ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

An Authentication of ATM System Using DNA bar Code

S.Buvaneswari[1], V.Vijaya Deepa[2]

Research Scholar, Dept. of CS, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[1]

HOD, Dept. of CS, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[2]

ABSTRACT: As the days passes, wide range of security flaws have been increased and at the same time security concerns in user identification and authentication has also increased and grabbed a prominent role in banking sector. This paper presents a high secure system that increases the ATM security. In this scenario no need to remember the passwords and the reference DNA data will be digitized and converted to barcode by using barcode generator, which is stored back of ATM card. This invention can identify the proper user of the ATM card by collating the measured DNA data and biometric security, Global positioning system(GPS) and mobile messaging we have design an algorithm which increase security of electronic transaction and more reliable to user. A three layer security model to enhancing security of electronic transaction is proposed in this paper. We can get rid of many financial losses and illegal attacks.

KEYWORDS: ATM , Authentication, DNA barcode generator, Security, Biometric Security, Finger Print, Iris recognition, Encryption, Decryption, GPS Authentication.

I. INTRODUCTION

There are two ways customer can perform their banking activities. First one physically interacts with banking staff and second one is Electronic transaction (ATM transaction, online transaction and E-coin). For the first case bank staff manually authenticates a user based on check book, customer signature and photo. In the case of Electronic transaction bank follows conventional method where authenticate a user based on user id and PIN (personal identification number). But in this case security is one of the major issues regarding electronic transaction. In recent year the rate of cyber-crime increases day by day. The criminal attack not only cyber security and cyber information they also collect personal information and attack on Electronic banking system.

Fraud technique like card skimming, shoulders surfing etc has been ascertained recently. So as to extend the amount of security in ATM system, use of biometric technique and DNA barcode helps for easy verification. Biometrics will be outlined as a measurable physiological and behavioral characteristic that may be subsequently compared and captured with another instance at the time of verification. These technologies area unit a secure means of authentication as a result of information of each method are distinctive, cannot be shared, cannot be traced and can't be unnoticed.
The main goal of this work is defining a system for Electronic transaction which is reliable to both a user and bank. In this paper we have design an algorithm which ensured high level security in Electronic transaction and define an efficient and highly scalable Money transaction system. I have designed an algorithm with combination of DNA and biometric security and also mobile securities are enable. This designed algorithm ensures e-security using three layer security systems.

These three layers are:

- Layer -1: Insert ATM card which is having DNA barcode.
- Layer -2: Biometric security using Fingerprint or Iris recognition.
- Layer -3: Mobile security using GPS or mobile SMS.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

II. RELATED WORK

Implementation of the security by using fingerprint recognition and GSM, by Pennam Krishna murthy & Maddhusudhan reddy using fingerprint recognition method, remote authentication, message alarming and Gobar and direction filter algorithm, it is more safe and reliable and easy to use but it is slow when dealing with high capacity requirements. The United Kingdom recently launched identity card scheme which has been analyzed by Shaikh and Rabaiotti(2009). They approach the scheme from the perspective of high volume public deployment and describe a trade-off triangle model. They have found that there is a trade-off between several characteristics, i.e., accuracy, privacy and scalability in biometric based identity management system, where emphasis on one undermines the other (Shaikh and Rabaiotti2009). Fingerprint recognition using minutia score matching by Ravi J K.B.Raja, Venugopal K.R. using the minutia score matching method and gives the better FMR value compare to the existing. Fingerprint validation and outlier detection using minutia approach in network security by Devi sirivella, Mrs.D.Raagavamsi gives the better result in real time applications from database type of attacks. Recently Govt. of India started a biometric based ID card i.e., „unique identification authority of India"; it provides a unique identity to person residing in India.

