Promote Mobile Banking Services by using National Smart Card Capabilities and NFC Technology

Reza Vahedi*
Department of IT Management, Electronic Branch, Islamic Azad University, Tehran, Iran
it.vahedi@yahoo.com
Farhad Hosseinzadeh Lotfi
Department of Mathematics,Science and Research Branch, Islamic Azad University, Tehran, Iran
farhad@hosseinzadeh.ir
Seyed Esmaeial Najafi
Department of Industrial Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
najafiisis@yahoo.com

Received: 06/Jun/2016 Revised: 03/Aug/2016 Accepted: 13/Aug/2016

Abstract

By the mobile banking system and install an application on the mobile phone can be done without visiting the bank and at any hour of the day, get some banking operations such as account balance, transfer funds and pay bills did limited. The second password bank account card, the only security facility predicted for use mobile banking systems and financial transactions. That this alone cannot create reasonable security and the reason for greater protection and prevent the theft and misuse of citizens' bank accounts is provide banking services by the service limits. That by using NFC (Near Field Communication) technology can identity and biometric information and Key pair stored on the smart card chip be exchanged with mobile phone and mobile banking system. And possibility of identification and authentication and also a digital signature created documents. And thus to enhance the security and promote mobile banking services. This research, the application and tool library studies and the opinion of seminary experts of information technology and electronic banking and analysis method Dematel is examined. And aim to investigate possibility Promote mobile banking services by using national smart card capabilities and NFC technology to overcome obstacles and risks that are mentioned above. Obtained Results, confirmed the hypothesis of the research and show that by implementing the so-called solutions in the banking system of Iran.

Keywords: NFC Technology; National Smart Card; Mobile Banking; Identity; Security.

1. Introduction

Today, by the mobile banking system and install an application on the mobile phone can be done without visiting the bank and at any hour of the day, get some banking operations such as account balance, transfer funds and pay bills did limited [1]. The second password bank account card, the only security facility predicted for use mobile banking systems and financial transactions. That this alone cannot create reasonable security and the reason for greater protection and prevent the theft and misuse of citizens' bank accounts is provide banking services by the service limits.

With the expanding use of smart phones and add NFC technology to this type of phones Applications and new capabilities in the tech world has been created That Comfort and increase the speed and security of different activities, such as Share files, used in opening and closing the doors locked, read information NFC tags installed on the books in the library, etc. [2].

The purpose of this research, exploring the possibility of promoting mobile banking services by using national smart card capabilities and NFC that is a new technology [3,4]. That this goal is by inserting the national smart card alongside mobile and Creation wireless communicate between them by the NFC technology for exchange information stored in the national smart card chip (Identity information, biometrics and digital signing keys) with the mobile banking system, it is possible [5]. And increase the level of security and thus enabling the development and promoting mobile services offered by banks.

1.1 History and Research Literature

In this section an overview of the history and technology concepts NFC, national smart card, mobile banking as well as the dematel method will have.

1.1.1 National Smart Card

National smart identity card (e_ID Card): The New Generation card having an electronic chip that can be programmed like a computer and have the memory, processor, operating system and application installation are applets. Issued by the organization for Civil registration and containing identity information and biometric (fingerprints and facial image) with the possibility of issuing identity certificates, digital signatures and authentication biometric (MOC) to identify and authenticate citizens [6,7].

* Corresponding Author

Smart cards can be either contact or contactless smart card. Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations.

Smart card types

- Contact Memory Card
- Contact CPU Card
- Contact-less Memory Card
- Dual Interface CPU Card

In national smart ID card project uses of type dual Interface CPU card. In the type of cards implement contactless and contact interfaces on a single card with some shared storage and processing.

Design

A smart card may have the following generic characteristics:

- Similar dimensions to those of a credit card. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimeters (3.370 in × 2.125 in). Another popular size is ID-000 which is nominally 25 by 15 millimeters (0.984 in × 0.591 in) (commonly used in SIM cards). Both are 0.76 millimeters (0.030 in) thick.
- Contains a tamper-resistant security system (for example a secure cryptoprocessor and a secure file system) and provides security services (e.g., protects in-memory information).
- Managed by an administration system which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates.

