Multi-layer Logon Verification System: A Case Study of Indian Banks

Mohammad Asim
Dept. of CSSE
University of Hail, KSA
m.asim@uoh.edu.sa

Abstract. Internet is only the medium which connects billions of people globally and finally has been removed all physical barriers. Bank is also one of the sector which greatly influenced with the invent of Internet. However, Internet banking is one of the service of the bank which provides many services online to the customers without being physically visit the bank. On the one end Internet banking bring many services to the customer but on the contrary also pose a risk of fraud, theft and vandalism.

The key aspect of any online services to authenticate the customer without any face-to-face communication which ultimately challenge for the technology to validate them without any compromise. In the whole scenario security can be compromised at three level; at the client, in transit and at the server. Presently there are number of authentications methods proposed by the researcher worldwide for the financial institutions but my study is particularly focus on Indian Banks. Moreover, a special focus given on online services providing by the banks to their customers. Study reveals the authentication methods is a layered approach to achieve high degree of privacy and security in online services and which is a combination of two approach such as mobile and Token based authentication methods.

I have conducted a study of 25 banks of India to collect the data regarding present Authentication methods adopted presently. The paper describe in detail working of the said authentication methods and future implementation of these technologies.

Keywords: Internet banking, Protection and Security, Mobile Authentication, Token Authentication.

1 Introduction

In the current scenario, the Internet has become extensively used gizmo for corporate organizations, education and bank is using Internet Technology to provide various online services to serve their customers with ease and comfort. However, with the growing application of the Internet, security has become an important area of attention for various levels of users and however, a big challenge for the organization to implement security methods for safe and hassle free services for their customers to gain their confidence. There are several factors that may be affecting the adoption of internet banking. However, an important factor is the level of security and the risk associated with it[1].
The paper mainly discusses and analyzes the current procedures adopted by major banks in India. However, it is important to note that whenever there is trust, there is risk. Thus, trust is accepting risk. Trust, risk, security, and reliability are fundamental to internet banking. I investigated the security of the internet banking systems in Banks in India including public, private, and foreign banks through visiting their sites and security guidelines/manual they have online.

The rest of the paper is outlined as follows. In section 2, I describe the current Internet Banking Authentication System adopted by Indian Banks. In section 3, I have proposed an approach for authentication. In section 4, I am concerned with the case study of the banks. In section 5, there are some recommendations for the banks and finally I concluded in section 6.

2 Existing Internet Banking Authentication Methods in India

I have conducted the study of 25 major banks in India through visit their official sites to obtain the information for their security methods adopted for authentication process:

\[
\text{SSL + HTTP + Virtual Keyboard}
\]

Authentication is a method to verify the credentials of the customer before using any online services without any paper work or physical identification system. However, now the question arises here for validating the credentials of the customer[2]. After a thoroughly studied of the banks sites, I have found that all the banks are using method of authentication based on HTTPS. Which allow a secure session between the clients machine and the bank’s server.

Presently the authentication system of the Internet banking in India is based on public key cryptography system and the digital signature technology for authenticating, thus the safe and smooth electronic transaction can be ensured. The Certificate based authentication system is a certificate center system based on PKI. The security authentication system of internet banking is composed of Central Bank Certification Authority (CA) and the Commercial Bank internal management CA. These two systems work independently and cooperatively. The tasks are divided as follows:

The Central Bank CA issues the digital certificates to the clients of the internet banking, and the internal management CA issues management digital certificates to commercial bank employees. These digital management certificates are mainly used in the Registration Authority (RA) system. The main purpose of Commercial bank employees to use digital certificate to authenticate ID, encrypt transmission and resist repudiation, also audit clients' certificate requests and create the clients' certificates.

Security proxy permit a web-based transaction interface embedded with functionalities such as authentication, integrity, non-repudiation, encryption, authorization and security enhancements. The main function of Digital signature is to ensure the integrity and non-repudiation of any transaction [3].