A Model for Transaction Authentication In Internet Banking

Mohamed A. Belal [1], **Sherif Kholeif** [2] , **Hytham Mahmoud Mohamed** [3]

[1]Department of Computer Science, Faculty of Computers and Information
Helwan University, Cairo, Egypt.

[2]Department of Information Systems, Faculty of Computers and Information
Helwan University, Cairo, Egypt.

[3]Academy of Scientific Research and Technology Egyptian Patent Office, Cairo, Egypt

dr.mohamedbelal@gmail.com , sherifkholeif@yahoo.com, hytham.mahmoud@gmail.com

Abstract

There are a continuously growing number of customers using Internet banking because of its convenience. Banks also encourage their customers to use Internet banking since it can lower banks' costs. Online systems which provide banking services need to offer strong security because of the confidential information involved, as well as attacks against Internet banking [1]. The Internet banking system, as a client server system, consists of three layers; user terminal, communications channel, and the Internet banking server. Security of the Internet banking system include providing a secure communications channel, preventing and detecting attacks against the Internet banking server, and authenticating the user terminal. Several methods are used to provide security for each layer. The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of the communication channel. Installing firewall and antivirus is commonly-used for protecting the Internet banking server. The proposed method provided in this research is concerned with transaction authentication. Transaction authentication means that individual transactions within the same session are authenticated. This method builds mainly on the user's previous transaction behavior. There is no need for using additional hardware. The user does not need to install additional software on his/her terminal. No training is required to be given for users to apply this method. A Prototype of the proposed method had been developed. A number of experiments had been performed to demonstrate the effect of the proposed method. Results of these experiments are used also to show the efficiency of the proposed method and explain the factors effect in the proposed method efficiency.

1. Introduction

The Internet plays a key role in changing how people interact with each other and how business is done today. As a result of the Internet, electronic commerce has emerged, allowing businesses to interact more effectively with their customers and with other corporations inside and outside their industries. The banking industry is considered one of these industries that use this new communication channel to reach their customers. Customers' demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges are considered most important trends which are addressed by the electronic banking system.

Today, international trade has grown significantly. The Internet and other global online networks have created new commercial opportunities for networked commerce. They offer the possibility of 'open systems' payment and settlement systems. The new payment and settlement systems operate in parallel to the existing traditional bank-based networks [2].

Internet-based electronic banking is also called online banking. There are a continuously growing number of customers using online banking. Most customers are using online banking because of its convenience. Online banking offers lower banks' costs. Banks encourage their customers to use online banking because of lower costs. Online systems which provide banking services need to offer strong security. Strong security is needed because of the confidential information involved, as well as attacks against online banking authentication mechanisms [1]. Online electronic banking systems give everybody the opportunity for easy access to their banking activities. These banking activities may include: retrieving an account balance, money transfers between a user's accounts, from a user's account to someone else's account, retrieving an account history. Some banks also allow services such as stock market transactions, and the submission of standardized accounting payment files for bank transfers to third parties [3].

The amount of money lost to online banking fraud is continuously increasing every year. According to financial fraud action UK, the amount of money lost on online banking in 2013 rose by 3%. Total losses on online banking increase by 48% between 2013 and 2014 [4].

A feature of the banking industry across the globe has been that it is increasingly becoming turbulent and competitive. While a few American banks (example Citibank) obtain more than half of their income from overseas operations, several international banks (e.g., Hong Kong Bank, Banque de Paris) have been entering the American market. Likewise, banks from Europe (e.g., London-based Standard Chartered Bank) have recently either taken control or bought over banks in Thailand, New Zealand, and Australia. To make matters more complex, a number of companies are entering the banking industry by offering financial products and services (e.g., Toyota's credit card, GM_s auto financing, and Merrill Lynch investments). This has given a myriad of options to customers in choosing banking services. Aided by technological developments, banks have responded to the challenge by adopting a strategy, which focuses on attempting to build customer satisfaction through providing better products and services and at the same time to reduce operating costs. Provision of e-banking services has been widely used, and an understanding of the customer preferences will have important implications for the banking sector [5].

From the above discussion the Internet bank security system is needed to improve.

