Analysis of Security of Online Banking in India (December 2017)

Ravneet Kaur
r.kaur@alumni.ubc.ca

Nishtha Chawla
nishtha8@ece.ubc.ca

ABSTRACT

Internet Banking provides the ease of doing the banking transactions from anywhere with the access of internet through online banking interface but the use of internet banking inherently comes with risks. It is very important to protect the confidentiality, preserve the integrity and promote the availability of data. It is of paramount importance to uphold the above-stated security goals as these have a negative impact on a massive user base. The vulnerabilities can be leveraged by adversaries to carry out financial fraud, identity theft and impersonation. We have analyzed and compare security mechanisms of five Indian banks, and how the online security in Indian banking system is different from the major banks in Canada. In addition to the findings of this paper, strict policies regarding security of online banking should be formulated and implementation of mechanisms need to take place in order to improve the current situation. Mitigation strategies should be developed and kept ready in place to put into effect in case of an attack. We have also made certain recommendations so as to enhance security, which primarily includes user awareness by conducting various training sessions and updating security information on the bank's website regularly.

I. INTRODUCTION

In this era of globalization, the internet has become a significant element in every aspect of our lives. One such noteworthy development in this aspect is the banking industry. With the advent of the Internet, we are able to integrate and transform existing businesses to the framework of electronic commerce (e-commerce). In addition to the traditional bank branch services, customers now have facilities and the convenience of electronic banking. Information security issue is a major concern while implementing Internet in banking sectors. As the world is becoming highly interconnected with the internet, there are many threats and risks which impact both the banks and the internet banking, customers. Majority of threats include Trojans, spyware, malware, keyloggers, and viruses. Additional threats include security awareness of the Internet banking customers and the banks, threats (both authentication and authorization), the mobile banking application security problem, protection against man-in-the-middle attack and man-in-the-browser attack. These factors have the potential to influence traditional banking customers from switching to the Internet banking. [1]Financial threats are a global problem and no country is really safe from them. Smaller countries may not make it to the top 10 list in terms of total detection numbers, but relative to the connected population, the risk can still be substantial. Figure 1 shows the countries ranked by percentage of global financial detections seen for the year 2015 and 2016.

Countries ranked by percentage of global detections seen per year

Region	Percentage of global detections 2016	Percentage of global detections 2015
Japan	36.69%	3.21%
China	6.92%	4.69%
India	6.37%	6.31%
United States	6.30%	8.54%
Indonesia	4.78%	6.31%

Figure 1: countries ranked by percentage of global financial detections seen for year the 2015 and 2016.

We aim to [1] highlight such major security threats and risks that plague the internet banking security in India. These risks have the capability to manipulate banking customers and acquire their information for illegal gain. We will also focus on [2] the open problems that still exist in online banking and the controls and measures being deployed by banks to mitigate these threats. Thus, we are doing an assessment study on security of internet banking systems of major Indian banks. We have localized this particular geographical region because the country has an enormous set of online banking customers who are not tech savvy. This is one of the prevalent vulnerability in the system which makes this survey all the more important. The paper also aims to find out [3] how the information security of banks in India is different from that of the banks in other parts of the World.

We intend to conduct a comparative analysis of the implemented security mechanisms and mitigation measures of the chosen banks. Highlights will include areas such as bank's internal security mechanism, bank's website authentication mechanism, and user site authentication technology including login requirements & password restrictions, bank's mobile application security mechanism in perspective of their policies, risks and mitigation efforts. We will track past and current

trends in regard to online banking security threats and the progress made so far with respect to these security attacks.

We also plan to analyze how the threats, risks, policies and mitigation efforts of online banking security systems of Indian banks differ from security mechanisms of rest of the world in this regard. We hope this will provide some insight and contrast of security measures of banks in different geographical regions.

Main resources of our research are the information reports provided on the bank websites along with annual Reserve bank of India reports. We will focus on internet banking security systems in five leading banks of India namely HDFC, ICICI, YES, IDBI and Axis bank.