Development of contactless systems

Contactless smart cards do not require physical contact between a card and reader. They are becoming more popular for payment and ticketing. Typical uses include mass transit and motorway tolls. Visa and MasterCard implemented a version deployed in 2004–2006 in the U.S. Most contactless fare collection systems are incompatible, though the MIFARE Standard card from NXP Semiconductors has a considerable market share in the US and Europe.

Smart cards are also being introduced for identification and entitlement by regional, national, and international organizations. These uses include citizen cards, drivers' licenses, and patient cards.

Smart card applications in finance:

Smart cards serve as credit or ATM cards, fuel cards, mobile phone SIMs, authorization cards for pay television, household utility pre-payment cards, high-security identification and access-control cards, and public transport and public phone payment cards.

Smart cards may also be used as electronic wallets. The smart card chip can be "loaded" with funds to pay parking meters, vending machines or merchants. Cryptographic protocols protect the exchange of money between the smart card and the machine. No connection to a bank is needed. The holder of the card may use it even if not the owner. Examples are Proton, Geldkarte, Chipknip and Moneo. The German Geldkarte is also used to validate customer age at vending machines for cigarettes.

Smart card applications in Identification

Smart-cards can authenticate identity. Sometimes they employ a public key infrastructure (PKI). The card stores an encrypted digital certificate issued from the PKI provider along with other relevant information. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC), and other cards used by other governments for their citizens. If they include biometric identification data, cards can provide superior two- or three-factor authentication.

Smart cards are not always privacy-enhancing, because the subject may carry incriminating information on the card. Contactless smart cards that can be read from within a wallet or even a garment simplify authentication; however, criminals may access data from these cards.

Cryptographic smart cards

Cryptographic smart cards are often used for single sign-on. Most advanced smart cards include specialized cryptographic hardware that uses algorithms such as RSA and Digital Signature Algorithm (DSA). Today's cryptographic smart cards generate key pairs on board, to avoid the risk from having more than one copy of the key (since by design there usually isn't a way to extract private keys from a smart card). Such smart cards are mainly used for digital signatures and secure identification.

The most common way to access cryptographic smart card functions on a computer is to use a vendor-provided PKCS#11 library. [citation needed] On Microsoft Windows the Cryptographic Service Provider (CSP) API is also supported.

The most widely used cryptographic algorithms in smart cards (excluding the GSM so-called "crypto algorithm") are Triple DES and RSA. The key set is usually loaded (DES) or generated (RSA) on the card at the personalization stage.

Some of these smart cards are also made to support the National Institute of Standards and Technology (NIST) standard for Personal Identity Verification, FIPS 201.

Advantages

The first main advantage of smart cards is their flexibility. Smart cards have multiple functions which simultaneously can be an ID, a credit card, a stored-value cash card, and a repository of personal information such as telephone numbers or medical history. The card can be easily replaced if lost, and, the requirement for a PIN (or other form of security) provides additional security from unauthorised access to information by others. At the first attempt to use it illegally, the card would be deactivated by the card reader itself.

The second main advantage is security. Smart cards can be electronic key rings, giving the bearer ability to access information and physical places without need for online connections. They are encryption devices, so that the user can encrypt and decrypt information without relying on unknown, and therefore potentially untrustworthy, appliances such as ATMs. Smart cards are

very flexible in providing authentication at different level of the bearer and the counterpart. Finally, with the information about the user that smart cards can provide to the other parties, they are useful devices for customizing products and services.

Other general benefits of smart cards are:

- Portability
- Increasing data storage capacity
- Reliability that is virtually unaffected by electrical and magnetic fields.