There are several methods are used to provide the security to the user:-

- Shared secrets: in this method the user must answer one or more questions after typing username and password to login. These questions ask for specific knowledge of something about the customer. This method is called 'what you know' [6].
- What you have: this method is considered stronger than something a person knows. This method includes tokens such as USB device, grid card, smart card, or password generator.

- Crypto-Biometric authentication: in this method, cryptography and biometric techniques are fused together for user authentication. The fingerprint is considered the most common approach for this method. This method is called 'who you are' [7].
- Fraud detection using location information: this method is built mainly on finding the user location using his/her mobile. The user location is identified using the connection IP. The fraud detection is applied by comparing the two location of the user of they are the same or not. This method is called 'where you are' [8].

The previous methods have some weak points. All of them focus on the entity authentication. Entity authentication means that the user is authenticated when initiating a session with the bank. Some of them require users to install new software on their terminals by using a USB device, smart card, or Crypto-Biometric authentication; all of which means the need for extra devices, and drivers must be installed for these devices. Grid card and Crypto-Biometric authentication require user to get training on how applying these methods. Fraud detection using location information requires data from third party. Location of user is obtained by IP using IP location databases which are provided by many companies. Getting user location from mobile signal also need third party data [9]. Giving user hardware device like USB device or enforce user to buy device such as fingerprint reader increase the cost of the authentication method.

An authentication method is needed to be proposed. The proposed method should avoid the disadvantages which are found in the current authentication methods.

The proposed method concerns with transaction authentication. This method built mainly on the previous user's transaction behavior. There is no need for using additional hardware. The user doesn't need to install additional software on his/her terminal. No training is required to be given to users to apply this method.

2. Related Works

While something a person knows is the most widely used (including username and password, or shared secrets), some would argue that it is the least secure form of authentication as it can be easily compromised. The most common example of a shared secret is a password or PIN [10]. However, shared secrets also include questions that require specific knowledge of something about the customer. These are questions such as "Which address have you previously been associated with?" or "What is the name of the city you were born in?" Shared secrets are often selected during the initial enrollment process or can be added as an additional security process after enrollment [11]. Often times the customers can select from a list of questions provided by the authenticator or create their own question; the customer then provides the answer to the question. The shared secret can then be used as an additional authenticator when a customer is attempting access. The important thing to remember about shared secrets is that they should be something that is not normally used for account purposes and that only the customer would know [6].

Shared secrets have a low cost to the financial institution, since they can be simply added to the login page and only require the capture of a small amount of additional information [6]. Shared secrets are also very easy to use from a customer stand point. They can be added to a standard login with minimal impact to the customer's login process. They also require no additional hardware for the customer to buy or install [6].

A disadvantage of using shared secrets is that since they are stored by the financial institution, they can be easily compromised. Another disadvantage is customers may use the same shared secrets for several different financial institutions, which will increase the probability of the shared secret being compromised [6].

Something a person has can be used as a second factor in the authentication process; this factor represents some sort of physical device that a person has that may be used in a multi factor authentication protocol. This factor in authentication is usually considered stronger than something a person knows. This authentication factor can include tokens such as a USB device, a grid card, a smart card, or a password generator.

Tokens are a device that the person has in their possession, such as a USB token. The USB token device is a small piece of hardware usually around the size of a key. USB devices are more widely known for their use as memory sticks. Once the computer recognizes the device it can be used as an additional authenticator. Each device contains some sort of unique identifier. When a customer attempts to login to the secure area the system will first look for this device; if the system recognizes the device, the customer will be asked for their password. The use of the USB and password together represent multi factor authentication. Since USB devices are so small they are convenient for a customer to carry and use, and they are not easily tampered with or duplicated.

Grid cards allow additional authentication to be deployed to customers via a printed card. The printed card contains a variety of numbers, letters, and characters arranged in a grid. The grid card can be distributed to customers and they can be prompted to use the card at login. Customer would enter their username and password as well as characters from various random locations on the grid card. Grid cards provide strong security since they allow for different values to be entered during each login. This means that for an attacker to compromise the login credential he or she would have to obtain all of the information from the grid card. Grid cards are very cost effective, requiring only a small piece of paper to be sent to the customer. Reissues can be done quickly and with little cost.