II. BACKGROUND

While the internet and mobile banking has made banking very easy by accessing the bank's website and bank's mobile application for transactions. But its inception took place in the early 1980s in New York, US, when four major banks offered to provide home banking services to their customers. The concept of online baking was familiarized in India in 1994 by ICICI Bank, with limited services. The internet banking has evolved to the current scenario which involves e-banking, digital wallets, plastic money, mobile application banking etc.
In the year 2016, Japan witnessed a substantial increase in threat detection count which attributed to its first rank in the list of most attacked countries globally, in which India ranks at 3rd position [1].

Graph 1
Computers compromised with banking Trojans, by country 2016

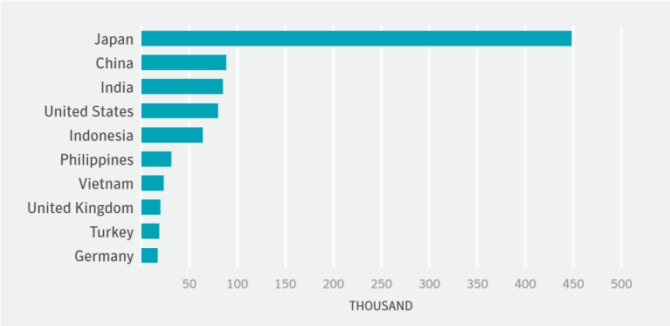

Figure 2: Computers compromised with banking Trojans by country, 2016

Mobile wallets are digital wallets which have gained a lot of popularity because they provide an easy interface. these wallets just need to be loaded with money through user's bank account, after which user can carry out any number of transactions without the hassle of carrying hard cash or plastic money. The graph 2 shows that mobile wallets have experienced increase of 500% in terms of value of transactions carried out from 2012-2016[9].

Graph 2
Transactions carried out through mobile wallets (Rs, billion)

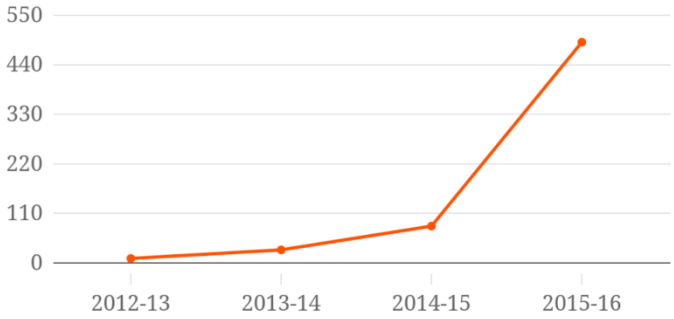

Figure 3: Transactions carried out through mobile wallets in Indian Currency in billions

According to the recent survey report by Facebook and Boston Consulting Group, the number of online banking users is expected to double to reach 150 million counts by 2020[10]. With such an upsurge in the number internet banking users in India, security is the major concern as the online user accounts are a major point of vulnerability.

In a move to digitize the Indian economy, the government introduced demonetization overnight in November**,** 2016 and banned the use of old currency notes. This lead to an 86% decrease in cash circulation which heightened increase in opening new bank accounts, exponential rise of e-services and crashed the cash on delivery in e-commerce. Currently**,** Indian economy ranks at number 3 based on GDP and is largely driven by its vast banking system. Thus, the security of its online banking is of paramount importance which provides services to millions of online users and contributes in billions to the world economy.

III. RELATED WORK

The relative amount of work has been done to analyze the potential threats to online Banking security across the world. Several types of research have been conducted worldwide on Online Banking Security. P. Subsorna and S. Limwiriyakul (2011) paper investigate the internet banking security system of the 12 Thai commercial banks by examining the information available on the bank's websites [3]. Their study reveals that bank websites did not provide sufficient security information to the customers [3]. To provide a comparative analysis, they contrast the findings from Thai banks with the internet banking security of 16 Australian Banks. Based on their research this paper generates a list of guidelines for Thai commercial banks.

