Authentication in Online Banking Systems through Quantum Cryptography

Anand Sharma[1], S.K.Lenka[2]

FET, MITS, Lakshmangarh
Sikar, Rajasthan, India
[1]anand_glee@yahoo.co.in, [2] lenka.sarojkumar@gmail.com

***Abstract*-The new information technology is becoming an important factor in the future development of financial services industry, and especially banking industry. Growing international trading and problems in transferring money have motivated researchers to introduce a new structure. Online banking is the newest delivery channel for retail banking services. Online banking facilitated by various Electronic Commerce technologies, has helped commercial banks to stay competitive through productivity gains, transaction cost reduction and customer service improvement. Security for online banking has changed considerably during the relatively short period that online banking has been in use. In particular, authentication in the early implementations was, and sometimes still is, vulnerable to various attacks such as phishing. It is known that the quantum cryptography protocols are able to detect immediately any attempt to attack the key exchange and the authentication process. This paper presents an introduction of online banking and quantum cryptography. In this paper we are proposing a model for authentication in online banking system with quantum cryptography.**

Keywords- Online banking. Quantum Cryptography, QKD, Security, Authentication.

I. INTRODUCTION

There are differing definitions related to online banking found in the literature, online banking refers to performing banking transactions using electronic medium over internet. Technological developments particularly in the area of telecommunications and information technology which are revolutionizing the banking industry [1] and the importance of online banking are growing because of its wider reach and lower cost per transaction. Most of banks are using the Internet as a new distribution channel. Online banking has triggered massive change in the commercial banking practices since it was first introduced as "home banking" services by the four major New York banks in 1981 [2]. The last few years have witnessed profound technological changes among which is the advent of electronic commerce, or the exchange of products (tangible and otherwise) and payments via telecommunication systems. It covers various initiatives such as Internet banking, Internet payment system, phone banking, and mobile banking. Potentialities of this technology are remarkable, specifically in banking industry. Many banks have established presence on the Internet and many others are in the process of doing so using telecommunication systems and technologies, a bank can reach out to users and provide them with not only general information about its services but also the opportunity of performing interactive retail banking transactions [3]. Capitalizing on e- Commerce's ability to offer productivity gains, transaction cost reductions, improved customer services and flexibility in fulfilling user's changing needs and lifestyles, online banking has enabled banking institutions to compete more effectively in this global environment, extending their products and services beyond the restriction of time and space [4].

Having an interactive nature, the Internet as a channel for services delivery is fundamentally different from other channels, such as branch networks or telephone banking [5]. Online banking has been introduced as a solution and started with the use of software and private network in first. Currently, the Internet and the World Wide Web have impacts on the way banks doing the business. Today, international trade has grown significantly. More recently, deregulation and globalization have led to a spectacular growth in the value of non-trade-related financial transactions.

The range of functions that are usually offered by telecommunication systems of online banking include displaying balances and statements, paying bills, transferring money between accounts, viewing standing orders and direct debits, viewing transactions with a search and sort facility, ordering cheque books, and transferring information into other software like a personal financial manager [6].

This paper is organized as follows. Section 2 presents the systematic approach for authentication in online banking system. Section 3 gives an overview of Quantum Cryptography and Quantum Key Distribution. Use of QKD in Online Banking System will be explained in section 4. Finally, conclusion and future work will be presented in section 4.

II. AUTHENTICATION IN ONLINE BANKING SYSTEM

In online banking systems, banks must ensure that users feel safe when using online banking services. They can control the level of authentication it takes to enter their sites. They can limit and deter attackers by making it far too difficult to have success in obtaining fraudulent access to a customer's account.

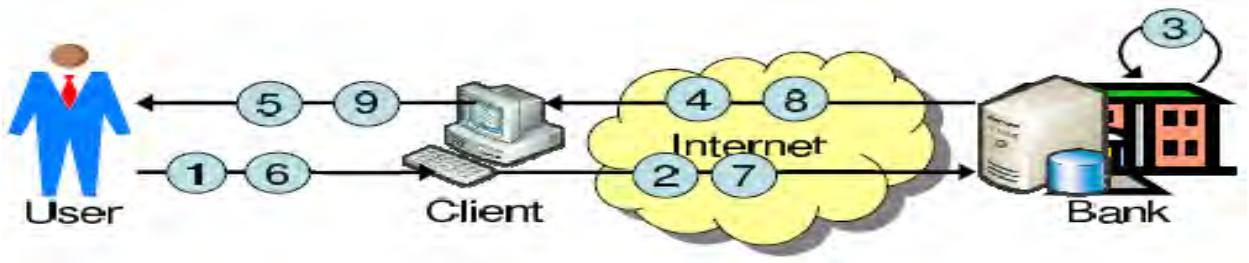

Fig. 1 Authentication in online Banking

Fig.1 shows the authentication process in a traditional online banking system. Following are the steps of authentication in an online banking system.

