International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.203-214
http://dx.doi.org/10.14257/ijsia.2015.9.2.19

An Algorithm for Electronic Money Transaction Security (Three Layer Security): A New Approach

Md. Syeful Islam

Samsung Research Institute Bangladesh Ltd. (SRBD), Dhaka-1205, Bangladesh,
Phone: +8801916574623
syefulislam@yahoo.com

Abstract

In the era of internet, most of the people all over the world completed their transaction on internet. Though the user of electronic transaction or E-money transaction system increase rapidly but the majority person are concern about the security of this system. The growth in online transactions has resulted in a greater demand for fast and accurate user identification and authentication. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. Identification and authentication by individuals' biometric characteristics is becoming an accepted procedure that is slowly replacing the most popular identification procedure – passwords. Among all the biometrics, fingerprint based identification is one of the most mature and proven technique. Along with the combination of conventional system, 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.

Keywords: *E-money, Electronic transaction, Authentication, Security, Biometric Security, Finger Print, Iris recognition, Encryption, Decryption, GPS Authentication*

1. Introduction

Today the regional economies, societies, cultures and educations are integrated through a globe-spanning network of communication and trade. Today's most of business dealings (order receive, delivery confirmation, transaction and business communication) are done on internet. Rapid development of banking technology, Banks provide facilities to their client to transaction their money from won account through a security system using internet. This system is known as electronic transaction. Notwithstanding, we lived in a world where people no longer want to encounter long queues for any reason, they don't not want to wait for too long time before they are attended to and this has led to the increasing services being rendered by banks to further improve the convenience of banking through the means of electronic banking. The growing rate of the popularity of Electronic transaction increased day by day. Now-a-days most of the people make their banking activities such as cash withdrawal, money transfer, paying phone and electricity bills, online purchase beyond official hour's without physical interaction with bank staff using internet. Bank fascinated their customers to carry out banking transactions like, deposits, transfers, balance enquiries, mini statement, withdrawal and fast cash etc. in various ways.

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). [1] 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

ISSN: 1738-9976 IJSIA

and PIN (personal identification number). But in this case security is one of the major issues regarding electronic transaction. Currently Bank provide conventional security (authenticate user using username and password).

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. A lot of criminals inter into the Banking database by breaking security and steal customers' personal details (account information, card details, user id, password etc.) by illegal means. Once criminal get personal information then, the users' account is vulnerable to attack. It's not only threaten for user, it's also for be bank. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation. Currently there is lots of scientist working on online transaction security. Here we have designed three layer security system for authenticate a user in electronic transaction.

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. The paper is arranged as follows. In section 2 we have to identify about the problem domain and motivates the research. Section 3 introduced with the Electronic transaction system and security. In Section 4 we have proposed a scalable electronic transaction system with 3 layer security. Section 5 presented the results analysis and section 6 concluded the work.

2. Problem Domain

Most of the banking system supported both physical and online transaction. But electronic money transaction system is increasingly popular due to the widespread use of the internet-based shopping and banking. That why all of bank think they provide there most of services at internet. In that case most concern is about security. So without ensuring security it's can't be a promising system to customer.

The crime over internet increases rapidly. The Criminal attack on various online system and hacked impotent both personal and professional information. In recent year cybercrime on banking is alarming for both customer and bank. A lot of criminals inter into the Banking database by breaking security and steal customers' personal details (account information, card details, user id, password *etc*.,) by illegal means. Once criminal get personal information then, the users' account is vulnerable to attack. It's not only threaten for user, it's also for be bank.

The need for security is a constant of doing business over the internet because; in essence the Internet is a broadcast medium. E-security enhances or adds value to a naked network and is composed of both "soft" and "hard" infrastructure. Soft infrastructure components are those policies, process, protocols and guidelines that create the protective environment to keep the system and the data from compromise. The hard infrastructure consists of the actual hardware and software needed to protect the system and its data from external and internal threats to security.