III. DISADVANTAGES OF EXISTING SYSTEM

This is a harmful function that is used to allow customer to select their PIN's online. In this an attacker discovers the PIN codes. For example those entered by customers while withdrawing cash from an ATM providing they have access to the online PIN verification facility. A bank insider could use an existing hardware security module to know the encrypted PIN codes. This attack required an insider such as an ATM technician who has a key to the machine to place the malware on the ATM. After this the attacker could insert a control card into machine card reader that act as the malware and give them control of machine through a custom interface and the ATM's keypad. Malware captures magnetic stripe data and PIN codes from the private memory space of transaction processing application installed on a ATM. In this attacker use sophisticated programming technique to break into website which reside on a financial institution network. They can access bank's system to locate the ATM database and collect card information which used later to make a clone card. Most of ATM hackings are due to the use of non-secure ATM machines.

IV. PROPOSED SYSTEM

In this scenario no need to remember the passwords and the reference DNA data will be digitized and converted to barcode by using barcode generator, which is stored back of ATM card. This invention can identify the proper user of the ATM card by collating the measured DNA data Identification and authentication by individuals' biometric characteristics and Mobile security using GPS technology with SMS.

Scalable Electronic Transaction System with 3 Layer Securities:

These three layers are:

- Layer -1: Insert ATM card which is having DNA barcode.
- Layer -2: Biometric security using Fingerprint or Iris recognition.
- Layer -3: Mobile security using GPS or mobile SMS.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

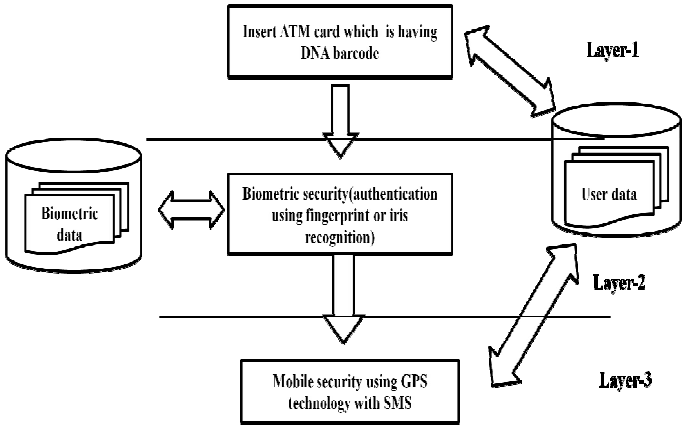

Figure1. Three Layer Security System Flow

Layer 1 Security

DNA is known as DNA profiling , or identity testing, in genetics science, method of isolating and identifying variable components within the base-pair sequence of DNA (deoxyribonucleic acid). This method is developed in 1984 by British bio gist Alec Jeffreys. The procedure for conducting a DNA identity test consist a sample of cells, such as skin, hair or blood cells, which contain DNA. The DNA is extracted from the cells and purified.DNA bar coding is an exciting new tool for taxonomic research. The DNA barcode is a very short, standardized DNA sequence in a well-known gene. It provides a simplest way to find the species to which a plant, animal or fungus belongs. The Consortium for the Barcode of Life (CBOL) is promoting international partnerships that will make people in all countries to better understand and protect their diversity. Barcoding is generating a worldwide, open access library of reference barcode sequences that allows non-taxonomists to identify specimens. The barcode of an unidentified specimen are often compared with the reference barcodes to find the matching species. Barcoding projects have already generated hundreds of thousands of reference barcodes for tens of thousands of species. These species have been selected because they are of special interest to users who need the ability to identify species of scientific, economic, or social importance. The Consortium for the Barcode of Life is creating partnerships among government agencies, local researchers, and NGOs that design and implement the highest priority bar coding projects. The DNA barcode of an unidentified specimen can be read using standard gene sequencing techniques. DNA bar coding includes three types of methods.

1) Working with organisms: grouping, distinctive, and protective voucher specimens in secure repositories
2) Laboratory procedures: Sampling and processing tissue from specimens to obtain DNA barcode gene sequences
3) Managing data: Sharing the DNA barcode sequence and data regarding its voucher specimen in a public database.

Figure2. ATM access using Bar code

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Layer 2 Security

After passing layer 1 system allows user to access layer 2 securities. It's biometric security system. In modern technology there are several biometric security system are available. But most common and reliable security system is Fingerprint and Iris recognition. This layer 2 to can accept both biometric techniques based on vendor and customer choice. Here I have only described fingerprint as a biometric security ensuring technique.