Smart cards and electronic commerce

Smart cards can be used in electronic commerce, over the Internet, though the business model used in current electronic commerce applications still cannot use the full potential of the electronic medium. An advantage of smart cards for electronic commerce is their use customize services. For example, in order for the service supplier to deliver the customized service, the user may need to provide each supplier with their profile, a boring and time-consuming activity. A smart card can contain a non-encrypted profile of the bearer, so that the user can get customized services even without previous contacts with the supplier [4,6,7].

1.1.2 Mobile Banking:

Mobile banking is a service provided by a bank or other financial institutionthat allows its customers to conduct a range of financial transactionsremotely using a mobile device such as a mobile phone or tablet, and using software, usually called an app, provided by the financial institution for the purpose. Mobile banking is usually available on a 24-hour basis. Some financial institutions have restrictions on which accounts may be accessed through mobile banking, as well as a limit on the amount that can be transacted.

The types of financial transactions which a customer may transact through mobile banking include obtaining account balances and list of latest transactions, electronic bill payments, and funds transfers between a customer's or another's accounts. Some also enable copies of statements to be downloaded and sometimes printed at the customer's premises; and some banks charge a fee for mailing hardcopies of bank statements.

From the bank's point of view, mobile banking reduces the cost of handling transactions by reducing the need for customers to visit a bank branch for non-cash withdrawal and deposit transactions. Transactions involving cash or documents (such as cheques) are not able to be handled using mobile banking, and a customer needs to visit an ATM or bank branch for cash withdrawals and cash or cheque deposits.

Mobile banking differs from mobile payments, which involves the use of a mobile device to pay for goods or services either at the point of sale or remotely, analogously to the use of a debit or credit card to effect an EFTPOS payment.

History

The earliest mobile banking services used SMS, a service known as SMS banking. With the introduction of smart phoneswith WAP support enabling the use of the mobile web in 1999, the first European banks started to offer mobile banking on this platform to their customers. Mobile banking has until recently (2010) most often been performed via SMS or the mobile web. Apple's initial success with iPhone and the rapid growth of phones based on Google's Android (operating system) have led to increasing use of special client programs, called apps, downloaded to the mobile device. With that said, advancements in web technologies such as HTML5, CSS3 and JavaScript have seen more banks launching mobile web based services to complement native applications. A recent study (May 2012) by Mapa Research suggests that over a third of banks have mobile device detection upon visiting the banks' main website. A number of things can happen on mobile detection such as redirecting to an app store, redirection to a mobile banking specific website or providing a menu of mobile banking options for the user to choose from.

A mobile banking conceptual

In one academic model, mobile banking is defined as:

Mobile Banking refers to provision and availment of banking- and financial services with the help of mobile telecommunication devices. The scope of offered services may include facilities to conduct bank and stock market transactions, to administer accounts and to access customised information.

According to this model mobile banking can be said to consist of three inter-related concepts:

- Mobile accounting
- Mobile brokerage
- Mobile financial information services

Most services in the categories designated accounting and brokerage are transaction-based. The non-transaction-based services of an informational nature are however essential for conducting transactions - for instance, balance inquiries might be needed before committing a money remittance. The accounting and brokerage services are therefore offered invariably in combination with information services. Information services, on the other hand, may be offered as an independent module. Mobile banking may also be used to help in business situations as well as financial.

Mobile banking services

Typical mobile banking services may include:

- Account - information
- Transaction
- Investments
- Support
- Content services

A report by the US Federal Reserve found that 21 percent of mobile phone owners had used mobile banking in the past 12 months.[5] Based on a survey conducted by Forrester, mobile banking will be attractive mainly to the

younger, more "tech-savvy" customer segment. A third of mobile phone users say that they may consider performing some kind of financial transaction through their mobile phone. But most of the users are interested in performing basic transactions such as querying for account balance and making bill payment.

Security

As with most internet- connected devices, as well as mobile-telephony devices, cybercrime rates are escalating year-on-year. The types of cybercrimes which may affect mobile-banking might range from unauthorized use while the owner is using the toilet, to remote-hacking, or even jamming or interference via the internet or telephone network data streams. In the banking world, currency rates may change by the millisecond.

