Analysis of Authentication Methods for Smartphone Banking Service using ANP

Keon Chul Park[1], Jae Woo Shin[1] and Bong Gyou Lee[1]
[1] Graduate School of Information, Yonsei University
Seoul, Korea
[e-mail: {parkkc, jaewoo.shin, bglee}@yonsei.ac.kr]
*Corresponding author: Bong Gyou Lee

Received April 6, 2014; revised June 7, 2014; accepted June 10, 2014; published June 27, 2014

Abstract

What is an ideal authentication method for smartphone banking services? And what are the critical elements to be considered when designing it? To provide valuable insight for these questions, this study investigates various authentication requirements to be considered in smartphone banking service with the aspect of security, convenience and cost. By applying Analytic Network Process (ANP), this study first analyzes priorities among the requirements and then draws an ideal authentication method for smartphone banking service. Moreover, a sensitivity analysis has been conducted by varying the relative importance of several requirements. The results from the judgment of 72 experts revealed that, although Korean government has obliged the use of Public Key certificate, OPT and biometric alternatives may prove to be more appropriate for the smartphone banking service. These results will contribute to the provision of more secured and convenient smartphone banking services.

Keywords: Authentication method, Smartphone banking service, Analytic Network Process, ActiveX, Public Key certificate

A preliminary version of this paper was presented at ICONI 2013 and was selected as an outstanding paper

http://dx.doi.org/10.3837/tiis.2014.06.016

1. Introduction

With the evolution of internet and mobile technologies, efforts have been made for the best practice of online and mobile service delivery in various industries and business sectors. Financial sector which traditionally had delivered various banking services through face-to-face channel has recognized the stream for the transition and has expanded its service to PC (e-Banking service) and mobile (m-Banking service). Moreover, as usage and distribution of smartphone have actively increased, application based m-Banking service (namely smartphone banking service) is gaining polpuarity thesedays. Fig. 1 shows the evolusion of banking service. As channels for banking service expand from bank windows(face-toface) to CD/ATM, tele banking, e-banking, m-banking and finnaly smartphone banking, the service has become more convinet as it provide automated, virtualized, anytime/anyplace and smart service. With increased accesibility and portability, customers can now use a variaty of banking services such as checking account, transfering fund, paying bill and many other services anytime, anyplace with the simple touch of their smartphone screen. More and more financial institutions are preparing to provide banking services through mobile channel. Recent study has revealed that 81 of the top 100 U.S. financial institutions already offer some form of mobile banking (in 2012) [1]. Moreover, in addition to offering access via smartphone and the mobile web, 26 banks have also launched an application optimized for tablets [1].

With the technical progress, the number of users and the amount of daily transaction via mobile channel has dramatically increased, and it is forecasted to grow even more [1, 2].

As shown in **Fig. 2**, mobile payment users in global would reach 616 million by 2016 with 582% increase from that of 2011. And as mobile banking service become more widely accepted by customers, the value of mobile payment transaction worldwide is forecasted to reach $447.9 billion with the 209.3 trillion use cases by 2016 [1].

Customers regard ‘Convenience’ as the most distinguishing feature of smartphone banking service from conventional banking services since it offers quick access and easy procedure for users [3]. From the security perspective, however, ‘Convenience’ from increased accessibility and simplified procedure of banking service means rather susceptible environment to hacker attempts which undermine the users’ financial data [4]. A number of attack cases e.g. Trojan, mobile phising, key logger and MITM (Man in the middle) have been reported since the launching of the first smartphone banking application [5, 6]. Security vendors now consider mobile banking service among the various mobile services as the highest security concern [7].

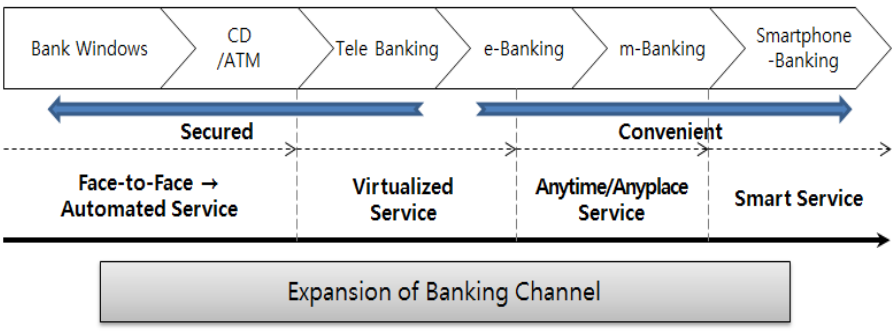

Fig. 1. Evolution of banking service

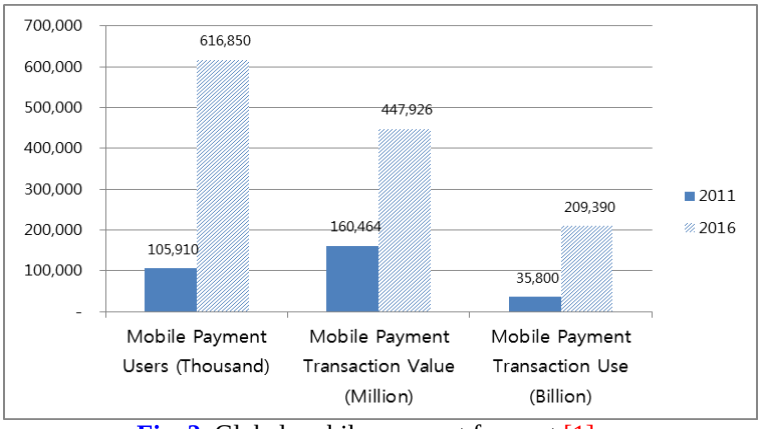

Fig. 2. Global mobile payment forecast [1]