Smart cards contain a microprocessor chip allowing the card to store and process data. Smart cards have multiple uses, but most importantly they have the ability to enhance the authentication process. To be read, smart cards require readers to be attached to a computer. The user would simply insert the card into the reader; the reader would validate the authenticity of the smart card, and if it validates, the user would be prompted to enter his or her password. Smart cards are a relatively simple and very secure form of authentication. They are extremely hard to duplicate and are tamper resistant. Smart cards can be provided to customers as part of their credit or debit card. Smart cards can store cryptographic keys. In this case, during the execution of a transaction, the user puts a chip card with a cryptographic key in the reader and enters a PIN code, i.e. When the card is used with a reader, the user must enter a PIN.[12] However, smart cards do have some drawbacks. Since the use of a reader is required, the customer will need to install additional hardware with the corresponding software/driver on their computer. This additional hardware can be intimidating and non user friendly, especially for those who are not technically savvy. Due to the need for additional software and the need to issue smart cards, this option can be difficult to justify as a form of additional authentication.

Password generating tokens provide a unique password to the customer at every login. These devices have a small screen that displays a password for around sixty seconds. The password changes at the end of the time frame. In a typical set up, the customer will be asked to enter their username and password, followed by the current code displayed on the token device. Password generating tokens provide excellent security due to the unpredictability and randomness they provide. Password generating tokens can be costly for an institution to deploy, since they must be purchased and distributed to the end user. In some cases, this cost could be absorbed by the customer; however, customers may not want to pay for this additional security. Some financial institutions may benefit from using this solution in a targeted approach. For instance, tokens could be deployed for a high end, high risk account, such as a brokerage account. Another drawback of using a password generating token is whenever customers want to access their accounts they must have their token available to them. This can become burdensome to the customer.

Cryptography and biometric techniques are fused together for person authentication to ameliorate the security level. The fingerprint template including singular points, frequency of ridges and minutiae are stored at the central banking server when enrollment. At the time of transaction fingerprint image is acquired using high resolution fingerprint scanner. The fingerprint image is enhanced and then encrypted. The encrypted image is transmitted to the central server via secured channel. At the banking terminal the image is decrypted [7].

Based on the decrypted image, minutiae extraction and matching are performed to verify the presented fingerprint image belongs to the claimed user. The authentication is signed if the minutiae matching are successful. Biometrics based authentication is a potential candidate to replace password-based authentication. Among all the biometrics, fingerprint based identification is one of the most mature and proven technique. Cryptography provides the necessary tools for accomplishing secure and authenticated transactions [13]. It not only protects the data from theft or alteration, but also can be used for user authentication. In a conventional cryptographic system, the user authentication is possession based. The weakness of such authentication systems is that it cannot assure the identity of the maker of a transaction; it can only identify the maker’s belongings (cards) or what he remembers (passwords, PINs etc.) Automatic biometric authentication is an emerging field to address this problem. Fingerprint authentication is the most popular method among biometric authentication.

Together with the development of biometric authentication, integrated biometrics and cryptosystems has also been addressed. Biometric authentication in this case is image based. For remote biometric authentication, the images need to be encrypted before transmitted. An embedded crypto-biometric authentication protocol is proposed. The fingerprint image acquired from the user is encrypted in the ATM or customer computer system terminal for authentication. The encrypted image is then transmitted over the secured channel to the central banking terminal. In the banking terminal fingerprint image is decrypted. The decrypted image is compared with the fingerprint templates. The authentication is valid if the minutiae matching are successful [14].

But there is a new method based on “Where you are” [8] type of authentication method, although very simple but promising, is proposed to identify potential frauds. This technique exploits the fact that almost every bank customer possesses a mobile phone.
Location of the customer is identified in two different ways: -

1. First approach identifies the customer location using customer computer system IP.
2. Second approach exploits the fact that almost all the online banking and card users own some kind of mobile phone. Mobile phone may be a smart phone, personal digital assistant (PDA) or a simple cellular phone. These mobile devices are used to identify present location of customer.