Security of financial transactions, being executed from some remote location and transmission of financial information over the air, are the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the banks' IT departments.

The following aspects need to be addressed to offer a secure infrastructure for financial transaction over wireless network:

1. Physical part of the hand-held device. If the bank is offering smart-card based security, the physical security of the device is more important.
2. Security of any thick-client application running on the device. In case the device is stolen, the hacker should require at least an ID/Password to access the application.
3. Authentication of the device with service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions.
4. User ID / Password authentication of bank's customer.
5. Encryption of the data being transmitted over the air.
6. Encryption of the data that will be stored in device for later / off-line analysis by the customer.

One-time password (OTPs) are the latest tool used by financial and banking service providers in the fight against cyber fraud. [8] Instead of relying on traditional memorized passwords, OTPs are requested by consumers each time they want to perform transactions using the online or mobile banking interface. When the request is received the password is sent to the consumer's phone via SMS. The password is expired once it has been used or once its scheduled life-cycle has expired.

Because of the concerns made explicit above, it is extremely important that SMS gateway providers can provide a decent quality of service for banks and financial institutions in regards to SMS services. Therefore, the provision of service level agreements (SLAs) is a requirement for this industry; it is necessary to give the bank customer delivery guarantees of all messages, as well as measurements on the speed of delivery, throughput, etc. SLAs give the service parameters in which a messaging solution is guaranteed to perform.

Mobile banking in the world

Mobile banking is used in many parts of the world with little or no infrastructure, especially remote and rural areas. This aspect of **mobile commerce** is also popular in countries where most of their population is **unbanked**. In most of these places, banks can only be found in big cities, and customers have to travel hundreds of miles to the nearest bank.

In Iran, banks such as Parsian, Tejarat, Pasargad Bank, Mellat, Saderat, Sepah, Edbi, and Bank melli offer the service [1].

1.1.3 NFC Technology

Near Field Communication or NFC technology is a short-range wireless encrypted communication at a distance of 4 cm or less that in the frequency band of 13.56 MHz ability to exchange data with speed 424 KB / s (on average). NFC can be with contactless smart cards ISO / IEC 1443 available as well as other devices equipped with the technology to easily communicate and exchange information with them. NFC specifically designed to work on mobile devices and has three general features' that make it transparent development process. In the first feature, this technology has the potential to be used instead of the existing contactless cards so much so that you can use exactly like cards available for micropayments. In the second feature, you can use this technology as a reader and RFID passive tags and use it in promotional interactivity. The third feature of this technology also this capability gives you that as a reader and sender used this feature and in a state person-to-person exchange of information between two powered device NFC to take advantage of it [2].

Applications

NFC allows one- and two-way communication between endpoints, suitable for many applications.

Commerce

NFC devices can be used in contactless payment systems, similar to those used in credit cards and electronic ticket smartcards and allow mobile payment to replace/supplement these systems.

In Android 4.4, Google introduced platform support for secure NFC-based transactions through Host Card Emulation (HCE), for payments, loyalty programs, card access, transit passes and other custom services. HCE allows any Android 4.4 app to emulate an NFC smart card, letting users initiate transactions with their device. Apps can use a new Reader Mode to act as readers for HCE cards and other NFC-based transactions.

On September 9, 2014, Apple announced support for NFC-powered transactions as part of Apple Pay. Apple stated that their approach to NFC payment is more secure because Apple Pay tokenizes its data to encrypt and protect it from unauthorized use.

Bootstrapping other connections

NFC offers a low-speed connection with simple setup that can be used to bootstrap more capable wireless connections. For example, Android Beam software uses NFC to enable pairing and establish a Bluetooth

connection when doing a file transfer and then disabling Bluetooth on both devices upon completion. Nokia, Samsung, BlackBerry and Sony have used NFC technology to pair Bluetooth headsets, media players and speakers with one tap. [citation needed] The same principle can be applied to the configuration of Wi-Fi networks. Samsung Galaxy devices have a feature named S-Beam—an extension of Android Beam that uses NFC (to share MAC Address and IP addresses) and then uses Wi-Fi Direct to share files and documents. The advantage of using Wi-Fi Direct over Bluetooth is that it permits much faster data transfers, running up to 300Mbit/s.