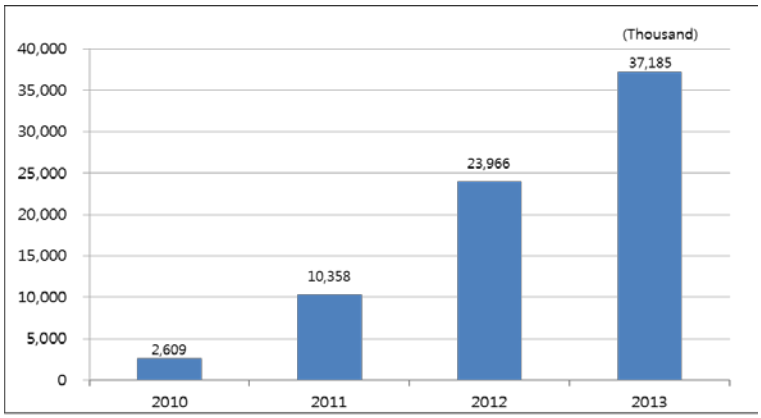

Fig. 3. Smartphone banking users in Korea [8]

Under these circumstances, it is urgent for financial authorities around the world to introduce security policies which seek out both security and convenience. In this regard, major countries around the globe have already put step forward to introduce national-level security standard, especially in authentication mechanism. However, Korea, which has now the second largest mobile banking users in the world (37.1 million users by end of 2013 as illustrated in **Fig. 2**), is experiencing trouble dealing with security policy especially in introducing authentication to smartphone banking service.

The Korea government has obliged the use of ActiveX plug-in based 'Public Key Certificate' on smartphone environment also as the PC environment through 'Smartphone E-Service Security Measures' established in December, 2009. However, serious problems regarding compatibility, security and convenience could occur when applying security measures to the smartphone environment as the internet banking environment. This is due to over 97.5% of the domestic PC environment uses 'Microsoft Internet Explorer' which results in internet banking service that is possible to implement only through ActiveX controls. Therefore, the Korean government announced 'Deregulation Measures of Using Public Key Certificate in e-commerce' to relieve the regulations on using in payment under 300,000 won in March 2010 and also announced 'Guidelines for Authentication Method in e-commerce' for financial institutions and e-commerce users to voluntarily self-select the authentication method in May 2010. However, these also suggest the same levels of security standard as the

Public Key Certificate which resulted in titular deregulation as the authentication system applied to the existing internet banking environment is kept.

The problems are primarily due to blindly pursuing on security measure in negligence of users' convenience. As mentioned above, convenience is the main reason customers use smart phones banking service, therefore optimal authentication methods for smartphone banking should reflect the balanced standards between security and convenience. In addition, cost or economic measures also need to be considered as well as security and convenience when introducing a new authentication mechanism. It requires tremendous time and money for financial service provider to implement a new security system. Moreover, users may need to purchase token or pay issuing cost for new authentication method. Therefore cost (economic aspect) need to be considered when introducing new authentication system. Hence, to derive the appropriate authentication method for smartphone banking services, this study make ANP approaches with prioritizing the authentication requirements in consideration of security, convenience, and cost.

2. Authentication Issues in Korea

2.1 Issues regarding 'Active X Control'

ActiveX control is a software component framework, sometimes called 'add-on' or 'plug-in' developed by 'Microsoft' and operated in many Microsoft applications such as Internet Explorer, Microsoft office, and Microsoft visual Studio. It enhances users' browsing experience in the context of World Wide Web by offering various functionalities and tasks that web browser cannot perform by itself [9].

Users can allow installing ActiveX control to perform certain tasks such as plying multimedia, watching streaming service and installing security updates.
This made the web "richer" but provoke serious problems including compatibility issues (since such controls are designed for Microsoft application and do not work on other platforms) and security risks issues (since cybercriminals can hide malicious ActiveX control in web pages) [10]. In principle, users can decide whether or not to download and install ActiveX control since the use of it is an optional. However, due to the decade-long monopoly of Internet Explorer in Korean web market, virtually all Korean web sites (private web sites such as finance, shopping and etc., and even government web sites including National Tex Service, Supreme Court of Korea and etc.) are designed on and optimized for Internet Explorer. For most of web users in Korea, it is almost mandatory to install ActiveX to fully explorer the web sites and use web services.

Moreover, since most of web sites in Korea are designed on Internet Explorer, users of Firefox, Google Chrome, Opera and Safari experience serious troublesome when browsing Korean web sites for those web site do not function properly on the platform other than Internet Explorer. It is seen that Korean web environment is highly dependent on Microsoft Internet Explorer.

According to the survey from 'Ministry of Science, ICT and Future Planning', only 22 web sites over top 100 domestic commercial web sites support more than 3 web browsers while 91 web sites over top 100 international commercial web sites support more than 3 web browsers [10]. In case of use of 'ActiveX control', 75 domestic commercial web sites over top 100 domestic commercial web sites use ActiveX control while 35 web sites over top 100 international commercial web sites use ActiveX control [10].

Table 1. The number of web sites that each browsers support [10]

	Internet Explorer	Google Chrome	Safari	Fire Fox	Opera
Domestic	100	24	21	21	11
International	100	93	80	90	62

Another survey from 700 citizens showed that about 88% of respondents experienced inconvenience due to the use of ActiveX, and 78.6% of respondents think ActiveX should be thrown out from web environment. Considering this result, there should be regulatory reform on overall security measure, especially on authentication method. And this applies to not only PC but also all smart media through which users can access to web [11].

2.2 Issues regarding use of 'Public Key Certificate'

National 'Public Key Certificate' system in Korea was introduced by 'Electronic Signature Act of 1999' which systemized the issuance and management of public key certificate. It is based on public key infrastructure which applied asymmetric key encryption/decryption mechanism and supports verification of digital signature, integrity on certification evidence, and non-repudiation [12].

It is widely used in online transaction, internet financial service and user identification for a variety of internet services in Korea. As shown in **Fig. 4**, by 2012, a total of 24.1 million public key certificates have been issued in Korea which exceed the economically active population in Korea(2,550 in 2012) now use public key certificate [13].

Until December 1999, the Clinton administration did not allow for the export of 128-bit encryption for international users. Most of exported browsers supported only 40-bit weak encryption and 40-bit encryption was not considered strong enough for online transaction in Korea. Therefore, in 1999, the Korea Information Security Agency developed its own encryption standard SEED, a block cipher which was based on 128-bit key encryption algorithm, and introduced own national certificate system with the aim of securing e-commerce and online transaction. Because every other nation waited for the 128-bit SSL protocol to be exported from the US and have standardized on that, SEED was used nowhere else except Korea [12, 27].