This type of authentication method is applied in three steps. The first step is to define IP Geo-Location. Geo-location technology provides the absolute geographic location by IP address of the computer system from which the transaction is made in real-time. By using the IP location database, location of the customer is known after the IP address is transformed into physical location. There are a number of free and paid subscription geo-location databases, ranging from country level to state or city - including ZIP/post code level - each with varying claims of accuracy. Some services that make use of IP location database are available online provided by companies [9].

The second step is to define Mobile Phone Location. Location of the user is identified using mobile phone. Three types of connection can be used to identify the location of mobile device:

- Global Positioning System (GPS),
- Wi-Fi triangulation and
- Cellular triangulation.

All the personal digital assistants (PDA) and smart phones support GPS and Wi-Fi. A GPS receiver uses information transmitted by three or four satellites which continuously transmit their orbital position and the time of transmission. The receiver uses the messages it receives to determine the transit time of each message and computes the distance to each satellite. These distances along with the satellites' locations are used to compute the position of the receiver [15]. There have been several companies like Skyhook Wireless [16] that offer Wireless Positioning Services that uses signal strength from various Wi-Fi hotspots to access a database of known locations of access points. Wi-Fi triangulation can give better results than GPS in urban areas where GPS signals find it difficult to penetrate into high buildings. For simple cellular phones, several techniques are available that use received signal strength (RSS) from the mobile phone [17]. These techniques exploit the fact that a mobile phone always communicates wirelessly with one of the closest base stations. Any one of the above method can be used to find the location depending on the type of mobile phone. GPS can be combined with Wi-Fi or cellular triangulation to achieve more accurate results in urban areas.
The final step is to Compare of Both Locations. Both of the user locations are compared and accordingly actions may be taken. If both locations are same then user is authenticated. Otherwise, security risk on the basis of difference between both locations is calculated. On the basis of security risk calculated, user may be abandoned or other security measures may be taken to authenticate the user. Accuracy of the proposed location based authentication system depends on the level of location details that is found using IP geo-location and mobile phone. Mobile phone with GPS can provide exact location in the range of 10 meters. Wi-Fi and cellular signals can also provide good location within the range of 100 meters in urban areas using triangulation of multiple receivers (access points or base stations). It may not always be possible to locate the user computer system exactly using its IP address. Sometimes it may provide location details up to city level. So it is necessary to define the level of sameness of the two obtained locations. Depending upon the level of sameness security risk associated can

be calculated. A simple location based authentication method is proposed for banking environment that utilizes user computer system IP and mobile phone. The authentication process can be used for online banking, credit and debit card processing where a computer system is being used. This system cannot be used in circumstances where user uses his PDA or smart phone for banking transactions because two different locations cannot be obtained then.

3. Proposed Model

The proposed method cannot be considered a standalone authentication method, but it is used to improve the security of current methods. It can be called "What you do". It gains the customer's behavior according to the previous transaction and verifies the coming transaction according to the customer's behavior. The Internet banking application is based on 3-tiered model.

1. Client: There will be two clients for the application. One will be a web-based user-friendly client called bank customers. The other will be for administration purposes.
2. Application Server: It takes care of the server script, takes care of ODBC (Open Database Connectivity) driver and checks for the ODBC connectivity for mapping to the database in Order to fulfill client and administrator's request.
3. Database:
   i. Bank Database stores actual customer's details information and bank data.
   ii. Customer History Database stores customer's history of previous transactions.

The proposed data flow model is based on these major steps as following:

- ***Extract customer behavior:*** In this step we get the customer previous transactions.
- ***Save customer behavior:*** In this step we create database to hold the customer behavior information which we obtain from the previous step.
- ***Verify the customer validation:*** This is the most important step. When the customer tries to make new transaction, we check new transaction to the previous customer behavior. If the new transaction is associated to the previous customer behavior then the customer is valid. If the new transaction is not associated to the previous customer behavior then the customer may be not valid.
- ***Add new customer transaction:*** If the new transaction is not associated to the previous customer behavior, the bank server sends an authentication key to customer via email or SMS according to bank system policy. If the customer enter the same authentication key, server complete the transaction and add it to the customer behavior database. But if the customer enters different authentication key, then this is not valid customer and the system cancel the transaction, changes the customer password and sends the new password to customer.