Social networking

NFC can be used for social networking, for sharing contacts, photos, videos or files and entering multiplayer mobile games.

Identity and access tokens

NFC-enabled devices can act as electronic identity documents and keycards.[53] NFC's short range and encryption support make it more suitable than less private RFID systems.

Smartphone automation and NFC tags

NFC-equipped smartphones can be paired with NFC Tags or stickers that can be programmed by NFC apps. These programs can allow a change of phone settings, texting, app launching, or command execution.

Such apps do not rely on a company or manufacturer, but can be utilized immediately with an NFC-equipped smartphone and an NFC tag.

The NFC Forum published the Signature Record Type Definition (RTD) 2.0 in 2015 to add integrity and authenticity for NFC Tags. This specification allows an NFC device to verify tag data and identify the tag author.

1.1.4 Dematel Technique

Dematel technique commonly used to investigate the very complex issues and apply for structuring a sequence of Supposed information. So that the intensity of relationship to be examined scoring, coupled with the importance of their Feedback to make search and accepts non-transferable relationships [8].

Dematel technique has two major functions:

1. Considering the mutual communication; advantage of this method compared to network analysis technique, clarity it to reflect mutual communication is among a wide range of components. So that specialists are able with greater mastery to express their opinions about the effects, the direction and severity of affective between the factors them.

2. Structuring the complex factors in groups of cause and effect. This case is one of the most important functions and one of the most important reasons for its frequent application in problem-solving processes. So that the classification of a wide range of complex factors in the form of cause-effect, the decision maker in better condition to understand the relationships. This results in recognizing the crucial status and role in the process of mutual effecting.

1.1.5 Research History

To some of the research on mobile banking, NFC and their applications and also the use of tools dematel for analyzing data in the studies, will be mentioned in table1.

Table 1. Research history

Year	Researcher	Work done	Ref. No
2015	Mohammadi S, Barkhordari Firouzabadi M	They offer a model for authentication and admission patient & payment of fees by health smart card, NFC and mobile payments	[9]
2013	Hosseinpour Soleymani A, Yousefi M	They assessed application and risk, mobile payment transactions by NFC technology	[10]
2014	Mohammadzadeh A, Ataei M, Salimi H	Identify and prioritize barriers the collected retarded banking debts using a combination model Dematel network and vikor	[11]
2013	Tabatabaei M, Hosseini S, Noori A	Identify and prioritize the criteria of quality services MCDM approach in the banking industry (by dematel technique)	[12]

2. Doing this Study Method and Tools for Data Collection and Analysis:

This research, using library studies and specialists, IT & electronic banking and interviews with them, possibility promoting mobile banking services using the capabilities of the national smart card and NFC technology review and after gathering the required information the mentioned method and criteria for specify and after preparing the appropriate paired comparisons questionnaire and complete it by the experts, analyzed the results using Dematel process.

3. Research Methodology

In figure 1 steps of this research are shown separately:

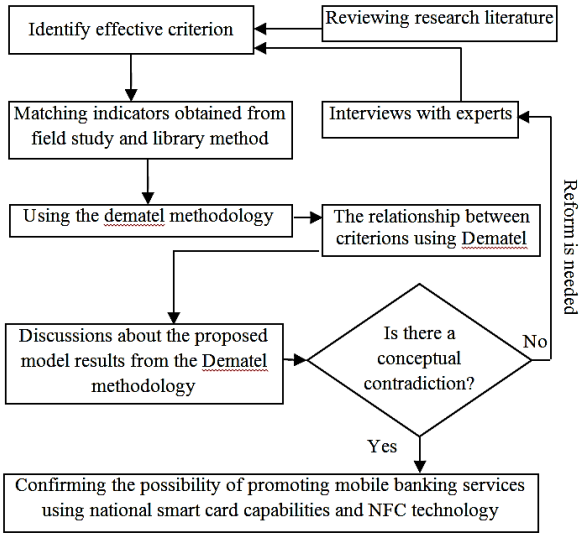

Fig 1. Research steps

3.1 Determine the effective criteria

According to the research literature and expert opinion, an effective criterion to achieve the research objectives within the framework of six criteria in table 2 was determined.

