E-Banking Frauds:
The Current Scenario and Security Techniques

4

Sandal Azhar
University of Delhi, India

Manisha Shahi
University of Delhi, India

Vikas Chhapola
University of Delhi, India

INTRODUCTION

Electronic banking or net banking includes any electronic payment system that permits clients of a bank to make transactions through the bank's internet-enabled website or app. It gives access to the facilities of the banks online if there is a required means for it. It provides various services like funds transfer, payment of bills, checking of account details, online shopping and recharge. E-banking has found its place in daily lives as it works as per the comfort and convenience, provides faster transactions, is cost effective and can be done from anywhere. With these advantages, it is also becoming a centre of attraction for Cyber frauds- online frauds in which a person's account is used to transfer funds for financial gain. The Cyber criminals make easy money by duping users, by methods like phishing, vishing (voice phishing), making people download Trojans and malicious softwares which can provide their credentials to the criminal.

E banking frauds have become the most common kind of Cyber frauds which is gaining high popularity. According to a global survey conducted by FIS, a financial services technology firm, Indians are among the most frequent victims of online banking frauds. (Jain, 2018). In comparison, only 8% of people from Germany reported a fraud followed by 6% in the UK. This scenario demands a high level of security measures using latest technology which the Cyber criminals cannot circumvent.

This paper aims at reviewing all types of banking frauds and the measures which should be taken at the bank as well as user level for maintaining the integrity of the online banking systems. It also studies about current scenario of security that is being implemented by the banks and the potential areas like machine learning and big data analysis which can be used as a tool to combat the plight of this blooming industry. The research also directs towards different cases of frauds globally, their cause and implications. It also provides an insight in the study of fraudulent certificates, the damage it causes, and the suggested certificate transparency phenomenon which can solve this problem.

The main focus of the study is to mention the emerging techniques of security that have the potential to combat this menace of e banking frauds. Certificate transparency, HTTP Security Response Headers Automated Analysis Tools, Behavioural analytics and Big Data can help us build systems that are secure against these attacks.

DOI: 10.4018/978-1-5225-9715-5.ch061

BACKGROUND

Online banking today is so prominent that it is hard to imagine that it was not far ago that this boon came into existence. The beginning of online banking dates back to as early as 1980s when biggest banks in New York started providing their customers home-based services. Customers could access their bank accounts to view statements and pay bills. However, the real breakthrough in internet banking arrived in mid 1990s when internet was acknowledged as a distribution media with great potential. The ease and comfort that this breakthrough brought with itself was commendable and life changing. While this mode of access to the banks and ease of handling the accounts was very convenient and had great potential, people soon realized that this flexibility came at a price. Cyber criminals started considering potential in e-banking to accomplish their vicious motives of financial gains by hacking into the systems. Conventional methods of banking frauds soon were replaced now by e-banking frauds. Technological innovations that the banking sector adopted in their quest for growth, in turn opened a gateway for higher levels of cyber risks. It probably introduced new vulnerabilities and complexities into the system. Hackers are now exploiting these loopholes or finding and inventing new technologies to find such vulnerabilities in the banking systems. Various studies and work have been directed towards this critical topic of online banking frauds. Research on this topic includes both the preventive security measures, strengthening the system and the detection of frauds. Banks are constantly working towards the enhancement of security and using various methods to keep the system safe, like encrypted channels for the transactions, two factor authentication and many technologies are being worked upon to secure the system from being exploited by the criminals. Data analysis software are used by examiners to analyse a bank's business data to gain insight into how well internal controls are operating and to find transactions that indicate fraudulent activity or the risk of fraud.

As the security measures on the bank's side tighten so do the advancement in technologies on the hacker's part, as they keep themselves a step ahead. So, this is a need of the hour to work and research in this direction of developing security measures which are technology at par with the technologies used in these cybercrimes. This industry needs more and more cyber security specialist and passionate minds that want to work for the security of online banking systems and find counter measures for all possible attacks on internet banking. Current research aims at reviewing E-banking frauds scenario as a whole, all kinds of attacks on the banking systems, the techniques used behind them and their potential preventions.

CURRENTLY ACTIVE COMMON ATTACKS:

This section first describes the basic model or nature on which the attacks are based on and the study goes on to explain the techniques currently active in deploying the attacks.

NATURE OF ATTACKS:

In this era where the demand for online transactions is growing at a very rapid pace, we need to have complete technical knowledge of the attacks that are committed online and the vulnerabilities they are based on, to provide appropriate security measures and the solution to the growing problem of e-banking frauds. Attacks are escalating their range and complexity to levels that need high technical understanding on the part of its developers. Every attack is determined to defeat in one way or the other, the authenti-