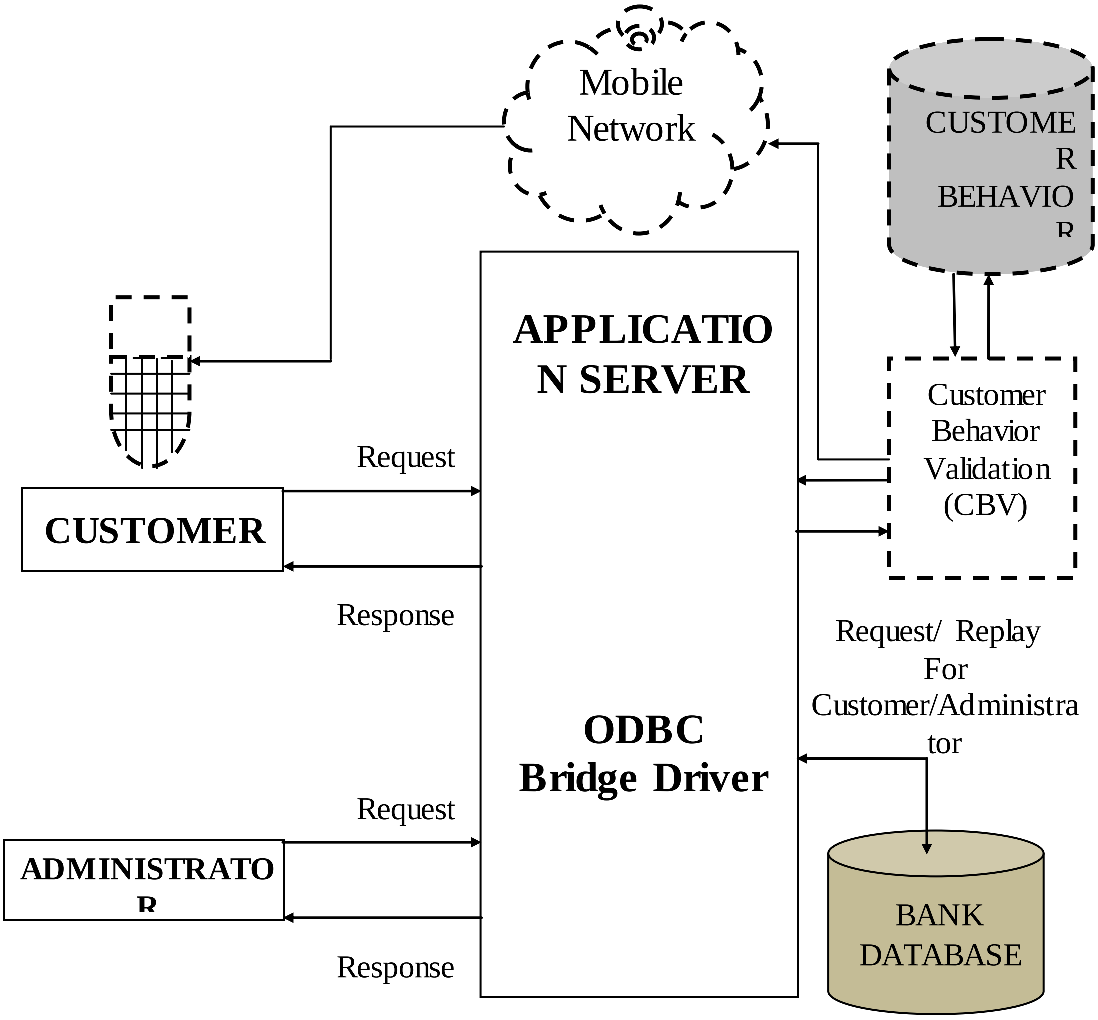

Figure 1: Architecture for Proposed Model

The proposed data flow model is based on these major steps as following:

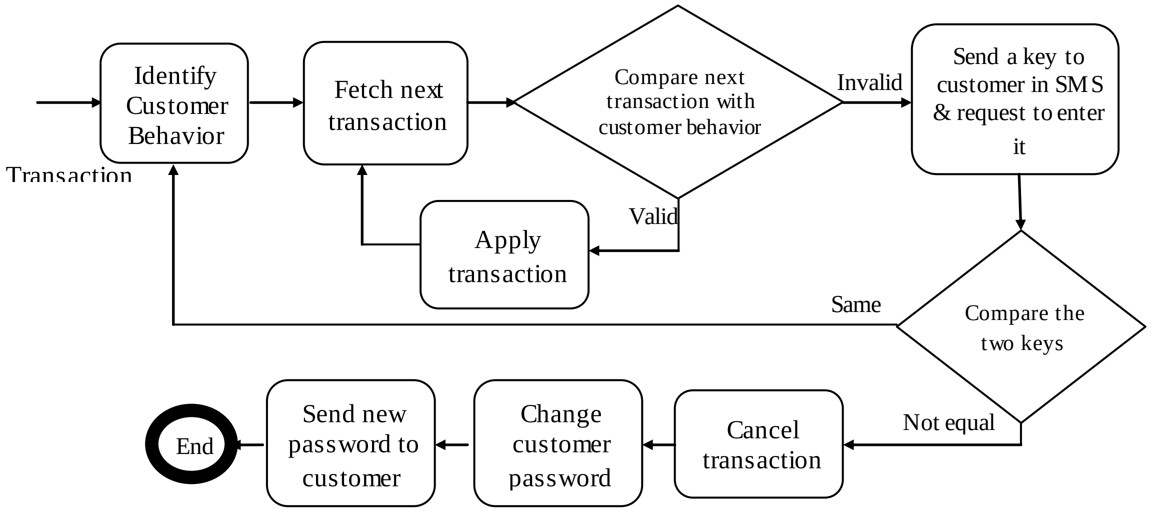
Transaction
Identify Customer Behavior
Fetch next transaction
Compare next transaction with customer behavior
Invalid
Send a key to customer in SMS & request to enter it
Valid
Apply transaction
Same
Compare the two keys
Not equal
Cancel transaction
Change customer password
Send new password to customer
End

Figure 2: Data Flow Diagram for Proposed Model

4. Implementation

The focus will be on one major transaction in the proposed model, funds transfer.

The following technologies are used to develop the proposed model:-

1. Active Server Page (ASP.Net).
2. Database (MS-SQL Server2008).
3. Internet Information Services (IIS7).

5. Results

The efficiency of the proposed model is tested depending on the changing in two factors. The efficiency is first tested according to the changing in number of available accounts, which the user can transfer to them. The changing in the number of previous user's transactions is then tested.

$$\mathit{The\ efficiecy} = \frac{\text{Total of detection fraud transfer number}}{\text{Total of trying fraud transfer number}} * 100$$

Because real bank data is secured with no clearance granted to the authors, it was deemed necessary a simulation for an online bank system be created to test the proposed model. It was implemented in three phases: researching and analyzing the online banking system data structure [18], designing and building the database using MS-SQL, and implementing the program using ASP.Net language. The values within the customers' accounts are generated randomly using 'RAND ()' function which is provided by MS-SQL. In other words, for each simulated account transactions were randomly generated to be used as customer transaction history. Ten different persons take different numbers of the simulated usernames and passwords and try to make fraud transactions. In other words, each of the ten persons chooses a randomly different number of accounts data (username and password) and tries to make ten fraudulent transfers to the available accounts. The account which the person tries to transfer from or to is selected by the person from the available total pool of simulated accounts.

The simulation for online bank system is used to test the efficiency of the model. The change of efficiency is also tested depended on the available accounts the user can transfer to it.

The next two tables show the result of the test when there is 20, and 100 account available.