Biometric authentication has become more and more popular in the banking and finance sector. The idea of fingerprint is not only for security but also to overcome the lack of customer understanding on ATM concept. We proposed ATM with biometric, a fingerprint security system, in order to meet its customers" needs who many of them have savings account and need to have access to their money during non-banking hours. The ATM with fingerprint scanner offer excellent security to customer since there is very low possibility of fraud. By using fingerprint recognition customers are more comfortable with the idea of saving their money with the bank because they understand that no one can replicate their fingerprint and take their money. Fingerprint authentication is the most popular method among biometric authentication, fingerprint based identification is one of the most mature and proven technique.

In banking system Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications. At the time of transaction customers enrolment their fingerprint to a high resolution fingerprint scanner. The fingerprint image is transmitted to the central server via secured channel. At the banking terminal the minutiae extraction and matching are performed to verify the presented fingerprint image belongs to the claimed user in bank database. The authentication is signed if the minutiae matching are successful. The proposed scheme is fast and more secure.

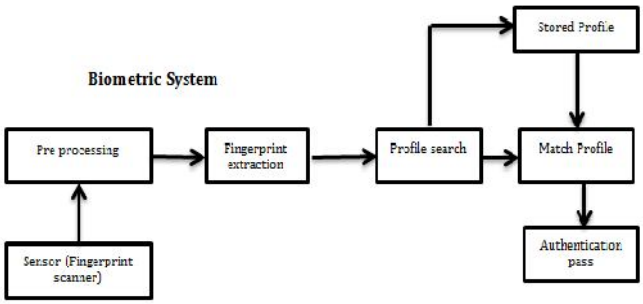

Figure3. Biometric Security

A basic biometric authentication system consists of six main components. These are: Fingerprint scanner, preprocessor, feature extractor, database, and matcher and decision module. The function of the scanner is to scan the biometric trait of the customer. Then pre-processor process biometric data and ready for feature extraction. The function of the feature extraction module is to extract the feature set from the scanned biometric data. This feature set is then stored into the template database. The matcher modules takes two inputs, *i.e.*, feature set from the template database and feature set of the user who wants to authenticate him/her and compares the similarity between the two sets. The last module, *i.e.*, the verification module makes the decision about the matching of the two feature sets. Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

In my system I have allowed 3 times to input fingerprint if it fails first 2 times to authenticate valid customer. If authentication passes then it goes to layer 3 security system.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Biometric Cryptosystem

Fuzzy vault and fuzzy commitment build the biometric cryptosystem**.** They do not generate revocable templates. In the enrollment phase, the helper data is extracted from the template and combine with secret key to form a secure sketch, In the authentication phase, the biometric query is compared with the template stored in the database and key is obtained to check whether the template is valid or not. Fuzzy Commitment is a biometric system that can be used to secure biometric traits represented in the form of binary vectors and fuzzy vault is represented in the form of point set.

Layer 3 Security

This layer ensures security using mobile. It's completely optional based on customer choice. If customers want to ensure high level security then he/she can allow mobile security. After successfully authenticate from layer 2 it check layer 3 is enable or not. If not then it goes to login into customer account directly. If layer 3 enables then it wait for authentication in this step. Here I have introduced 2 type of mobile security.

- GPS based authentication.
- Authenticate via Mobile messaging

GPS based authentication:

This step is optional and enable based on user choice. In GPS based authentication customer need to register valid mobile device and no. into system. And it's mandatory to bring mobile when go for transaction. ATM ensures valid customer based on customer mobile location. If customer mobile location is same as ATM location then system ensure that this customer is valid and proceed to login into customer account. Otherwise it rejects the transaction process and goes to offline.

Authenticate via Mobile messaging:

It's also a common technique to authenticate valid user to send a credential data via SMS. SMS based authentication is used most of the online authentication system. In modern system user get a SMS after login any system for authentication. SMS contain a security code for ensuring security. User provides credential data after getting message in mobile. If user input correct then system consider this user as a valid user.