R. Lal and R. Saluja (2012), the paper discusses the surfacing of electronic banking as an innovative development. The advancement in e-banking in Indian banking industry is calculated through numerous parameters such as Computerization of branches, Automated Teller Machines, Transactions through Retail Electronic Payment Methods etc. [6]. The data has been collected from Report on Trends and Progress of Banking in India issued by Reserve Bank of India.
Chauhan & Choudhary (2015) talk about the internet banking in Indian context in association with the challenges and

opportunities present in the current system [5]. Security risk, privacy risk, trust factor and less awareness among consumers are the obstacles in the e-banking facilities as suggested by this paper [5]. The paper also lists the increase in electronic banking delivery channels such as a number of mobile banking users, number of ATM's deployed, number of credit and debit cards issued which clearly entail the wide acceptance of e-banking among masses.

P. Subsorn, S. Limwiriyakul(2011) paper inspects Internet banking security systems in Australian banks by examining six main security feature categories which can be used as an Internet banking security guideline and benefit both existing and potential customers[2]. The main purpose of this paper is to probe the security of Internet banking systems of Australian banks [2]. To offer a wide scope for the relative analysis of the Internet banking security checklist, 16 Australian banks were selected [2].

IV. SECURITY THREATS

Below are the current threats to Indian Banking which we have discovered so far and we are looking forward to including more recent threats and security incidents in this section.

1. Identity Threat

Identity theft occurs when an adversary or an intruder forges someone else's identity by obtaining information about the person illegally. This information may include Aadhaar card number (UID), account number; credit/debit card number, PAN number etc. attacker can use this information to initiate any illegal financial transactions on the client's name or may even open a new account on the client's name. These threats are most common and can be easily avoided by following certain simple steps like not sending identity information on public channels like email or an SMS, never perform any financial transaction on a public system, shred expired documents that are no longer in use.

2. Phishing

Phishing occurs when the attacker tries to get client's personal information by appearing to be someone else through the phone call or an email. The attacker tries to get the sensitive data of the customer by forging bank's identity. Many times fraudsters pose as bank officials to get client's personal information. Phishing is categorized in two types: Vishing and Smishing. Vishing is where the attacker poses to be the employee of the bank or other financial institution to get personal information. Smishing is used by the attacker to send SMS to the client which contains some hyperlink, which if clicked would take the client to hacker's website or may download some virus on customer's device. In July, 2016 Union bank faced a major crisis, where $171 million was transferred from its bank account due to phishing.

3. Sim swap

In this threat, the attackers try to get the SIM card issued against the customer's name. It is the way for an attacker to get control of the cell phone communications of the target. The attacker can thus carry out any number of fraudulent transactions using the target's mobile number. To prevent this fraud, IMEI number of the phone should not be shared, also customer service provider should be contacted immediately if there is some indication of SIM swap.

4. Money mule

Money Mules are typically known by the name of 'smurfer' is a third party who transfers money from the client's account either online or through the courier service. The smurfer with the bank accounts are typically hired online and receive money through cheque deposits or through online transfer. When caught, the bank accounts for the money mules are suspended which causes financial loss. Many times the contact and the address of the money mules are found to be fake which makes it difficult to locate them [7].

5. Trojan

This is one of the earliest and common ways of attack. Trojan is a piece of software which may contain malicious code, which if runs may lead to deletion of files, data theft, or leaking some personal information. Victims fall prey to Trojan by clicking the infected links either on social networking sites or by downloading malicious software into their systems. According to Symantec report 2015, India is ranked 3rd for countries with most number of financial Trojan infections [8].

V. METHODOLOGY

We are deploying a comparative analysis approach by applying a qualitative research method. This comparative analysis will be conducted by examining the availability of Internet banking security features of the selected Indian banks. In order to fulfill the agenda of this paper, 5 Indian banks have been selected as they provide a good set up for the analysis of the proposed security checklist. We are currently focusing on security systems in five leading banks of India namely HDFC, ICICI, YES, IDBI and Axis bank.