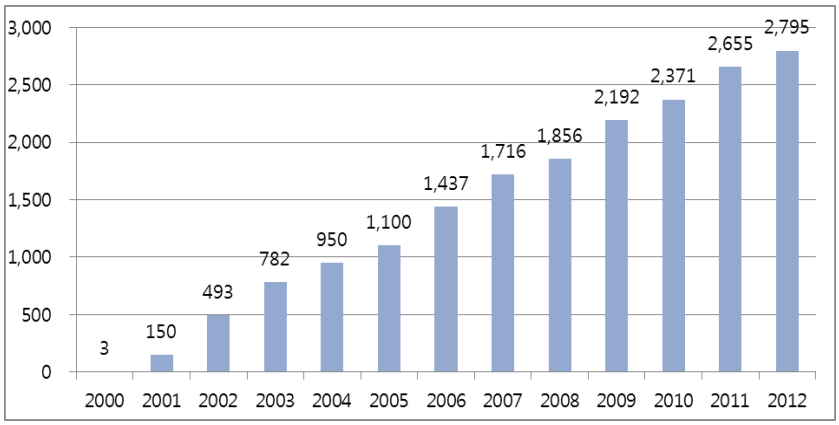

Fig. 4. The number of issued Public Key Certificate in Korea [13]

Moreover no major SSL libraries or web browsers supported SEED, it required users to install plugins for use SEED in web sites. At the begging, users chose and installed either ActiveX control or NSplugin based on their Web browser (Internet Explorer of Netscape) for the SEED plugin, which was then tied to public key certificate issued by Korean government certificate authorities. However, after the years of browser competition, over 97.5% of PC users in Korea uses Internet Explorer and this has resulted that users' only choice to do any kind of encrypted communication online is installing ActiveX control [14]. And of course, this has troubled Mac and Linux users on using internet banking and raised compatibility issues in Korean web environment.

Basically, there are three fundamental security considerations for implementation of internet banking service. First one is a "Encryption for confidentiality" to protect the transaction data between user and banks from hacker's attempt by encryption mechanism. Second one is "Server/user authentication". Either users or servers in bank verify the user's identification thereby prevent illegal attempt of hacker who disguised as user. Third one is an "One Time Pass(OTP)" which produce exclusive and dedicated password for each transaction event to prevent hackers' attempt [15].

Among the considerations, public key certificate provides "Encryption for confidentiality" and "Server/user authentication". Meanwhile, most of banks abroad use SSL to provide confidentiality. Even though public key certificate was regarded as more secured mechanism because when it was first introduced, it provided higher levels of encryption transaction (128bit) than 40-bit SSL (Secure Socket Layer), there is no difference between these two mechanisms in these days. SSL was standardized and renamed as TLS (Transport Layer Security), and an encryption level has strengthened gradually from AES 56-bit to 128-bit and 256-bit. In early 2012, public key certificate was enhanced to 256-bit after AES 128-bit encryption [28].

In Korea, user authentication in internet banking process should use public key certificate issued by certificate authority in Korea to prove his or her identity. In contrast, most of foreign banks do not require user authentication. They skip this procedure because banks are responsible for all about user authentication. This could be possible through 'EV SSL Certificate': a web standard authentication issued by third-party certification authority like the VeriSign or Comodo Group.

Under current Korean law, electronic financial transaction over 300,000 WON requires user authentication through public key certificate. Since banks substitute for user authentication, domestic users could be issued public key certificate through internet banking. In case of foreign users, situation becomes much more complicated. They should visit few of Korean certificate authorities in person and request for public key certificate which is almost impossible. From 2010, Korean government announced that they would admit alternative authentication mechanisms which could meet the same levels of security standard as public key certificate. However until now, there is no other alternative technologies which has passed current security standard. Korean government has recognized the problems and preparing to regulatory reform. In 'Regulatory reform committee meetings in March, 2014', the committee agreed to deregulate the obligatory use of public key certificate and to introduce a new authentication system (as the first regulatory reform, authentication by PK Certificate became optional with credit card payment in online from May, 2014). It is not decided yet which alternative mechanism would substitute the public key certificate and how to provide more secured and convenient authentication with considering the nature of media that authentication process is carried out.

3. Requirements for Authentication in Smartphone Banking Service

3.1 Security

Requirements for authentication in smartphone banking service with the perspective of security aspect can be drawn from the security requirements in e-Banking service context. Authentication for smart phone banking service should satisfy the fundamental security requirements for electronic financial transactions that is protecting user's financial data from hacker's attack and prevent forgery of confidential data [16].

Table 2 shows fundamental requirements for authentication in smartphone banking service in security aspect. According to ISO 2002 (ISO 7498-2) and several researchers, fundamental security requirements for electronic financial transactions (via internet and mobile) can be classified into (user/server) access authority management, (communication channel) confidentiality, (communication channel/transaction data) integrity, (transaction data) non-repudiation [17, 18]. That is, the method must not give away critical information and alter transaction information in response to malware and phishing so that the attackers could not use the information they obtained. The server must grant information only to authorized users, and prevents reading, piracy, and transformation by illegal subjects. And it must provide non-repudiation to prevent transaction and exchanged data at wrong transaction and error event [17, 18].

Table 2. Requirements in security aspect

Requirement	Definition
Authority Management [16,17]	Identify and authenticate legitimate users when providing electronic financial transaction
Confidentiality [16,17,18]	Assurance of privacy and anonymity, as well as prevention of abuses of anonymity
Integrity [16,17,18]	Confirm the forgery of electronic financial transaction data
Non-repudiation [18]	Provide proper electronic financial transaction fact that users and financial institutions cannot deny

3.2 Convenience

The introduction of smartphone banking service results in a more convenient way to acquire financial service than the existing conventional service since it provide anytime, anyplace service with increased accessibility, mobility and availability [19, 20]. However, the intensive emphasis on security aspect might violate convenience, so there is a need to derive authentication method consisting of appropriate harmony between security and convenience. Any inconvenience of usage from the strengthening process of security would reduce user preference no matter how secure the authentication method is [21].