In that case like as other existing SMS based authentication technique, after passing layer 2 security it send a message to customer mobile with credential data (4 digit code). After getting message customer provide it into system as an input. If Mache credentials data then it ensure customer is authenticate provide permission to access account and transaction money. If user provide wrong code then it's provide three times option to re-input security data. After trying three times system terminate the transaction process.

After passing all layer authentication system guaranteed that this user valid and ensure customer account form fraud access. If any customer passes authentication then he/she can transaction there money electronically. Customer can deposit there money, can withdraw or bill payment. Customer can make e-coin from system.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

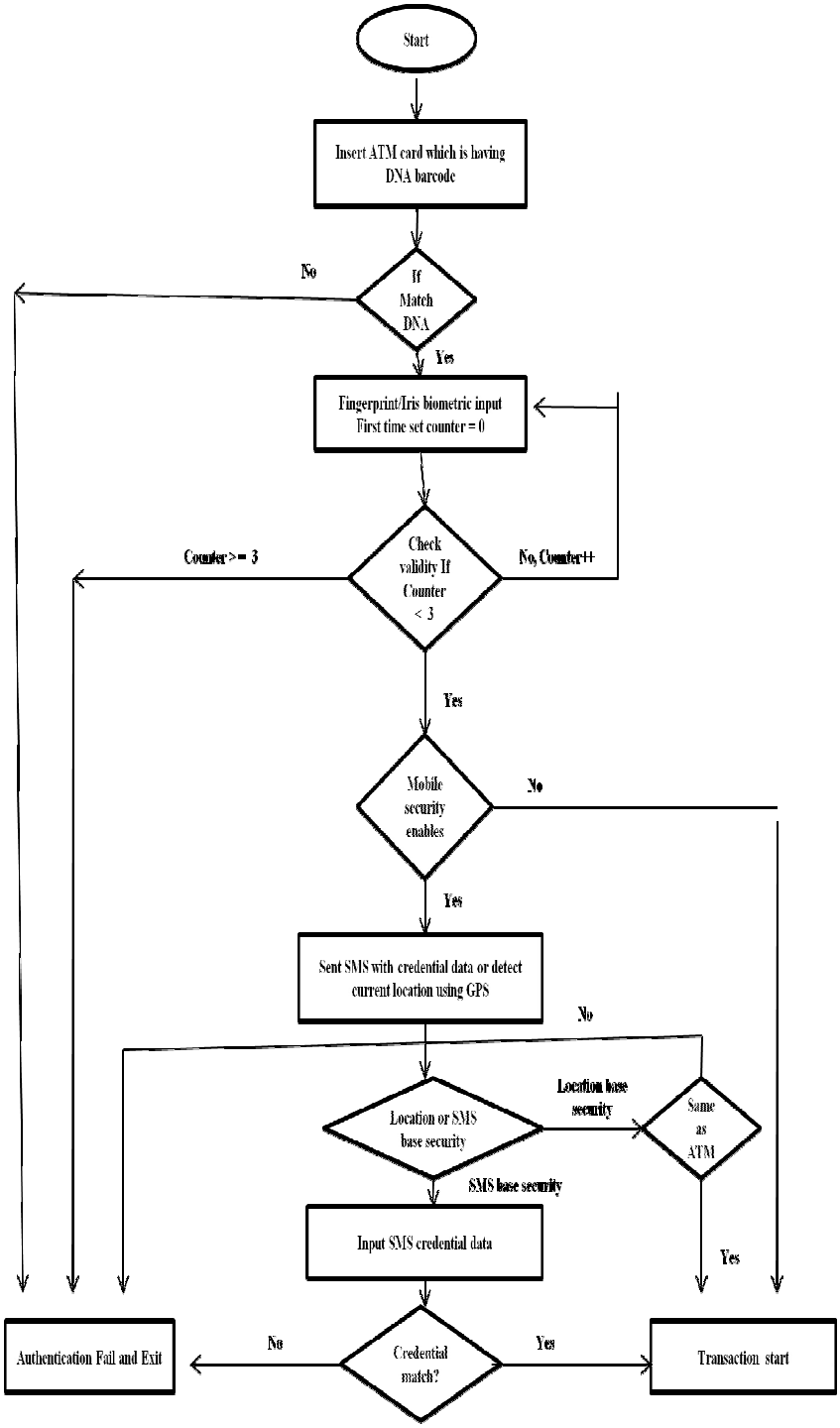

Figure4. A Scalable Electronic Transaction System with 3 Layer Securities

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Advantages of Proposed System

The combination of finger print and DNA data gives more accurate and precise results than existing methods as ATM access with fingerprint and GSM, ATM access with multi modal biometrics and Mobile Security.

- It is used for fast and accurate authentication. It is used as evidence in many applications in computer forensics. It cannot be copied or forged.
- DNA evidence is key to the conviction or exoneration of suspects of various types of crime. Even this method can be used in performing E-transactions and identification of users in many applications. It will provide strong authentication.
- The DNA barcode is a very short, standardized DNA sequence in a well-known gene.

V. RESULT ANALYSIS

This system contains the following infrastructure:

- An ATM with High quality Fingerprint scanner, DNA barcode generator and GPS enable device.
- Server for storing user data (account information, personal information etc.)
- Mobile device with GPS system.