Table 2. Effective criteria

Proprietary word	Criteria	Definition
C_1	Identification	Identify the people, by self-expression profile and provide identification documents
C_2	Authentication	Proof of correctness, identity of people information that was given in Identification stage
C_3	Undeniable signature	Acceptance and approval documents, commitments and requests in electronic transactions so that there is no possibility of denial.
C_4	Security requirements	Protocols and security guidelines
C_5	Technical Requirements	Software and equipment, hardware and communication Infrastructure
C_6	Macro banking services	Main banking services such as account opening, apply for a loan, transfer too much money and...

Applicability and purpose of this study was determined as follows:

A (application): use of national smart card capabilities in mobile banking system by NFC technology

P (main purpose): promoting security and development services provided by mobile banking.

3.2 Analysis of relations among of criteria and create a total relation matrix using Dematel

The structure decision to confirm possibility promote mobile banking services by using national smart card capabilities and NFC technology were discussed and reviewed conforms to the figure 2, According to which and based on dematel methodology, domestic relationships are managed.

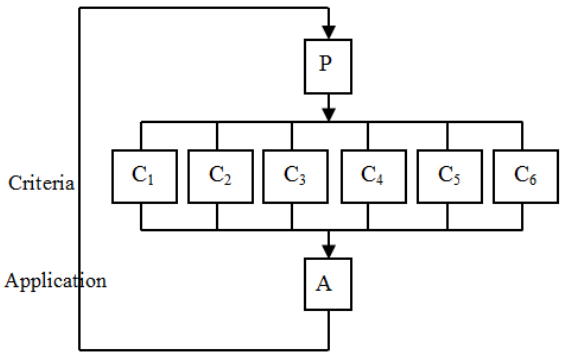

Fig. 2. Structure Design

To determine the relationship between effective criteria, dematel technique is used. This technique involves four main steps. In the first stage should be paired comparison matrix of criteria that were scored by experts and its numbers are ranging from 0 to 4, to be created. The number zero is showing that they are on each other ineffective and number 4 is representing the greatest impact. To review criteria, from the standpoint of five experts has been used that for the consideration of the opinion of all experts, according to formula 1 of them we the arithmetic mean.

$$Z = \frac{x^1+x^2+x^3+\cdots+x^p}{p} \quad (1)$$

P In this formula, the number of experts and x^1, x^2... x^p, respectively, are paired comparison matrix expert 1, expert 2 and expert p and for normalizing the matrix obtained from the formulas 2 and 3 is used.

$$H_{ij} = \frac{z_{ij}}{r} \quad (2)$$

That r is obtained from the following formula:

$$r = \max_{1\le i\le n}\left(\sum_{j=1}^{n} z_{ij}\right) \quad (3)$$

Table 3 shows the normalized matrix.

Table 3. Normalized matrix

	C_1	C_2	C_3	C_4	C_5	C_6
C_1	0.00	0.19	0.21	0.19	0.13	0.21
C_2	0.00	0.00	0.24	0.26	0.21	0.29
C_3	0.00	0.00	0.00	0.28	0.26	0.29
C_4	0.00	0.00	0.00	0.00	0.21	0.26
C_5	0.00	0.00	0.00	0.00	0.00	0.18
C_6	0.00	0.00	0.00	0.00	0.00	0.00

After calculating the above matrix, the total relation matrix is obtained according to the formula 4.

$$T = \lim_{k\to+\infty}\left(H^1 + H^2 + \cdots + H^k\right) = H \times (I - H)^{-1} \quad (4)$$

In this formula, *I* is the unit matrix.

Table 4 shows the T matrix.