Arguments with the obligatory use of Public Key Certificate for smartphone banking in Korea have been occurred due to the complexity of use, proceeding speed, compatibility issues which bear tremendous of inconvenience to users [22].

Table 3. Requirements in Convenience Aspect

Requirement	Definition
Compatibility [3, 19]	Supports various OS and maintain neutrality on technology (platform, device)
Ease of Use [3, 34]	Convenience in program installation to use authentication mechanism, easily identify the authentication mechanism
Process Speed [19, 20]	Quick response in authentication processing and provide real-time service
Portability [19, 20, 35]	No burden or inconvenience in carrying authentication token/ method
Issuing Easiness [3]	Provide simple and easy procedure when issuing new authentication or reissuing authentication

3.3 Cost

Another point that should be considered apart from security and convenience when introducing authentication method is a cost [23].

Costs in relation to authentication mechanism are in two terms: service provider's implementing costs for system setup for smartphone banking authentication and users' purchasing or issuing costs for authentication use. No matter how secure and convenient the authentication is, high-price to use would mean falling of user's preference [21].

Businesses' economic burden such as system setup costs and user program setup should be major standards in selecting authentication alternatives [24]. In terms of users' economic burden, there are electronic banking transaction like terminal-of-pocket costs and network interconnection costs and authentication setup costs like cost of issuing new authentication and renewal cost [25].

As users' major choice of electronic banking transaction is by economic ones like saving service fees and cost, and service non-choice is by financial burden to service use, authentication method for smartphone banking should be made to guarantee to minimize users' economic burden.

Table 4. Requirements in cost aspect

Requirement	Definition
Implementation Cost [22, 24]	Businesses' economic burden such as system setup costs and user program setup
Issuing Cost [23, 25]	Terminal-of-pocket costs and network interconnection costs and authentication setup costs like cost of issuing new authentication and renewal cost

4. Authentication Alternatives for Smartphone Banking Service

Authentication method are generally classified with three universally recognized authentication factors: what you know (e.g. ID & PW), what you have (e.g. tokens), and what you are (e.g. biometrics) [27]. Among the various mechanisms and methods, this study draws 3 alternative methods which can substitute Public Key Certificate: OTP, Biometric and Security Card.

4.1 OTP (One-Time Password)

OTP (one-time password) is impossible to mathematically seek out password from the current password, and its dynamic password generation method is complicated. OTP changes ID/PW fixed password every time to prevent authentication information intercept and reuse attack [3].

So, the problems of password-based authentication such as password reuse attack and keylogger attack could be managed so as to be widely used in sensitive areas like electronic banking transaction and corporate in-house information system access control.

However, OTP has a defect that it should be hand-carried to use separate token or battery consumption to be reissued. To complement the problems, one-time password can be generated for smartphones, but it also has the problem of real-time phishing or intercepts attack [29].

4.2 Biometrics

Easy-to-memorize ID/PW can be attacked for easy association. On the other hand, hard-to-memorize ID/PW cannot be easily recalled. Token-based authentication can be easily forgotten, lost, or stolen. However, the user's identity (what you are) is ensured by the result of matching a biometric template with the enrolled data. Since the biometric data comes from the user him/herslef, only the biometric data can be physically bound to the smart phone as the user's identity. The increasing capabilities of biometric capture on smart phones such as signature, face, voice, fingerprint, etc. makes biometric recognition practical [30].

Many of the limitations of password-based key release can be eliminated by incorporating biometric data. Since biometric trait cannot be lost or forgotten, it is inherently more reliable and secure than other methods. Further, biometric characteristics are difficult to copy, share, and distribute, and require the person being authenticated to be present at the time and feature of authentication. Thus, biometrics-based solution is a potential candidate to replace password-based solution, either for providing complete authentication mechanism or for securing the traditional cryptographic keys [31].

4.3 Security Card

Security card is one of two-factor authentication method to complement security vulnerability of one-factor authentication which lists password sequentially in the list type at authentication. However, it has management problem, where financial institutions use different security cards, and hard to deal with in case of hacking, exposure, a stolen [3].

5. The Analytic Network Process

In this study, ANP developed by Thomas L. Saaty was applied to analyze appropriate authentication method for smartphone banking service. To draw the ideal solution and selects the optimized alternative in complex decision making processes, Saaty introduced analytic process methods; AHP and ANP which derive priorities of criteria based on relative

importance judged by pairwise comparison. Both AHP and ANP allow decision makers to reach final decision and achieve goal by quantifying qualitative or descriptive opinions gathered from expert in the relevant field [32]. However, while AHP assumes independent relation and hierarchical decision making process among criteria, ANP assumes interdependence and feedback relation among criteria and networked decision making process [33]. Feedback and inner/outer dependence better capture the systemic effects of complex decision making process [32]. In ANP feedback relation between the criteria in different levels of decision process and also between criteria in the same level are considered, thereby the decision criteria are organized into networks of clusters and nodes. ANP analysis derives network model by analyzing feedback relations among each criteria. The main object of drawing network model is to determine the overall influence of all the criteria.

Following the model, decision criteria and their sub elements are organized into complex network which involve several sub-networks. The criteria are prioritized in the framework of control hierarchy (or sub-network) and then, relative influence among sub-elements in feedback system with respect to each of criteria is derived. The results are weighted by relative importance of criteria and overall influence of all elements is obtained. Finally, optimized solution and ideal alternatives are evaluated based on the overall priorities of criteria and their sub-elements [33].

To derive ideal authentication method for smartphone banking service, this study first drew overall complex network and sub-network which describe the feedback and dependence relation among criteria (security, convenience and cost) as **Fig.5**. And then based on the pairwise comparison from 72 experts in financial security (from government authority, financial institute and Telco), relative importance among criteria and elements are evaluated. With the results ideal authentication method for smartphone banking service is derived.