As there are problems in identifying the fingerprints of users in accessing ATM System, a new method is proposed in which normal fingerprint scanner add-ons to DNA barcode generator. At very first the users have to give his or her fingerprint impressions generated by fingerprint scanner and DNA samples while opening the account in the bank. Sampling and processing has been done on DNA samples and finally they are converted to barcode by using DNA barcode generator. The obtained barcode is attached on the back of individuals ATM card. While processing with the ATM, the fingerprint scanner has to be attached with the ATM terminal. When the user inserts his or her ATM card, and then places their finger on fingerprint scanner which captures the impression of fingerprint. The DNA barcode which is present on the back of ATM is scanned. The impression of finger and DNA barcode are taken as input and some of the features are extracted and stored as template. This template verifies with the stored database at bank.

Now user goes to ATM and start accessing his/her account by passing 3 layer securities. Firstly Insert ATM card which is having DNA barcode generator. Figure 5 shows the user interface for 1st layer authentication system. If match the DNA, goes to second layer, otherwise the transaction has been denied.

Figure 5. ATM access using Bar code

In second layer customer input his/her fingerprint using fingerprint scanner. The fingerprint matcher algorithm matches information and authenticate user. Figure 6 shows 2nd layer authentication User interface. If information matches with database then it goes to third layer. Otherwise provide 3 times option for re-try then exit from system. After passing second layer it shows customer basic data on screen for short time and goes down to next phase. Figure 7 shows customer basic data after passing biometric authentication.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

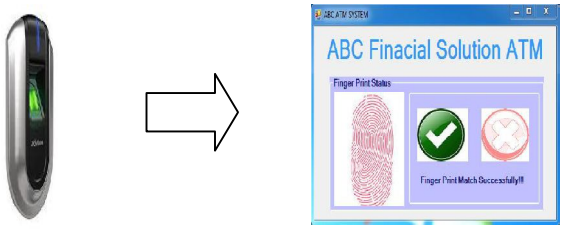

Figure 6.Authentication using Fingerprint

If mobile security is enable then it precede for third layer. Otherwise after passing second layer it directly permitted the user to access his/her account. For the case of GPS based authentication, if there GPS system technique avails then ATM system finds out the current location of customer mobile. If current location of customer is same with ATM location then it consider as a valid user.