1. Produce Login Id and Pass-code
2. Transmit Login Id and Pass-code
3. Verify Login Id and Pass-code
4. Transmit service options
5. Present service options
6. Transaction request
7. Transmit transaction request
8. Transmit transaction confirmation
9. Present transaction confirmation

III. QUANTUM CRYPTOGRAPHY

The quantum cryptography is based on the Heisenberg uncertainty principle of quantum mechanics and photon polarization. According the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the point when it is measured. Secondly, the photon polarization principle describes how light photons can be oriented or polarized in specific directions. Moreover, a polarized photon can only be detected by a photon filter with the correct polarization or else the photon will be destroyed. It is this "one-way-ness" of photons along with the Heisenberg Uncertainty principle that make quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdroppers.

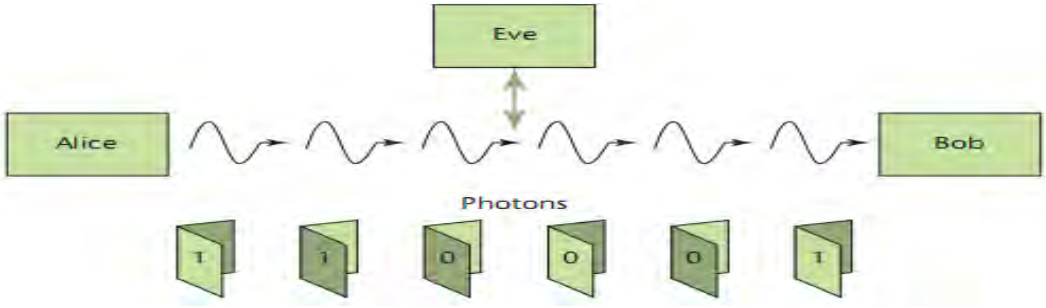

Fig. 2.The basic idea of Quantum Cryptography.

The concept of quantum cryptography (QC) was introduced by Bennett and Brassard in the early 1980s [7]. The BB84 protocol is the first quantum key distribution (QKD) protocol, which was proposed by Bennett and Brassard in 1984.

Then other protocols succeeded like the protocol with two states, the protocol with six states, the protocol of Einstein- Podolsky-Rosen and others. They all exploit the disturbances of the quantum states inevitably caused by the indiscretions. But the majority of the experiments of quantum cryptography are now limited to protocol BB84 because it is simple and due to limited physical devices necessary for its implementation. In the beginning of the year 90, the first experiment was carried out by Charles Bennett and

Brassard and their colleagues at the laboratory of IBM over 30cm through the air [8]. The first demonstration on an optical fiber was successfully executed in the university of Geneva in 1993 [9].

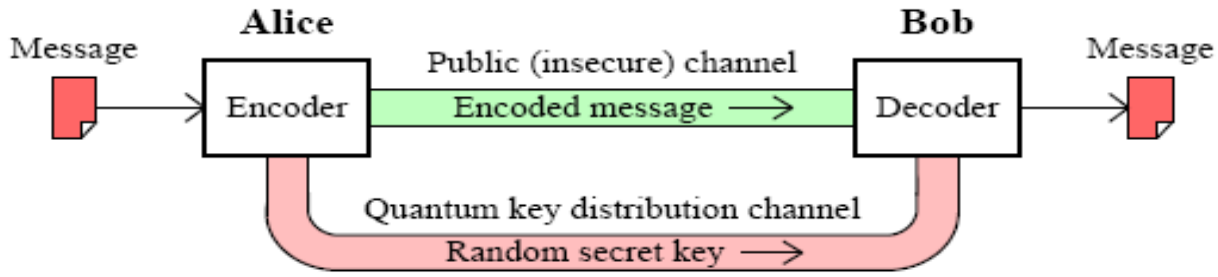

Fig. 3. Conventional Model for Quantum Cryptography

IV. QC in ONLINE BANKING

Online banking is increasingly becoming more complex and sophisticated. As internet is becoming more popular to check account balances and transfer funds between accounts worldwide. As wired and wireless banking are becoming more popular worldwide, their securities continue to be major concerns among users.