There is lots of scientist work on cyber security and proposed there technique to protect online user from cybercrime. Currently there are several techniques available for ensuring security but not satisfy to all labels of users. The goal of this paper is provide a concrete solution regarding cyber security in electronic money transaction. In this paper I have proposed an algorithm with three layer security for ensuring security at electronic transaction.

3. Electronic Money Transaction and e-security

Electronic money or e-money is an evolving term that can have different meanings but in principle involves the use of computer networks and digital stored value systems to store and transmit money. It may have official legal status or not. It may be historical, current or theoretical. The underlying principle of electronic money involves the use of computer networks such as the Internet and digital stored value systems. Examples of electronic money are bank deposits, electronic funds transfer, direct deposit, payment processors, and digital currencies. Electronic money can be understood as a way of storing and transmitting conventional money through electronic systems or as digital currency which varies in value and is tradable as a currency in its own right. [2] Electronic money is a digital equivalent of cash, stored on an electronic device or remotely at a server.

There are several aspects to security when dealing with E-transaction. The first issue is the security of the transaction. How does one know that the customer is valid? Encryption and special serial numbers are supposed to allow the issuing bank to verify (quickly) the authenticity of E-money. The ultimate area of security is faith in the currency.

E-security can be described on the one hand as those policies, guidelines, processes and action needed to enable electronic transactions to be carried out with a minimum risk of breach, intrusion or theft. On the other hand, e-security is any tool, technique or process used to protect a system's information assets. Information is a valuable strategic asset that must be managed and protected accordingly. The degree of e-security used for any activity should be proportional to the activity's underlying value. This security is a risk-management or risk-mitigation tool, and appropriate security means mitigation of the risk for the underlying transaction in proportion to its value. [3-4]

Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities and causation in civil litigation and banks must meet certain standards in order to ensure a safe and secure banking environment for their customers.

4. Proposed a Scalable Electronic Transaction System with 3 Layer Security

Electronic money transfer system facilitates the transactions over internet. Also known as a sample of Electronic Data Interchange (EDI), e-payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking. We have already describe the major challenges of online transaction are security. I have designed an algorithm with combination of conventional and advanced security ensuring technology. This designed algorithm ensures e-security using three layer security systems (Figure 1). These three layers are:

- ✓ Layer -1: Conventional E-security using Username and PIN number.
- ✓ Layer -2: Biometric security using Fingerprint or Iris recognition.
- ✓ Layer -3: Mobile security using GPS or mobile SMS.