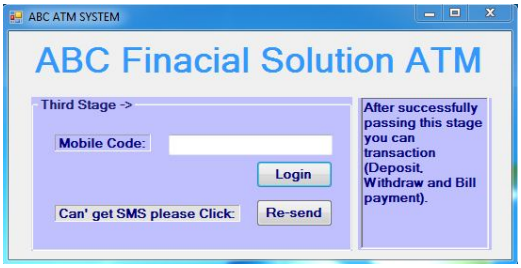

Figure 7. User Interface after Passing Second Layer Authentication

If Mobile messaging system enables then system send a message to customer with a credential data (4 digit code). User input this code into system which uses to authenticate this user at last stem. If input data match with sending data, then system permit to access user account. Figure 8 shows the interface for SMS base authentication.

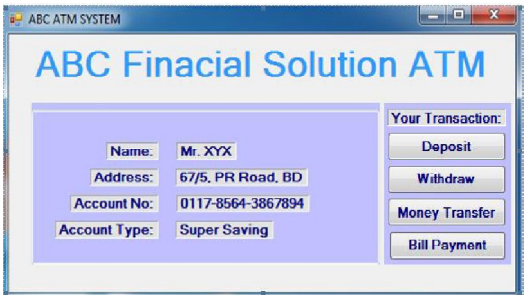

Figure 8. User Interface of SMS based Authentication

Thus authentication completed via three stages. After complete authentication user can deposit there money, can withdraw or bill payment. Customer can make e-coin from system. In figure 9 shows main menu of transaction after login into system. As an example here a customer selected withdraw option to withdraw money from my account. When customer select withdraw option then system provides a screen to input the amount which he/she want to withdraw. The withdraw window shown in Figure 9.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

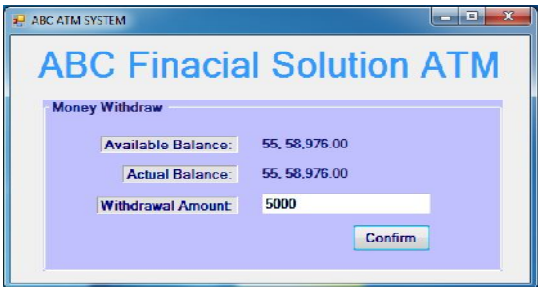

Figure 9. Money Withdraw Window

Thus any valid user can perform transaction deposit, Money transfer from one account to another account, Bill payment or E-coin generation etc. as like as withdraw. Though this system maintains all of existing authentication combines with different layer, it ensure top most security at money transaction electronically.

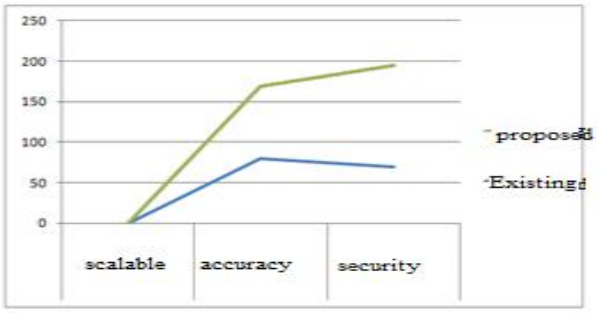

Figure 10. Result Analysis.

VI. CONCLUSIONS AND FUTURE WORK

The growth in the electronic transaction has resulted in greater demand for accurate and fast user identification and authentication. Biometrics refers to the automatic recognition of a person based on physiological and behavioural characteristics. The main reason for introducing biometrics system is to increase overall security. It offers greater security and convenience than traditional methods. The combination of DNA barcode and fingerprint biometric authentication method is very effective in protecting information and it can be a resource in a large area of applications. Security issues related to previous methods can be solved using this technique. In this paper DNA identifying test is time taking process, but it is a unique identification test that no one can forge it or copy it. The authentication method provided to ATM system will be extended in future to minimize the time consumed than the proposed one.