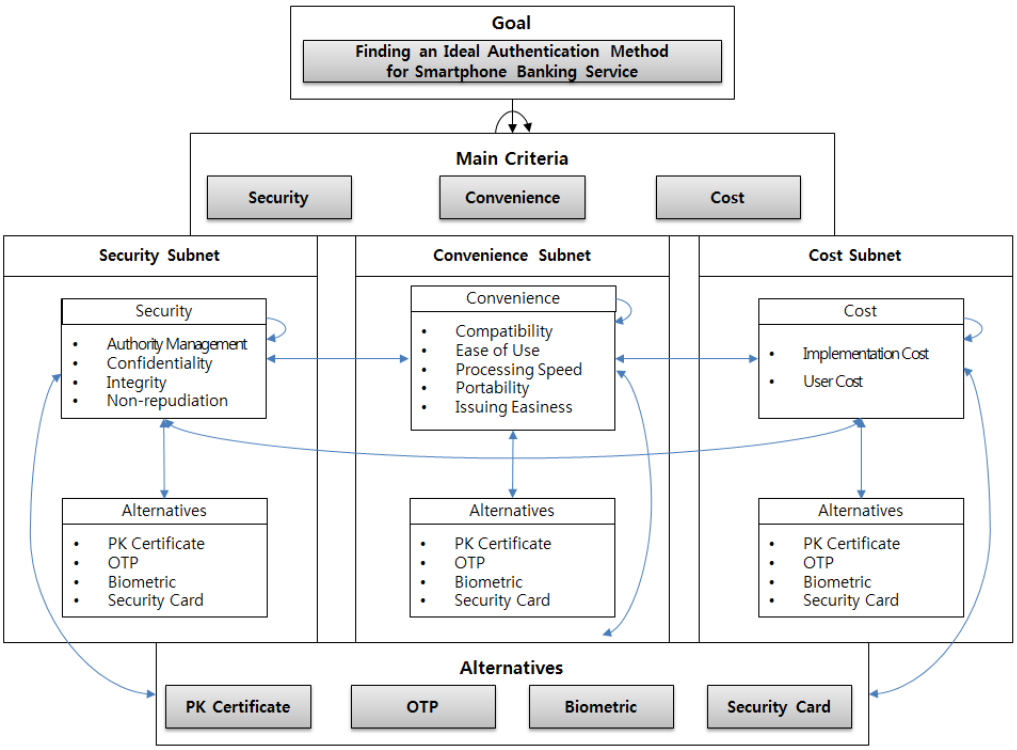

Fig. 5. Whole network model

6. Results of Analysis

6.1 Ideal Authentication Method for Smartphone Banking Service

The result of evaluation in security network shows that biometric is the most appropriate and ideal authentication method with the weight of 0.593. Biometric is a strong authentication based on user's biological traits such as fingerprint, iris, retina, and hand geometry so as to make it hard to try piracy and the modulation to user's information. On the other hand, when security card's number position is exposed; anybody can pass authentication process so as to make it vulnerable to security.

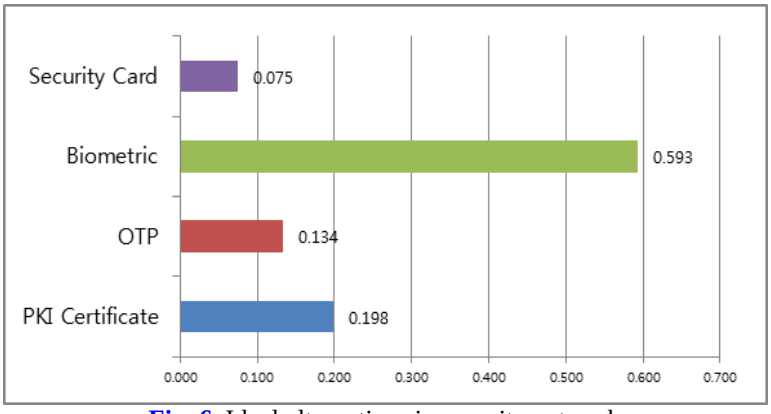

Fig. 6. Ideal alternatives in security network

The result of evaluation in convenience network shows that OTP is the most appropriate authentication method with the weight of 0.694. In traditional channels, OTP authentication should be accompanied by OTP Token for password generation; for authentication, token should be carried; battery problems were inconvenient. But, as generated OTP information gets transmitted by mobile device, these problems would be solved. The most inconvenient media is security card: it should be carried, always. And for Public Key certificate, speed and process problems were tricky, and hard to install on smartphones. As for biometric, it was inconvenient in that it should be installed on the separate recognition device but by the smartphone-embedded sensor solved these problems, making it the next best authentication convenience beside OTP.

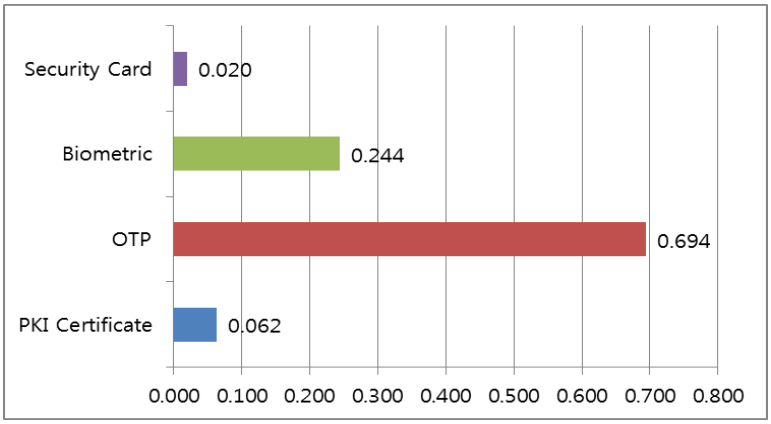

Fig. 7. Ideal alternatives in convenience sub-network

The result of evaluation in cost network shows that biometric is the most appropriate and ideal authentication method with the weight of 0.453. Cost-side user burden is all the same for the four options. But, for service provider-side, there are significant differences in authentication system setup cost: for new authentication system, massive initial cost such as homepage setup and management, network security maintenance, server operation (text treatment, transaction system record keeping). But as for public authorization authentication, it is already required for PC-based environment, so that with no massive initial cost it can be set up easy.