Sample:

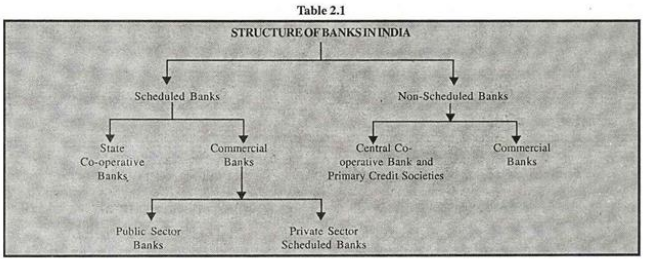

Figure 4: Structure of Banks in India.
Source: Wikipedia

There are currently 27 public sector banks and 30 private sector banks in India. For the purpose of analysis, we have selected 4 private commercial banks and 1 Public sector bank as this

provides a good setting for comparative analysis. The list of Indian banks used for analysis is displayed below:

Table 1: List of Indian banks used in analysis

S.No.	Name of Bank	Headquarter
1.	ICICI Bank	Mumbai
2.	HDFC Bank	Mumbai
3.	YES Bank	Mumbai
4.	OBC	Gurgaon
5.	Axis Bank	Mumbai

Data Collection:

Data has been sourced from secondary data points which are freely and easily available on the banks' websites. This data has been used to measure the internet banking security features. Internet banking security checklist has been drafted to evaluate the security features of the selected Indian banks. The results and findings of the security features according to the checklist can be used as a benchmark to improve the performance in the relevant security aspect. The checklist is enlisted and explained in detail in further sections.

Table 2:Six main security feature categories used for analysis

General online security and privacy information to the internet banking customers	• account aggregation or privacy and confidentiality • losses compensation guarantee • online/internet banking security information • bank security mechanism system
Information Technology (IT) assistance, monitoring and support	• Hotline/helpdesk service availability
Software and system requirements and settings information	• Compatibility with the popular Internet browsers on Desktops • Compatibility with the popular Internet browsers on Mobile phones • Availability/Recommendation of Security Software to the Internet banking customers
Bank site authentication technology	• employed encryption and digital certificate technologies
User site authentication technology	• two-factor authentication for logon and/or for transaction verification available • login requirements • failure limitation • user input type • scramble an on-screen input keypad • password restriction/requirement • transaction verification
Internet banking security features	• automatic timeout feature for inactivity • limited default daily transfer amount to third party account/BPAY/international transactions • logging information • notifications and alerts • session management
Mobile Application Technology	• Application availability • Login requirements for app • Mobile number on login device • Parallel login sessions on mobile app and desktop • Biometric authentication/fingerprint sensors • Session Management • Additional security measures

Analysis:

Category 1: General online security and privacy information to the Internet banking customers

1.1 Account aggregation or privacy and confidentiality: This section investigates the aggregation policy followed by the bank. Aggregation allows banks to consolidate account information from several sources into one location for the ease of the customer. An aggregator works by collecting the usernames and passwords that clients use to enter into their accounts. This allows banks to deepen their trust relationship with the customer. Also, the privacy and confidentiality of user's data must be ensured by the bank and the banks also must comply with the laws and regulations in protecting the confidential information

1.2 Losses compensation guarantee: This section investigates that whether the banks provide any kind of compensation against any financial losses faced by the client in case any unauthorized transaction occurs on client's account by someone other than the customer.

1.3 Online/Internet banking security information: This section examines whether or not the information regarding various security threats, guidelines to manage finances online is provided by the bank. These include the basic tips to make any financial transactions online and the risks associated with it.

1.4 Bank security mechanism system: This section investigates the measures the bank takes to implement security by implementing firewalls and Intrusion Detection System which enhance the security of the user's data.

Category 2: IT assistance and support

This section consists of the support and assistance provided to users by the banks. This includes customer care support or any kind of assistance being offered via the bank's website. This evaluates the channels and types of assistance offered via the Help or contact us webpage of each website.

2.1 Hotline/helpdesk service availability: This subsection investigates the bank's websites to check the helpdesk and hotline service options available to the customers or the users. This evaluates the number of communication channels offered by banks to internet banking customers to provide assistance. Most common methods are via Telephone/Customer care, Email, Service Request portals, Chatbots, FAQ's and Write to Us options. The most innovative feature uncovered here is providing customer support via social media accounts such as official Facebook and official Twitter handle.

Category 3: Browser compatibility on different devices and Security Software availability:

3.1 Compatibility with the popular Internet browsers on Desktops: This subsection researches the competency of the banks' Internet banking systems in regard to their compatibility with the most accepted Internet browsers such as Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, and Safari.