Nowadays, Banks and financial institutions use either symmetric cryptography or asymmetric cryptography. However, due to the advent of sophisticated technology and cryptanalysis techniques, security solutions are not unconditionally secure. As computers become more powerful, encryption and decryption keys have to be longer in order to retain the level of difficulty. So transactions could be corrupted and altered without the awareness of the bank. This constitutes a serious danger because criminals and malicious organizations could profit of the breach to steal and highjack. Securing critical financial transaction is mandatory and will be more and more necessary to master economical crime.

One of major concerns in online-banking is a security threat. This section discusses on main challenges in online-banking i.e. authentication. Since most online-banking applications use some pass-code or PIN for commercial transaction settlements. Researchers have been actively involved in development of secured methods for online-banking over the Internet. Authentication is even more sensitive issues in online banking. The banking industry is regulated and monitored by governments and online-banking need to assure regulators of security for their clients.

Researchers throughout the world are experimenting new techniques in authentication for online banking security. The idea is that user information can be transmitted through QKD. The quantum cryptography performances have already captured the interest of banks, companies and institutions, and many of them are testing this technology, that is commercially available: MagiQ Technologies, New York; idQuantique, Geneve and SmartQuantum, New York .

Single factor authentication in online banking is no longer sufficient to protect accounts. Our objective is to propose an authentication method for the online banking security. Our proposed model can be seen in figure 4. The starting point is the user's request. In the event of a request, the user is redirected to authentication service, carrying with him/her some kind of Pass code or PIN. After verifying that pass code or PIN the user will access that Quantum cryptosystem. Quantum Cryptography / Quantum Key Distribution involvement is needed only to authenticate.

Entities involved are the user, user's pass-code/PIN and the quantum cryptosystem.

Fig. 4. Quantum Cryptography for User Authentication

We are sketching out the entire process of authentication using a user authentication and QKD user authentication to decide whether access is granted or not.

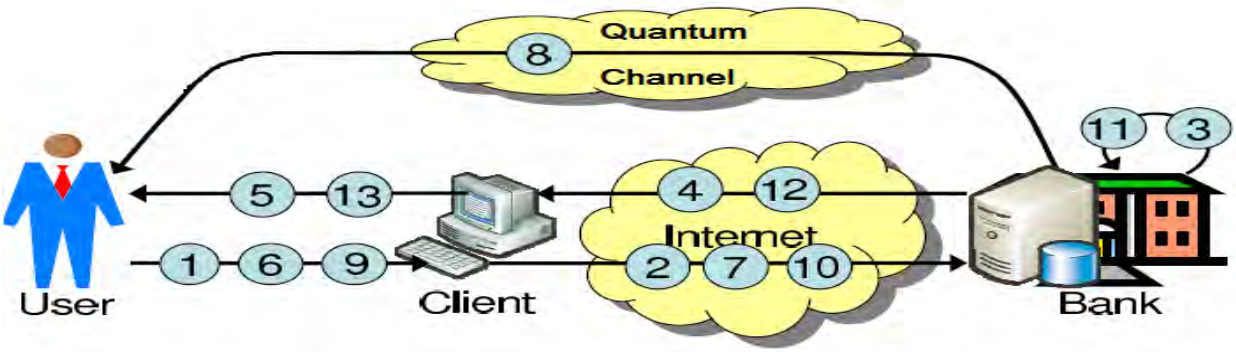

Fig. 5. User Authentication through Quantum Cryptography

Here we are having step by step scheme for our proposed authentication mechanism. In this proposed model we have introduced quantum cryptography concept for authentication. Figure 5 shows the steps for authentication. The two levels of authentication we have used in an online banking system to stronger the authentication.