Table 4. Total relation matrix

	C_1	C_2	C_3	C_4	C_5	C_6
C_1	0.00	0.19	0.25	0.31	0.30	0.47
C_2	0.00	0.00	0.24	0.33	0.34	0.51
C_3	0.00	0.00	0.00	0.28	0.32	0.42
C_4	0.00	0.00	0.00	0.00	0.21	0.30
C_5	0.00	0.00	0.00	0.00	0.00	0.18
C_6	0.00	0.00	0.00	0.00	0.00	0.00

The next step is to obtain the sum of rows and columns of the matrix T. The sum of rows and columns according to formulas 5 and 6 obtained.

$$(D)_{n\times 1} = \left[\sum_{j=1}^{n} T_{ij}\right]_{n\times 1} \quad (5)$$

$$(R)_{1\times n} = \left[\sum_{j=1}^{n} T_{ij}\right]_{1\times n} \quad (6)$$

That D and R are respectively matrix n × 1 and 1 × n.

Next, the importance of $(D_i + R_i)$ and the relationship between the criteria $(D_i\text{-}R_i)$ is determined. If $D_i\text{-}R_i>0$ is the

relevant criteria is effective and if D_i-R_i<0 is the relevant criteria is receptive effect. Table 5 D_i+R_i and D_i-R_i shows.

Table 5. The importance and effectiveness criteria

Criteria	$D_i + R_i$	$D_i - R_i$
Criterion 1	1.53	1.53
Criterion 2	1.60	1.22
Criterion 3	1.51	0.54
Criterion 4	1.43	-0.41
Criterion 5	1.34	-0.99
Criterion 6	1.88	-1.88

Chart 1 shows the importance and effectiveness between the criteria. The horizontal axis shows the importance of the criteria and the vertical axis shows the impact or receptive effect the criteria.

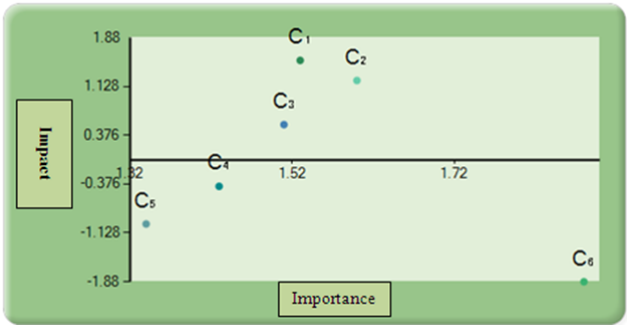

Chart 1. The relationships and the importance of criteria

According to the Chart 1, the criteria C_1 (identification), C_2 (authentication), C_3 (signature undeniable), effective criteria (cause) and the criteria C_4 (security requirements), C_5 (technical requirements), C_6 (macro banking services) as criteria affected (disabled), are introduced.

In the final step, according to negotiate with experts, threshold value in this study, average total numbers obtained from the matrix table of the total relationships (direct and indirect relationships) were considered. Therefore, this study is a threshold value equal 0.14.

On this basis and according to the results of total relation matrix, As shown in Figure 3, criterion C_1 to C_2, C_3, C_4, C_5, C_6 and criterion C_2 to C_3, C_4, C_5, C_6 and criterion C_3 to C_2, C_4, C_5, C_6 and criterion C_4 to C_5, C_6 and criterion C_5 to C_6 is affected. And to criterion C_6 (macro banking services) affect all other criteria. In other words criteria C_1 up to C_5 affecting the criterion C_6 (Macro Banking Services) is.