Table 1: Efficiency Result when 20 Accounts Available

	Available Account	Previous Transactions	Trying Fraud Transfer Number	Detection Fraud Transfer Number
Person1	20	10	10	5
Person2	20	10	10	8
Person3	20	10	10	6
Person4	20	10	10	4
Person5	20	10	10	7
Person6	20	10	10	4
Person7	20	10	10	4
Person8	20	10	10	6
Person9	20	10	10	6
Person10	20	10	10	4
Total			100	54

From the previous table the efficiency = $\frac{54}{100} * 100 = 54\%$

Table 2: Efficiency Result when 100 Accounts Available

	Available Account	Previous Transactions	Trying Fraud Transfer Number	Detection Fraud Transfer Number
Person1	100	10	10	10
Person2	100	10	10	9
Person3	100	10	10	10
Person4	100	10	10	9
Person5	100	10	10	9
Person6	100	10	10	8
Person7	100	10	10	10
Person8	100	10	10	9
Person9	100	10	10	9
Person10	100	10	10	9
Total			100	92

From the previous table we can say that: efficiency = $\frac{92}{100} * 100 = 92\%$

Thousand customers' accounts are created to test the efficiency of the model. The change of efficiency is also tested depended on the previous user's transaction behavior.
The next two tables show the result of the test when there are 100, and 900 previous user's transactions.

Table 3 Efficiency Result when Customer has 100 previous transaction

	Available Account	Previous Transactions	Trying Fraud Transfer Number	Detection Fraud Transfer Number
Person1	1000	100	10	9
Person2	1000	100	10	9
Person3	1000	100	10	10
Person4	1000	100	10	9
Person5	1000	100	10	10
Person6	1000	100	10	8
Person7	1000	100	10	9
Person8	1000	100	10	10
Person9	1000	100	10	10
Person10	1000	100	10	9
Total			100	93

From the previous table we can say that: efficiency = $\frac{93}{100} * 100 = 93\%$

Table 4 Efficiency Result when Customer has 900 previous transaction

	Available Account	Previous Transactions	Trying Fraud Transfer Number	Detection Fraud Transfer Number
Person1	1000	900	10	1
Person2	1000	900	10	4
Person3	1000	900	10	5
Person4	1000	900	10	2
Person5	1000	900	10	6
Person6	1000	900	10	6
Person7	1000	900	10	6
Person8	1000	900	10	6
Person9	1000	900	10	4
Person10	1000	900	10	4
Total			100	44

From the previous table we can say that: efficiency = $\frac{44}{100} * 100 = 44\%$