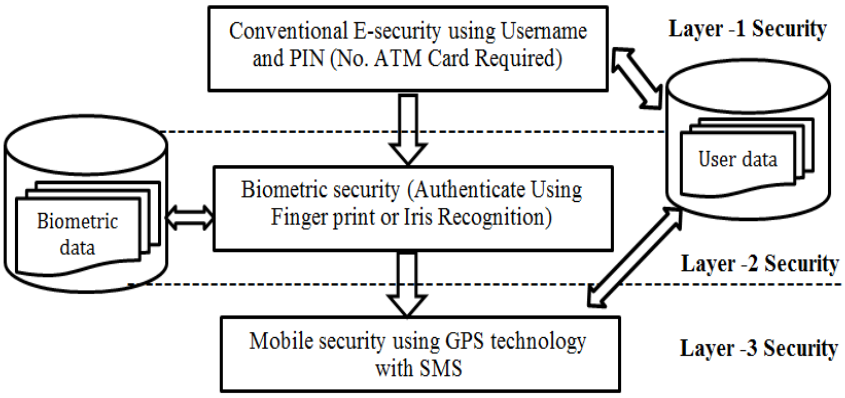

Figure 1. Three Layer Security System Flow

4.1. Layer 1 Security

This is conventional system for authenticate user in online. Not only electronic transaction system, most of the system authenticates their user using a username and password. As a basic in this proposed algorithm 1st steps customer use ATM system by his/her user name and PIN. There is no need to convey any physical device like as ATM card. It's our main challenges that proposed system eliminate conventional ATM card. Customers get username and PIN when he/she open an account for transaction on any bank. PIN generation technique is system generate a PIN and sent it to corresponding customer mobile. Customer can change PIN by login into system. When customer provide username and PIN in ATM system it authenticate user from user information data table from bank server. If authenticate It allows customer to proceed layer 2 security otherwise it provides 5 times resubmit username and PIN. After trying 4 times, it's terminating the transaction and offline for a 30 minute for this user. In that time customer can't transaction from any ATM system. If essential cases customer need to contact on bank physically.

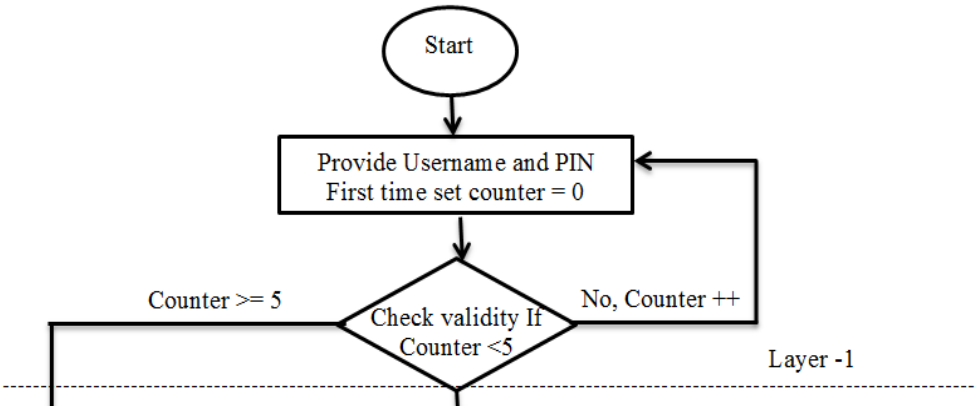

Figure 2. Layer 1 Security System Flow

4.2. 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 [5]. 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 [6-7].

In banking system Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications [8]. 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 (Figure 3).

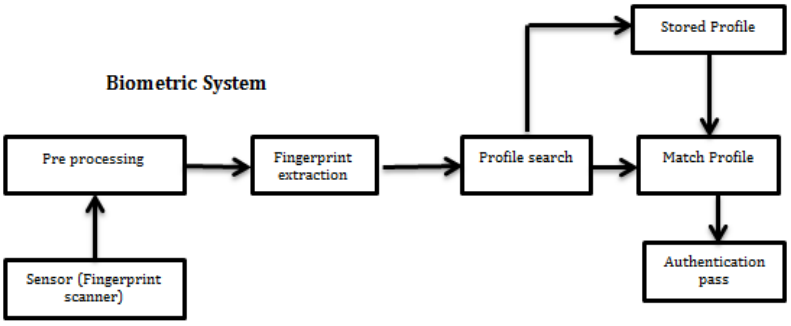

Figure 3. Biometric Security

A basic biometric authentication system consists of six main components [8]. 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. [9-10] 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 [11]. 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. Same as layer 1 security it off-line for 30 min if customer accede trying limit. The whole system is shown in Figure 5. If authentication passes then it goes to layer 3 security system.

4.3. 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

4.3.1. 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.

4.3.2. 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. The full work flow for this system is shown in Figure 4.