REFERENCES

1. Mohammed Lawan Ahmed "Use Of Biometrics to tackle ATM fraud," International Conference on Business and Economics Research, IACSIT Press, Kuala Lumpur, Malaysia, Vol. 1, pp.: 331-335, 2011.
2. Yang Yun, Mi Jia "ATM terminal design is based on fingerprint recognition," IEEE, 2nd International Conference on Computer Engineering and Technology, pp.: 92-95, 2010.
3. Ravi Kumar Sowmya, Vaidyanathan Sandhya, Thamotharan B. "A new business model for ATM transactions security using fingerprint recognition," International Journal of Engineering and Technology(IJET), ISSN: 0975-4024, Vol. 5, pp.: 2041-2047, Issue No. 3, Jun-Jul 2013.
4. Devi CHSN Sirisha, Patil Maya "Security System For ATM Terminal By Using Biometric Technology and GSM," Global Journal of Advanced Engineering Technologies (GJAET), ISSN: 2277-6370, Vol. 11, pp.: 124-127, Issue No. 3, Year 2012.
5. Indi Trupti S, Raut Suhas D"Person Identification based On Multi-biometric Characterstics, " IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology(ICECCN), pp.: 45-52, Tirunelveli, 25-28 March 2013.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

6. Padmapriya V, Prakasam S. "Enhancing ATM Security Using Fingerprint and GSM Technology," International Journal of Computer Application (IJCA), ISSN: 0975-8887, Vol. 80, pp: 43-46, Issue No. 16, October 2013.
7. Duvey Anurag Anand, Goyal Dinesh, Hemrajani Dr. Naveen "A Reliable ATM Protocol and Comparative Analysis on Various Parameters with other ATM Protocols," International Jouranl of Communication and Computer Technologies (IJCCT), ISSN: 2278-9723, Vol. 01, pp.: 192-197, Issue No. 56, 06 Aug 2013.
8. Sudiro Sunny Arief, VOINE Michel PANDA, Kusuma Tb. Maulana "Simple Fingerprint Minuitiae Extraction Algorithm Using Crossing Number On Valley Structure," IEEE, pp.:41-44, 2007.
9. Das SS, and Jhunu D (2011) Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System. International Journal of Information and Communication Technology Research 197-203.
[10] M.A. Jobling,P.Gill,Encodedevidence:DNA in forensic analysis,Nat.Rev. Genet.5(2004) 739–751.
[11] N. Morling, Forensic genetics, Lancet 364 (Suppl. 1) (2004) s10–s11.
[12] M. Lynch, God's signature: DNA profiling, the new gold standard in forensic science, Endeavour 27 (2003) 93–97.
[13] DNA barcoding- URL: http://www.dnabarcoding101.org/bioinformatics.html
[14] J. Leon, G. Sanchez, G. Aguilar, L. Toscano, H. Perez and J. M. Ramirez, "Fingerprint Verification Applying Invariant Moments", IEEE International Midwest Symposium on Circuits and Systems, **(2009)**, pp.751-757.
[15] L. O'Gorman, "Overview of fingerprint verification technologies", Elsevier Information Security Technical Report, vol. 3, no. 1, **(1998)**.

BIOGRAPHY

Ms.S.BUVANESWARI was born on 15.05.1991 in Tamilnadu, India. She received BSc in 2011 from Vivekanandha College of Arts & Science for Women, Elayampalayam, Affiliated to Periyar University, Salem, Tamilnadu, India. She received B.Ed in 2012 from Vivekanandha College of Education for Women, Elayampalayam, Affiliated to Tamilnadu Teachers Educational University, Chennai, Tamilnadu, India. She received M.Sc in 2014 from Muthayammal College of Arts & Science, Rasipuram, Affiliated to Periyar University-Salem, Tamilnadu, India. She is Pursuing M.phil (full time) from Muthayammal College of Arts & Science in Periyar University, Salem, Tamilnadu, India. Her interested area is ComputerNetworks.

Mrs.V.Vijayadeepa M.Sc.,M.C.A.,M.Phil.,[Ph.D].,received her B.Sc from University of Madras and M.Sc and MCA from Periyar University. She has completed her M.Phil at Bharathidasan University. She is having 10 Years of experience in collegiate teaching and she is the Associate Professor and Head of Department of Computer Science and applications in Muthayammal College of Arts and Science, Rasipuram Affiliated by Periyar University. Her main research interests include personalized web, web information retrieval, data mining, data warehousing and information systems.