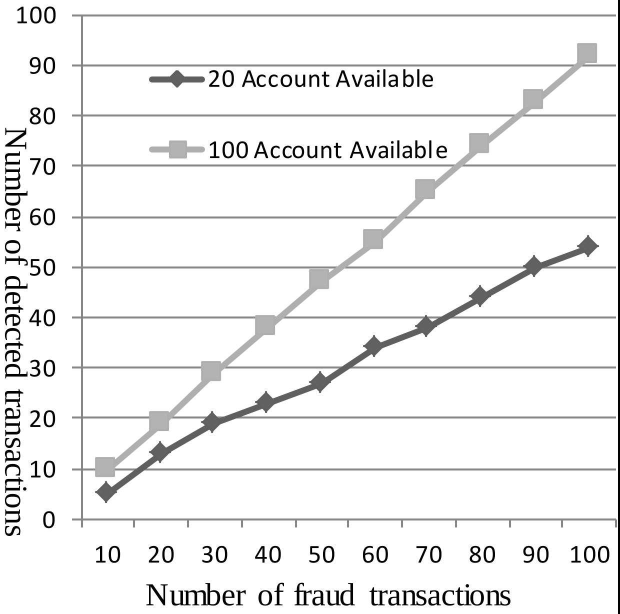

Figure 3 Efficiency According to Available Accounts

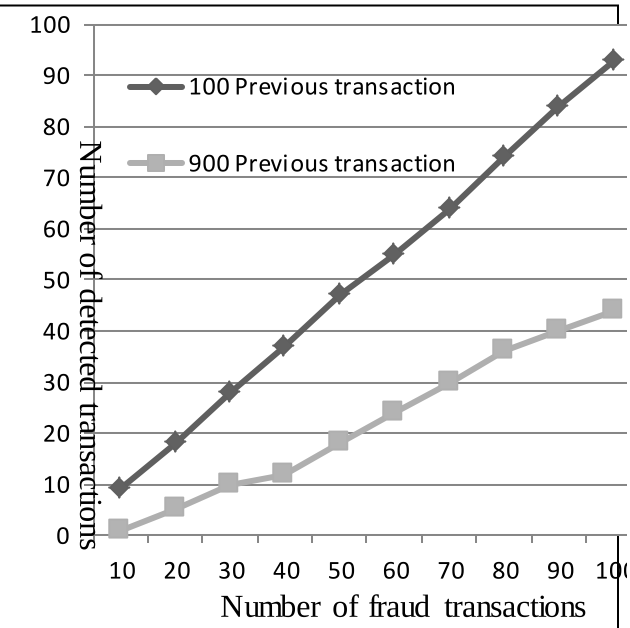

Figure 4 Efficiency According to Previous Transactions

6. Conclusion

By studying the result of the prototype, it is found that the worst efficiency for this proposed method is 44 percentages of fraud transactions are detected. The efficiency of this method is reach to 93 percentages of fraud transactions are detected. The efficiency of the proposed method depends on two factors the accounts available to transfer to (recipient accounts), and the number of previous user transactions. As the results show increasing the number of available recipient accounts makes this method more efficient. Increasing the number of users' previous transactions makes this method less efficient.

References

[1]. Secure Internet-banking. A. Hiltgen, T. Kramp, T. Weigold. 2006.

[2]. Electronic Banking Secuirty-Issues And Challenges. Raksha Chouhan, Dr. Vijay Singh Rathor. May, 2011. ISSN- 0974-2832.

[3]. On the Security of Today's Online Electronic Banking Systems. Joris Claessens, Valentin Dem, Danny De Cock, Bart Preneel and Joos Vandewalle. s.l. : Elsevier Science Ltd, 2002, Vol. 21.

[4]. Financial Fraud Action UK Report. http://www.financialfraudaction.org.uk/download.asp?file=2980. [Online] 2015.

[5]. E-banking and customer preferences in Malaysia: An empirical investigation. M. Sadiq Sohail, Balachandran Shanmugham. 2002.

[6]. Enhanced Authentication In Online Banking. Gregory D. Williamson, GE Money – America's. 2, s.l. : Journal of Economic Crime Management, 2006, Vol. 4.

[7]. A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm. N.Selvaraju, G.Sekar. s.l. : International Journal of Computer Applications (0975 – 8887), June 2010.

[8]. Real Time Online Banking Fraud Detection Using Location Information. Nadeem Akhtar, Farid ul Haq. Aligarh, India : s.n., 2011.

[9]. http://www.maxmind.com. [Online]

[10]. Authentication in an Internet Banking Environment. Council, Federal Financial Institutions Examination. October, 2005.

[11]. Customer Perspectives on Identity Theft and Phishing. s.l. : Entrust Internet Security Survey, 2005.

[12]. Electronic Business 2nd Part. Parusheva, S. et al, Software Development Management. Publishing house, "Science and Economics", University of Economics – Varna, 2015, p. 56.

[13]. Biometric cryptosystems: Issue and challenges. U.Uludag, S.Pankanti, S.Prabhakar andA. K.Jain. s.l. : Proceedings of the IEEE, vol.92, no.6,, 2004.

[14]. A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm. N.Selvaraju, G.Sekar. s.l. : International Journal of Computer Applications, June 2010, Vol. 3.

[15]. Continuous Navigation Combining GPS with Sensor-Based Dead Reckoning. GPS World. Zur Bonsen, G., Ammann, D., Ammann, M., Favey, E., Flammant, P. (April 01, 2005).

[16]. http://www.skyhookwireless.com. [Online]

[17]. Location Based Services for Mobiles: Technologies and Standards. Wang, Suman Kumar Mishra, Ajay Pratap. Beijing, China : IEEE International Conference on Communication (ICC), 2008.

[18]. Uml Modeling for Online Banking System Using Object Oriented Database. Harsh Dev, S., Min, J., Yi, B.K. International Journal of Computer Engineering & Technology (IJCET), 2012.