3.2 Compatibility with the popular Internet browsers on Mobile phones: This subsection checks the compatibility of the banks' Internet banking systems with regard to the most accepted Internet browsers such as Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, and Safari on different mobile devices. The main aim of this subsection is to check whether the mobile websites for selected banks work well enough on different devices to offer the internet banking services similar to desktops.

3.3 Availability/Recommendation of Security Software to the Internet banking customers: This part investigates whether the banks have provided any Internet security software tool or made recommendations to their consumers to reduce possible risks to the Internet banking customers' personal computers.

Category 4: Bank site authentication technology

4.1 Employed encryption and digital certificate technologies: In this section, we identify the authentication technologies used by the banks to implement SSL Secure Socket Layer, digital certificate technology, and Certificate authority. SSL is a security mechanism by which a browser establishes a secure connection with the server so as to reduce the risk to sensitive data over the public network. It authenticates the identity of the website and also transmits the data by implementing cryptography. For an SSL certificate to be valid, it must be signed by a Certificate Authority (CA) which verifies that a third party has authenticated the organization's identity.

Category 5: User site authentication technology: This section involves applying authentication techniques to identify users who interact with the bank website to manage the finances and carry out financial transactions. So, it is bank's responsibility to authenticate the users by applying various techniques. These involve:

5.1 Two-factor authentication for login and/or for transaction verification available: Two-factor authentication is a two-step verification method to authenticate the users by adding an extra layer of security on the basis of something that only the user knows or user possesses. This method doesn't rely only on the username and password to authenticate the user but also on something that is only known by the user. This can be an OTP (One Time Password), which may be generated through an SMS or on call, and is valid for a specific duration of time after which it becomes invalid. This can also be any Secure Access Image and a particular pre-specified Message that user may verify before logging in. Two-factor authentication makes the transaction much more secure and can help in detecting the phishing attacks which directs users to the attacker's website.

5.2 Login requirement: This section recognizes the requirements to log in to the bank website. The login requirements may include specifying an email address, phone number of the customer along with the username which is known to both the bank and the user. Then it may involve specifying information which is known only to the user such as card number, pin number, password or answers to the secret security questions. Also, user site may also request the user to fill in the CAPTCHA to make sure that the user trying to log in is not a robot.

5.3 Failure limitation: This includes specifying how many attempts any user can make trying to log in to the account. If a user exceeds the maximum number of attempts, the user's account may get locked and user's id and password may get disabled. In such a case, the user then has to walk into the bank or can generate the login information online by proving their identity. Generating a new password may take few hours to get generated, which may slow down the attacker's activity who may be trying to fraud the identity of the user.

5.4 Log In user input type: This subsection spots the input type required to log in to a bank's internet banking website. Generally, input information from a keyboard is required to log in to the internet banking website. However, this may be improvised to include input from another device such as mouse pad or keypad.

5.5 Scramble an on-screen input keypad: This subsection checks whether the virtual keyboard feature provided by bank website changes at every new login session through a scramble feature which alters the order of keys on the virtual keyboard. Protection from keylogger attacks, which steal the customer's

keystroke information such as login id and password without their knowledge, can be provided by shuffling of keys on the virtual keyboard of the Internet banking customers. This is checked individually for customer ID or user ID login field and password field.

5.6 Password restriction/requirement: This clause probes the restrictions and requirements imposed on creating passwords for customer accounts of Internet banking. This includes but is not limited to the minimum and maximum length for a password, alphanumeric requirement for passwords, case sensitivity of characters, mandatory or restricted use of special characters, limitation on using old passwords and providing users with a password strength measurer while creating or changing passwords. This section also checks the validity of the password where the password may also expire after a specific duration of time, after which user may be prompted to update/reset a new password.

5.7 Transaction verification: This subsection verifies whether verification is done by the bank when the user undertakes or initiates a transaction especially if it is an external transaction. Such verifications may include methods such as SMS, unique identification numbers, transaction passwords etc.

Category 6: Internet banking security features

This section focuses on the remaining security features provided by the bank for internet banking activity.