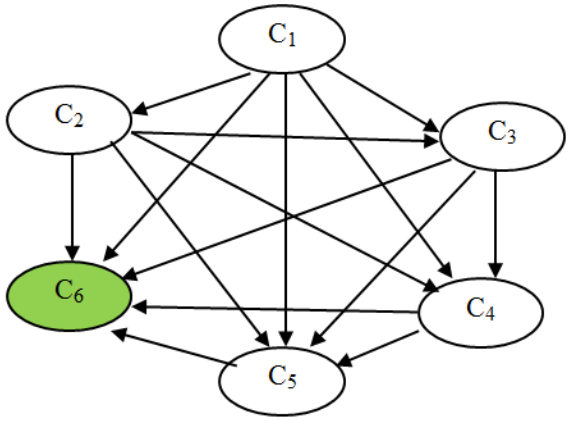

Fig. 3. Relationship between criteria

4. Conclusions

The aim of this study was to promote mobile banking services by using the capabilities of the National Smart Card and NFC technology. That's according to the research literature and expert opinion and the results of data analysis research by providing conditions (criteria C_1 to C_6) by inserting the national smart card alongside mobile and Creation wireless communicate between them by the NFC technology for exchange information stored in the national smart card chip (Identity information, biometrics and digital signing keys) with the mobile banking system, it is possible. And increase the level of security and thus enabling the development and promoting mobile services offered by banks.

4.1 Future research

It is suggested to the researchers that the use of the national smart ID card and NFC technology in the field of micro-payments, investigate.

References

[1] https://en.wikipedia.org/wiki/Mobile_banking
[2] https://en.wikipedia.org/wiki/Near_field_communication
[3] Project Management Office, National smart card applications, Tehran: NOCR, 2010, pp.5-45.
[4] Project Management Office, Some of the dimensions of a national smart card application, Tehran: NOCR, 2010, pp.12-67.
[5] A. Riyazi, National Smart Card (Secure, standards, biometrics), Tehran: Nass, 2009, pp.63-101.
[6] NOCR Education Center, The National Smart Card-structure and its role in e-government, Tehran: Institute of Danesh Parsiyan, 2011, pp.51-64.
[7] Project Management Office, National Smart Card Project for Metropolitan Architecture, Tehran: NOCR, 2010, pp.167-198.
[8] S. M. Arabi, and N. Azad, "The effects of the implementation of the ASYCUDA system in the country's business sector", Iranian journal of Trade Studies, Vol. 29, pp.137-165, 2003.

[9] M. Barkhordari Firouzabadi, and S. Mohammadi, "A Review and Proposal of a Model for Patient Authentication and NFC Mobile Payment with Smart Health Card", in 1st National E-Conference of Technology Developments on Electrical, Electoroncs and Computer Engineering, Iran, 2015.
[10] A. Hosseinpour Soleymani, and M. Yousefi," Introduction to NFC technology and its application in mobile payments", in the 1st Regional Conference on Information Technology, Iran, 2013.
[11] A. Mohammadzadeh, and M. Ataei, and H. Salimi, "Identifying and Prioritizing the Obstacles Leading to Bank Overdue, Using DEMATEL and VIKOR", Journal of Development Evolution Management, Vol.16, pp.15-26, 2014.
[12] M. Tabatabaei, and S, Hosseini, and A. Noori, " Identify and prioritize the criteria of quality services MCDM approach in the banking industry", in 9th International Conference on Industrial Engineering, Iran, 2013.

Reza Vahedi is a M.A graduate of Information Technology Management at Electronic Branch, Islamic Azad University. He got his B.Sc in Computer Engineering. His research interests include Business intelligence (BI), decision support system (DSS), Management Information System (MIS), software Engineering, Expert systems (ES), Data modeling And e-banking.

Farhad Hosseinzadeh Lotfi is a Ph.D graduate of Applied Mathematics (O. R.) at Science & Research Branch, Islamic Azad University, Tehran in 2000. He currently is a professor of Operation Research. His main research interests are in the fields of Operation Research, Data Envelopment Analysis (DEA) and Application of DEA in Banking. He has published more than 340 papers in various journals and conferences as well as 17 books.

Sayed Esmaeail Najafi is a Ph.D graduate of Industrial Engineering(System Management and efficiency) at Science and Research Branch, Islamic Azad University, Tehran in 2009. His research in the fields of Data Envelopment Analysis (DEA), organization Architecture and Decision Making Methods. He has published more than 31 papers in various journals and conferences as well as 5 books.