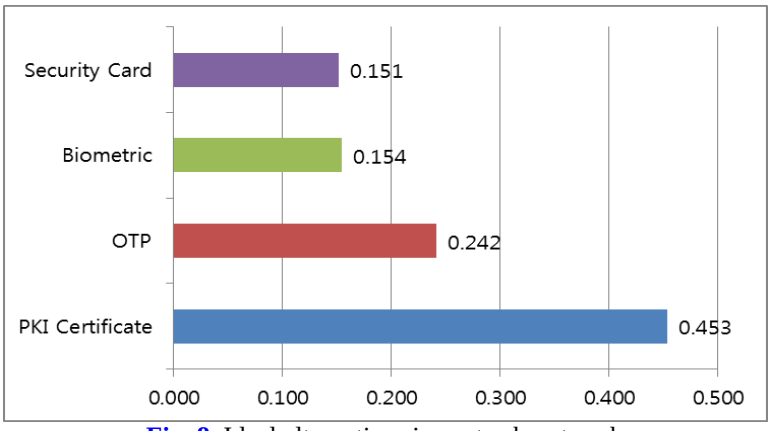

Fig. 8. Ideal alternatives in cost sub-network

Fig. 9 is the priority from the overall network which encompasses detailed element weight and criteria weight including all authentication elements such as stability, convenience, and cost. From the total network perspective, setup cost is also the most consideration, the result of provider consideration that provides financial authority and service. Authentication process speed is also important, in that it reflects customer's demand who expect real-time access and mobility anytime, anywhere. On the other hand, smartphone is vulnerable to exposure and stolen; if these problems would admit other's access to the account, the person can easily access and cause massive financial loss. So at the event, the user's identification should be evaluated right.

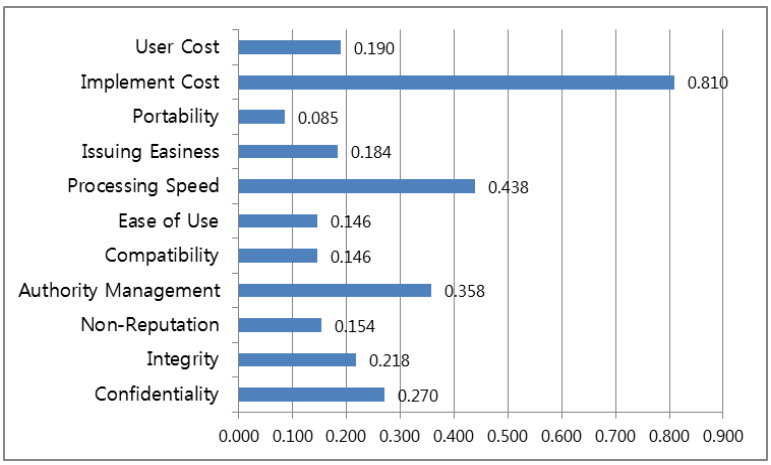

Fig. 9. Priorities among all requirements

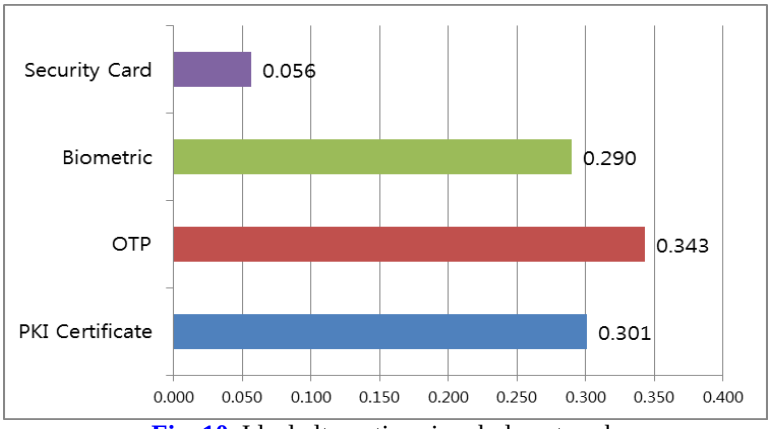

Fig. 10. Ideal alternatives in whole network

Given all the factors, the ideal choice would be OTP. OTP may be weak at security over other devices, but it may be the best in that it provides the most differential convenience for smartphone banking. Also, biometric authentication could meet authentication requirements at the same as now-used public authorization method.

6.2 Sensitivity Analysis

In this study, we tried to find out authentication media preferences according to the changes of users' consideration as well as ideal smartphone banking authentication means. In sensitivity analysis, changes in weight of media according to changes in parameter for three factors were evaluated.

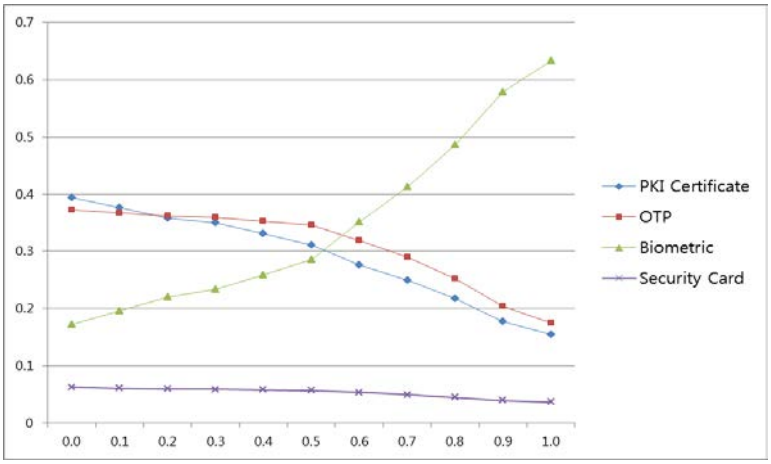

Fig. 11. Sensitivity for authority management

In terms of authority management, Public Key certificate could be the best alternative, but as the authorization management parameter gets more importance, preference for Public Key certificate decreases. On the other hand, biometric, which provide encryption with means of 'what you have' offers the strongest identification method; at the scale of 50% increase in parameter, it exceeds Public Key certificate.