1. Produce Login Id and Pass-code
2. Transmit Login Id and Pass-code
3. Verify Login Id and Pass-code
4. Transmit service options
5. Present service options
6. Transaction request
7. Transmit transaction request
8. Quantum Key Distribution
9. Produce Quantum code
10. Transmit Quantum code
11. Verify Quantum code
12. Transmit transaction confirmation
13. Present transaction confirmation

This scheme of authentication is an enhancement of the standard authentication scheme which authenticates the customer to the online banking system. Strength of this Quantum authentication is that it allows the user to have a higher level of trust in any communication they receive from the banks and it allows users to feel safe when logging into their accounts.

V. CONCLUSION

The new information technology is becoming an important factor in the future development of financial services industry, and especially banking industry. Online Banking is multifaceted and impacted by changes in such technology, deregulation of many parts of finance, the emergence of new banking institutions and economic restructuring. The relationship between theory and practice may be considered weak and unstructured, as qualitative approaches have been criticized for not infusing theoretical factors. To this end, in this paper an attempt was made to address this issue by developing a theoretical framework which may improve the online banking security. Nowadays the cost of a Quantum Cryptography system can be estimated around one hundred of thousands of dollars, but we expect that it will get cheaper and will be implemented in banks in the next few years.

REFERENCES

[1] M.S. Sohail, B. Shanmugham, E-banking and customer preferences in Malaysia: An empirical investigation, Information Sciences (2003).
[2] Osho, G.S., How technology is breaking traditional barriers in the banking industry: Evidence from financial management perspective. European Journal of Economics, Finance and Administrative Sciences, 2008(11): p. 15-21.
[3] A.M. Aladwani, Online banking: a field study of drivers, development challenges, and expectations, International Journal of Information Management 21 (2001) 213-225.
[4] Turban, E., et al., Electronic commerce: a managerial perspective. 4th Edition ed. 2008: Prentice Hall.
[5] M.H. Shah, F.A. Siddiqui, Organisational critical success factors in adoption of e-banking at the Woolwich bank, International Journal of Information Management 26 (2006).
[6] C.S. Elizabeth Daniel, On-line Banking: Strategic and Management Challenges, Long Range Planning 30 (1997) 890-898.
[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, New York, Bangalore, India, 1984, pp. 175-179.

[8] C.H. Bennett, G. Bessette, G. Brassard, L. Salvail, and 1. Smolin, Experimental quantum cryptography, Advanges in Cryptology Eurocrypt '90 Proceedings, pages 351-366, May 1990.
[9] Muller, 1. Breguet, and N. Gisin, Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than lkm, Europhysics Letters, 23:383-388, August 1993.
[10] Anand Sharma, Vibha Ojha, R.C.Belwal, Vishal Goar "Quantum cryptography – The Concept and challenges" in proceeding of 2nd International Conference on Computer and Automation Engineering (ICCAE 2010) Singapore, volume 1, 2010 pp. 710-714.
[11] Lee Y. G., "The influence of security and risk perception on the reuse of internet banking", The Journal of MIS Research, Vol.17, No.1, 2007, pp.77-93
[12] Anand Sharma, Vibha ojha, R.C.Belwal, Gaurav Agarwal "Transmission and System Control in Quantum Cryptography" International Journal of Computer Technology and Applications. Volume 2 (3) 2011 pp. 590-593
[13] Suh, B. and I. Han, "Effect of trust on customer acceptance of Internet banking", Electronic Commerce Research and Applications, Vol.1, 2002, pp.247-263
[14] Yu I. and So S. H., "An empirical study on the factors influencing the usage intention of internet banking systems", The Journal of Industrial Economic Research, Vol.17, No.6, 2004, pp.2383-2404
[15] M. Quaddus, D. Achjari, a model for electronic commerce success, telecommunications policy (2005) 127-151.
[16] M. Pohjola, "The New Economy: Facts, Impacts and Policies," Information Economics and Policy, 14, 2002. pp. 133–144.
[17] C.S. Yiua, K. Grantc, D. Edgar, Factors affecting the adoption of Internet Banking in Hong Kong—implications for the banking sector, International Journal of Information Management 27 (2007) 336-351.
[18] C.S. Elizabeth Daniel, On-line Banking: Strategic and Management Challenges, Long Range Planning 30 (1997) 890-898.
[19] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS Quarterly, vol. 27, no. 3, pp. 425-478, 2003.
[20] B. H. Wixom and P. A. Todd, "A theoretical integration of user satisfaction and technology acceptance," Information System Research, vol. 12, no. 1, pp. 85-102, 2005.