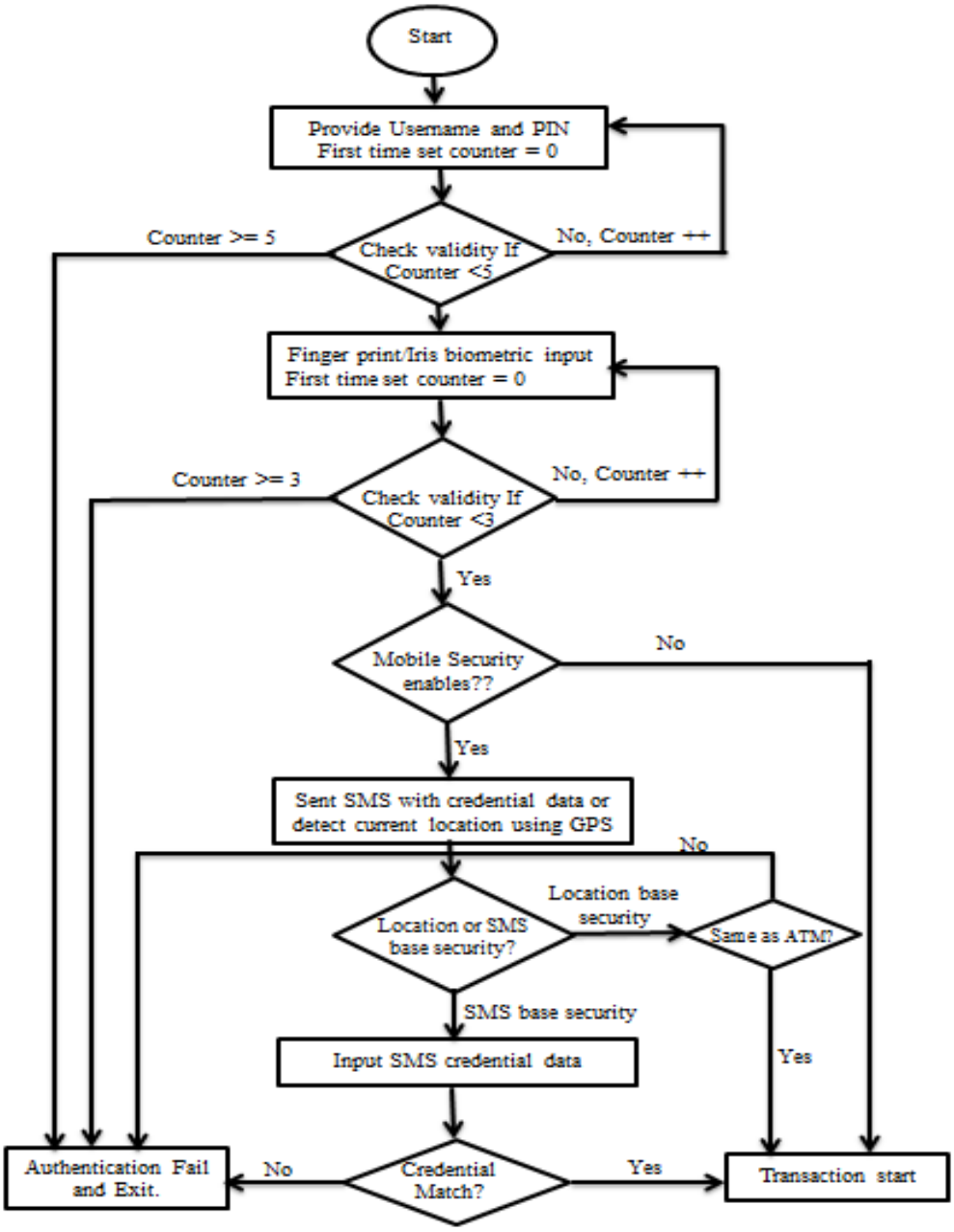

Figure 4. A Scalable Electronic Transaction System with 3 Layer Security

5. Result Analysis

This system contains the following infrastructure:

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

For the first time, user needs to open account at bank for money transaction. Bank store both personal information with biometric data and financial information. If user has account on bank then he/she can be transaction from ATM. Now user goes to ATM and start accessing his/her account by passing 3 layer securities. Firstly provide username and PIN. Figure 5 shows the user interface for 1st layer authentication system. If matches provide information then goes to second layer.