6.1 Automatic timeout feature for inactivity: The bank's system timeout the session of the customer due to the prolonged inactivity by the user. This security feature protects user's data from any unauthorized person from viewing the account information while the system is unattended. This automatically logs out the user from their account after the specified period of time if the user stays inactive during that time.

6.2 Daily Transfer limit on external transaction amount: This subsection looks for whether or not a maximum limit has been imposed on the currency and denomination value of a daily transaction amount that a user can transfer externally from his account. This subsection aims to verify that banks impose a daily amount limit on external fund transfers.

6.3 Logging information: This subsection investigates whether previous Internet banking login details are available to the Internet banking customers. Generally, the login activity details include last login date and time. Additionally, last account activity details may be provided such as browser details and I.P address and country of the last login. This may be used as a check by the customers to ensure that their activities are regular and usual.

Category 7: Mobile Application Banking

This section examines the security features deployed by banks to secure their mobile application banking services. This section investigates the most basic but essential features of mobile applications provided by the banks to access net banking.

7.1 Application availability: This subsection checks whether the bank provides a mobile application for android play store or apple store through reliable sources. The aim is to check the availability of net banking services via secure mobile banking applications.

7.2 Login requirements for the app: This section explores the login requirements to log in to each mobile banking application. Login requirements include a combination of customer ID and password, or user id, password and security image access or security code.

7.3 Mobile number on login device: This section investigates whether the mobile banking application allows a user to login to his account if the sim card for the registered mobile number is not present in the device through which the user attempts to log in. This is a security measure which is often overlooked by mobile applications but is essential for mobile banking applications.

7.4 Parallel login sessions on mobile app and desktop: This subsection examines simultaneous login into user's net banking account. This checks whether the bank allows similar services concurrently to the same user on multiple logins from different devices such as simultaneous login from a desktop bank website and another login via the mobile application.

7.5 Biometric authentication/fingerprint sensors: The market is now flooded with cell phones which provide biometric authentication by reading fingerprints. Banks can and should leverage this technological advancement to make mobile banking more safe and secure. This section explores whether or not the mobile banking applications have this feature incorporated to read fingerprint scan of the user for the user to login to his account.

7.6 Session Management: This section evaluates whether the mobile banks incorporate an idle timer system that logs out the user if the user remains inactive for a specified period of time. This security measure is one of the most important ones to make mobile banking safe.

VI. COMPARISON OF INDIAN AND CANADIAN BANKS

At present, there are 30 domestic banks in Canada, and 57 in India, which provides walk-in and online services to millions of users every day. Indian economy is one of the largest in the World, where Canada just comprises of mere 2.8% of total population of India. This makes it more challenging for the Indian banks to provide enhanced security along with making their customer's experience more enjoyable and trouble-free. Listed below are major differences security features between the Indian and Canadian banking systems.

1. Storing session cookies

We surveyed few Indian and Canadian bank websites and noticed a major difference regarding storage of session cookies. Indian bank websites don't allow storage of session cookies when the logged in user closes the current browser window, so the user is prompted to re-login with the credentials when the user again opens the bank's website. But in case of the Canadian bank website, users can access their account without the need to log in again. This is the major security vulnerability, if a user is using any public system directly closes the browser without logging off, the attacker can take the advantage and access the same user's session to carry out malicious activity.

2. Disabled Right Click Feature

Indian bank websites have disabled the Right-click features on the user account session once the user logs in on their website. When the user attempts to do Right Click on any link or drop down menu then a security message gets displayed stating that "Right Click has been disabled due to Security reasons". This is done mainly to prevent resubmission and avoid problems like double billing. This resolves the problem of duplicate sessions during the payment. However Canadian banks' websites offer the Right Click feature when the user is logged in to his bank account.

3. Saving Log-In Credentials

Surveyed Indian Bank websites do not offer to save the user credentials required to access the online account. There is no provision to store/save either of the fields such as User Id and password. Most of the surveyed Canadian banks offer the "Remember Me" feature for the User ID/Card number required by the user to access the online account. However, Scotia Bank, one of the major Canadian bank, allows the user to store both the user-id and password for the future log-ins.