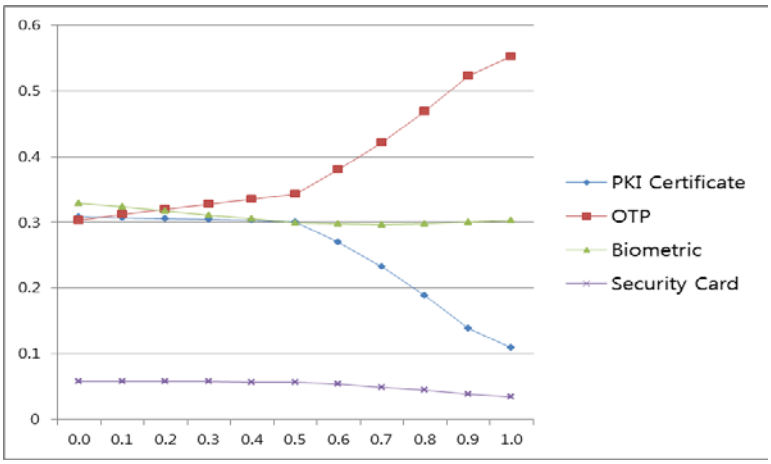

Fig. 12. Sensitivity for processing speed

Second, in terms of processing speed, biometric is most preferred, but as parameter increases, preference for OTP increases. When parameter changes by 20%, it provides more excellent function over other methods; at 50% preference for Public Key certificate get much smaller, which shows that Public Key certificate process is complicated so as to make it less preferred on smartphone.

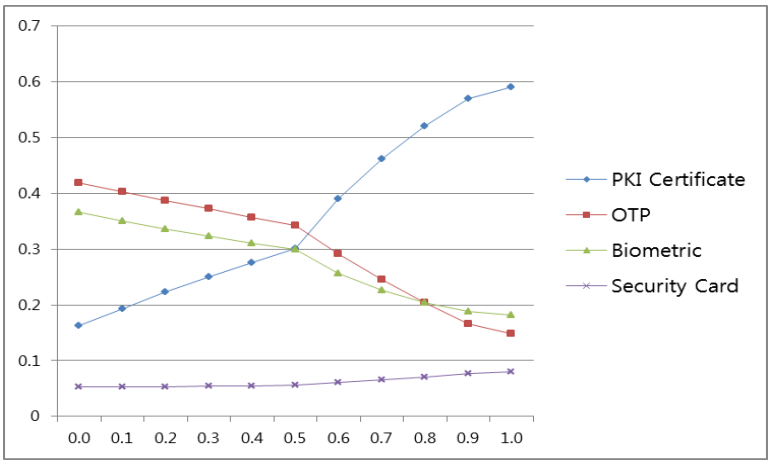

Fig. 13. Sensitivity for implementation cost

On the other hand, in terms of setup cost, OTP is preferred most based on convenience and etc., but at over 50% point, preference for Public Key certificate raises sharply. That is, as mentioned above, as service spreads and businesses have increasing burdens of initial setup cost, Public Key certificate would be the best media now in circulation.

7. Conclusion

In this study, we have conducted ANP approaches to derive the ideal and most appropriate authentication method for smartphone banking service.

Within three criteria (security, convenience and cost) which should be critically considered when introducing authentication method, eleven sub-elements were derived to create a whole network with three sub-network and four alternatives of choice. And then, based on the

judgments of 72 experts in the relevant field, all criteria and elements were prioritized by pairwise comparison of their relative importance.

There are several significant findings from this study. The results of analysis within sub-network reveals that biometric is most ideal in the aspect of security, OTP is most ideal in the aspect of convenience and Public Key certificate is most ideal in the aspect of costs.

Moreover, the result of priority analysis within whole network reveals that implementation cost, processing speed and authority management is the most important consideration in introducing a new authentication mechanism. Considering all aspect in the whole network, OTP is proved to be the most ideal and appropriate authentication method which fits all aspects of criteria.

This research offers several implications and contributions in both practical and theoretical perspectives. A primary contribution is that not only Public Key certificate which is obligatorily used in some countries including Korea, other mechanisms such as OTP and biometric is proven to be more applicable alternatives in smartphone banking environment. This implies that both government and financial service provider need to make significant effort to diversify the authentication mechanisms to reflect the evolutionary changes in both technologies and service environment and to provide more secured and convenient services.

With theoretical perspective, this study has drawn research results by applying ANP, a scientific decision making method which is developed in business field to the policy making process(issues of national security policy). Moreover, although most of previous studies on authentication method focused on security measurement and technical development within the perspective of service provider, this study has not only focused on provider's perspective but also focused on user perspective by including convenience and economic measurement to provide more balanced and concrete result.

Nation-wide financial policies should reflect technological advancement and changes of users' preference. Especially, considering the fact those users of smartphone banking service regard convenience as the most distinguishing aspect of accepting the service, diversification of methods and giving user chances to select authentication method based on their own preference may be more appropriate security policies.

Nonetheless, this study has some limitation in that the analysis of study is mostly based on the opinions of service provider's side which results the high considerations on implementation cost. Therefore, to provide more balanced and concrete implications, future research should reflect more diverse opinions from interested party. In addition, investigating security threats by transmitting data to analyze specific security mechanism and examining how much such security threats can be coped should also be examined.

References

[1] First Annapolis Consulting, "2012 Mobile Banking and Payment Study," 2012.11
[2] Gartner, "Forecast: Mobile Payment, Worldwide, 2009~2016," 2012.5
[3] S. M. Lee, "Trends of Authentication and Forecast," *Information Technology & e-Commerce*, vol.46, pp.31-69, 2011.
[4] K. C. Park, S. J. Kim, and B. G. Lee, "Analysis of Security Priorities of u-Learning Environments using ANP," In *Proc. of 6th International Conference on Ubiquitous Information Technologies & Applications, Korea*, pp. 177-182, 2011.
[5] K. Tracy, "Zeus Strikes Mobile Banking," BankInfo Security, Oct. 2010. http://www.bankinfosecurity.com/articles.php?art_id=3005
[6] A. Castiglione, R. D. Prisco, and A. De Santis, "Do You Trust Your Phone?," *EC-Web 2009, LNCS 5692*, pp. 50-61, 2009. Article (CrossRef Link)