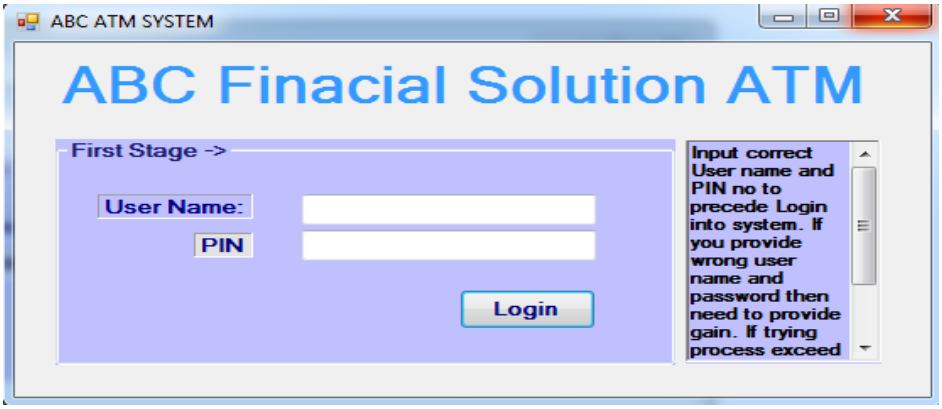

Figure 5. User Interface of First Layer Authentication System

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.

Figure 6. Fingerprint Authentication

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.

Figure 7. User Interface after Passing Second Layer Authentication

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.

If Mobile messaging system enables then system send a message to customer with a credential data (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.

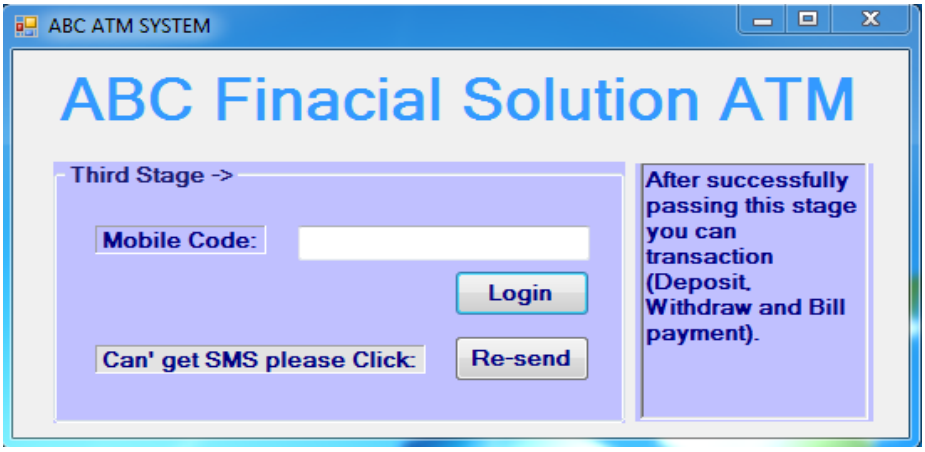

Figure 8. User Interface of SMS based Authentication

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 10.

