, p. 012033.

[22] P. Sevugan, P. Swarnalatha, M. Gopu, and R. Sundararajan, *Iris recognition system*, International Research Journal of Engineering and Technology, (2017).

[23] Y. Shah, S. Joshi, P. Oza, and S. Agrawal, *An insight of information security: A skeleton*, International Journal of Recent Technology and Engineering, (2019), p. 2600–2605.

[24] A. Taralekar, G. Chouhan, R. Tangade, and N. Shardoor, *One touch multi-banking transaction atm system using biometric and gsm authentication*, in 2017 International Conference on Big Data, IoT and Data Science (BID), IEEE, 2017, pp. 60–64.

[25] A. Tyagi, R. Simon, et al., *Security enhancement through iris and biometric recognition in atm*, in 2019 4th International Conference on Information Systems and Computer Networks (ISCON), IEEE, 2019, pp. 51–54.

[26] B. Özdenizci, M. Aydin, V. Coskun, and K. Ok, *Nfc research framework: A literature review and future research directions*, (2010).

Edited by: Pradeep Kumar Singh et al.
Received: July 1, 2021
Accepted: Oct 25, 2021