[7] McAfee, “Moile security report 2009,” 2009. http://www.mcafee.com/us/resources/reports
[8] Bank of Korea, “Domestic Internet Banking Service Trends in 2Q. 2013,” Aug., 2013.
[9] A. Denning, *ActiveX Controls Inside Out,* 2nd Edition, Microsoft Press, Washington, 1997. http://www.microsoft.com/security/resources/activex-whatis.aspx
[10] Ministry of Science, ICT and Future Planning, “2013 Investigation of Web Compatibility,” *A press release*, January 14, 2014.
[11] The Federation of Korean Industries, “Survey on ActiveX Usage,” *A press release*, March 24, 2014.
[12] P. Kang, “Status of Public Key Certificate and Policy Direction in Mobile Innovation Era,” *KIISC review*, vol.21 no.1, pp.51-56, 2011.
[13] National Information Society Agency, *National Informatization white paper 2012*, National Information Society Agency, Seoul, 2012.
[14] G. Kanai, "The Cost of Monoculture," Retrieved from blog, January 29, 2007. http://kanai.net/weblog/archive/2007/01/26/00h53m55s#003095
[15] I. Y. Kang, “The problem is not ActiveX but Public Key Certificate,” IT Donga, March 25, 2014. http://it.donga.com/17704/
[16] B. G. Lee, Y. K. Yeo, K. Y. Kim, and J. H. Lee, “Effect of Trust and Cognitive Absorption on Smartphone Use and User Satisfaction,” *The KIPS Transations: Part D*, vol.16, no. 6, pp.471-480, 2010.
[17] Comptroller of Currency, “Internet Banking--Comptroller's Handbook,” OCC, Washington, 1999.
[18] P. Hanaeek, K. Malinka, and J. Schafer, “e-Banking Security-A Comparative Study,” In *Proc. of IEEE International Carnahan Conference on Security Technology*, pp. 326-330, 2008. Article (CrossRef Link)
[19] T. Laukkanen, “Internet vs. mobile banking: comparing customer value perceptions,” *Business Process Management Journal*, vol. 13, no. 6, pp. 788-797, 2007. Article (CrossRef Link)
[20] M. Pura, “Linking perceived value and loyalty in location-based mobile services,” *Managing Service Quality*, vol. 15, no. 6, pp. 509-538, 2005. Article (CrossRef Link)
[21] H. J. Lim, H. W. Shim, S. H. Seo, and W. J. Kang, “Authentication Technology Status Analysis of Electronic Financial Transaction Environment,” *Korea Institutes of Information Security and Cryptology*, vol. 18, no. 5, pp. 84-98, 2008.
[22] H. Kim, J. H. Huh, and R. Anderson, “On the Security of Internet Banking in South Korea,” *Oxford University Computing Laboratory, CS-RP-10-01, University of OXFORD*, 2010. http://www.cs.ox.ac.uk/publications/publication3442-abstract.html
[23] S. C. Hwang, “A study on next generation e-banking Service channel,” *Information Technology & e-Commerce*, vol. 39, pp. 29-54, 2010.
[24] T. Dube, T. Chitura, and L. Runyowa, “Adoption and Use of Internet Banking in Zimbabwe: An Exploratory Study,” *Journal of Internet Banking and Commerce*, vol.14, no.1, pp.1-13, 2009.
[25] D. Sergios, and K. Nikolaos, “Linking Trust to Use Intention for Technology-Enabled Bank Channels: The Role of Trusting Intentions,” *Psychology & Marketing*, vol. 27, no. 8, pp. 799-820, 2010. Article (CrossRef Link)
[26] N. Mallat, M. Rossi, and V. Tuunainen, “Mobile Banking Services,” *Communications of the ACM*, vol 47, no. 8, pp. 42-46, 2004. Article (CrossRef Link)
[27] KISA, “Forum for Secured Online Transaction”, May. 2010.
[28] H. Marko, H. Konstantin, and T. Elena, “Utilizing national public-key infrastructure in mobile payment systems,” *Electronic Commerce Research and Applications*, vol. 7, pp. 214-231, 2008. Article (CrossRef Link)
[29] N. H. Kim, “Voice-based OTP Generation Techniques for Mobile Banking,” *Journal of KIIT*, vol. 11, no. 5, pp. 113-119, 2013.
[30] S. Yun and H. Lim, “The Biometric based Mobile ID and Its Application to Electronic Voting,” *TIIS*, vol. 7, no. 1, pp.166-183, 2013. Article (CrossRef Link)
[31] S. Lee, Y. Chung, D. Moon, S. B. Pan and C. Seo, “A Practical Implementation of Fuzzy Fingerprint Vault,” *TIIS*, vol. 5, no. 10, pp. 1783-1798, 2011. Article (CrossRef Link)

[32] Saaty, T.L. *Decision Making with Dependence and Feedback: The Analytic Network Process*, 2nd Edition, RWS Publications, Pennsylvania, 2001.
[33] Saaty, T.L. *The Analytic Network Process*, RWS Publications, Pennsylvania, 1996.
[34] J. H. Lee, "Development of Smart Mobile and Information Security," *Communications Policy*, vol. 22, no. 13, pp. 17-33, 2010.
[35] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in eBanking and the effects of experience," *Interacting with Computers*,vol. 22, no. 3, pp. 153-164, 2010. Article (CrossRef Link)

Keon Chul Park is a research fellow at the Communications Policy Research Center(CPRC) of Yonsei University. He received his M.S degree from Yonsei University in 2011. And now he is in Ph.D course at Yonsei University. His research interests include digital convergence and ICT/Smart media policy.

Jae Woo Shin is working for Korea Telecom. He received B. A. from the Department of Business Administration at Korea University and MBA from Purdue University. Now he is in Ph.D course at Yonsei University. His research interests include ICT digital convergence and ICT/Smart media policy.

Dr. Bong Gyou Lee, Professor at Graduate School of Information, has served as a director of Communications Policy Research Center (CPRC) in Yonsei University since 2009. Dr. Lee received B.A. from the Department of Economics at Yonsei University and M.S, Ph.D. from Cornell University. During 2007 and 2008 he served as Commissioner of the Korea Communications Commission.