Figure 9. User Interface of Transaction Main Menu

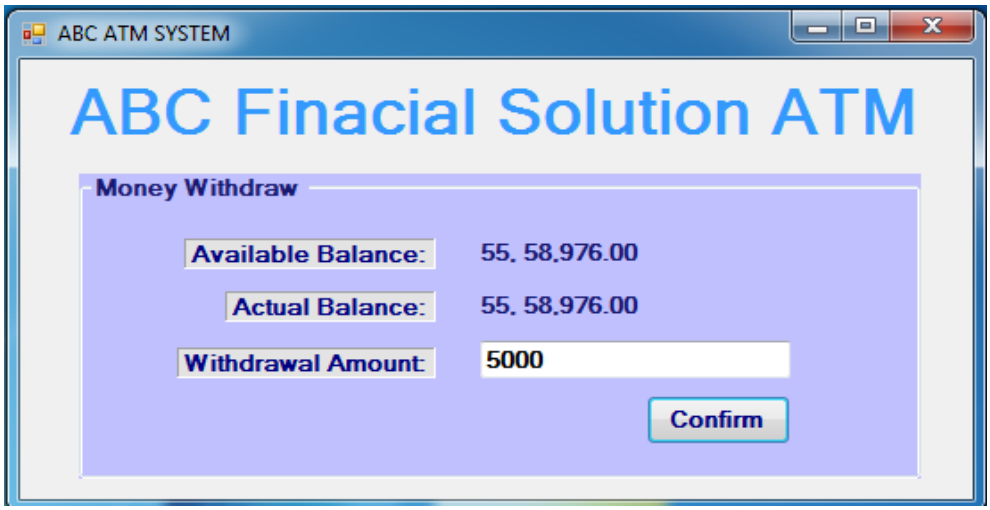

Figure 10. Money Withdraw Window

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.

6. Conclusion

Here we have defined a procedure to ensuring high label security in electronic transaction format ATM system. IT's ensure 100% security on authenticate access and preventing from any fraud. It's comfortable to all level of user. These eliminate conventional system to caring an ATM card for transaction and provide no card solution for transaction. Hope this will be most promising technology at electronic money transaction. I have also work on further security at transaction time and universal money transaction. My future plan in this regards is give the complete solution in money transaction all level of financial operation.

References

[1] N. Selvaraj and G. Sekar, "A method to improve the security level of ATM banking systems using AES algorithm", International Journal of Computer Applications (0975-8887), vol. 3, no. 6, **(2010)** June.
[2] http://en.wikipedia.org/wiki/Electronic_money, last access, **(2015)** January.
[3] T. C. Glaessner, T. Kellermann and V. McNevin, "Electronic Security: Risk Mitigation in Financial Transactions: Public Policy Issues", World Bank Publications, Electronic security systems, **(2002)**, pp. 3-5.
[4] W. W. N. Wan, C. L. Luk and C. W. C. Chow, "Customers Adoption of Banking Channels", Hong K34rong, International Journal of Bank Marketing, vol. 23, no. 3, **(2005)**, pp. 255-272.
[5] B. Richard and M. Alemayehu, "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons", Journal of Internet Banking and Commerce, vol. 11, no. 2, **(2006)**.
[6] N. K. Ratha, J. H. Connell and R. M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems", IBM Systems Journal, vol. 40, no. 3, **(2001)**, pp. 614-634.
[7] J. Yang, N. Xiong, A. V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon, S. Xie and Y. Yang, "A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications", IEEE Systems Journal, **(2011)**.
[8] 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.
[9] L. O'Gorman, "Overview of fingerprint verification technologies", Elsevier Information Security Technical Report, vol. 3, no. 1, **(1998)**.

[10] G. B. Iwasokun, O. C. Akinyokun, B. K. Alese and O. Olabode, "Fingerprint Image enhancement: Segmentation to thinning", International Journal of Advanced Computer Science and Applications, vol. 3, no. 1, **(2012)**, pp. 15-24.
[11] Facial Verification Technology Use in ATM Transactions- Aru, Okereke, Eze, Ihekweaba Gozie.

Author

Md. Syeful Islam, he obtained his B.Sc. and M.Sc. in Computer Science and Engineering from Jahangirnagar University, Dhaka, Bangladesh in 2010 and 2011 respectively. He is now working as a Senior Software Engineer at Samsung R&D Institute Bangladesh. Previously he worked as a software consultant in the Micro-Finance solutions Department of Southtech Ltd. in Dhaka, Bangladesh. His research interests are in Natural Language processing, AI, embedded computer systems and sensor networks, distributed Computing and big data analysis.