4. Validating secure access image to log-in

The secure access image is a way to ensure that the customer is accessing the bank's website and not any phishing website. This reassures the user that they are not entering the details on any fraudulent website as the details of secure access image are known only to the user and the bank.

VII. CONCLUSION AND RECOMMENDATIONS

With the rise of new security threats, the security of the banking sector needs to be developed manifold. The surveyed Indian banks provide basic security features and mechanisms to keep user's data and transactions secure by implementing certain layers of security. All the surveyed banks websites include a security policy, which alerts users regarding the ways to safeguard their online banking activity. Security issues include updating the minimum technology standards for firewalls, verification of digital signature, implementing encryption/ decryption etc. by banks [11].

Additionally, users need to stay updated with the security policies to ensure secure transactions. Also, Banks should take actions to increase user awareness. This can be achieved by displaying security/ safe login tips to users at the time of user login. The user should check that the web addresses begin with https which ensures that the information being transmitted is encrypted and has a valid SSL certificate. They can also look for security symbols such as the lock symbol used by browsers to verify that the website being accessed is secure. The user must change their passwords regularly and should use different passwords for different accounts. Users should make sure not to carry out their banking transactions on the public computers and use a secure password protected internet connection to carry out their financial transactions online. The user can add a layer of protection by installing a good anti-virus and firewalls software which can protect against malware and Trojans.

Banks should also continually review and update their security policy and should ensure its implementation. Banks should upgrade their security mechanism to include new features to their security implementation such as biological detection tools such as biometric scan, retina scan, face recognition etc. Also, regular surveys should be conducted by the bank to stay updated with the security issues faced by the users. Every bank should have a dedicated department of cybersecurity officials to enforce security mechanism and provide support if any security emergency occurs.

The Government should enforce legislation to fine the banks in case banks are not able to properly implement the security mechanisms to keep the user's data and transactions safe.

VIII. ACKNOWLEDGEMENT

We would like to thank P. Subsorn, [2][3] and S. Limwiriyakul, for their detailed research and analysis on the security of internet banking of Australian and Thai Banks. Their multiple research papers form the core of this analysis paper. Taking inspiration from their work, we have conducted a survey on similar lines on internet banking of selected Indian banks. However, the idea of analysis of the security of internet banking based on the checklist is their brainchild and we have gratitude to their research in this regard as it proved as an invaluable asset for our paper.

Table 3: Summary of internet banking checklist for Indian banks

	Security feature categories	ICICI Bank	HDFC Bank	YES Bank	AXIS Bank	OBC
1.	General online security and privacy information to the Internet banking customers					
1.1	Account aggregation or privacy and confidentiality					
1.1.1	Complies with the Privacy Principles and Data Protection law	✓	✓	✓	✓	✓
1.2	Losses compensation guarantee					
1.2.1	100%					
1.3	Online/internet banking security information					
1.3.1	Threats: Hoax, email, scam, phishing, spyware, virus and trojan	✓	✓	✓	✓	✓
1.3.2	Keylogger	✓	✓	NI	NI	NI
1.3.3	General online security guidelines	✓	✓	✓	✓	✓
1.3.4	Security alert/ up-to-date issue	✓	✓	✓	✓	✓
1.3.5	Provides password security tips	✓	✓	✓	✓	✓
1.4	Bank security mechanism system					
1.4.1	Antivirus protection	✓	✓	NI	✓	✓
1.4.2	Firewalls	✓	✓	NI	✓	✓
1.4.3	IDS alert system	✓	✓	NI	✓	NI
1.4.4	Other	✓	✓	✓	✓	✓
1.4.5	No information					
2	IT assistance, monitoring and support					
2.1	Hotline/helpdesk service availability for internet banking customer					
2.1.1	24/7 customer contact centre by phone OR	✓	✓	✓	✓	✓
2.1.2	Not 24/7 customer contact centre by phone					
2.1.3	Social Media	✓	✓	✓	✓	✓
2.1.4	E-mail	✓	✓	✓	✓	✓
2.1.5	FAQ/online support form	✓	✓	✓	✓	✓
3	Software and system requirements and settings information based on the bank website's information					
3.1	Compatibility "best" with the popular internet browser					
3.1.1	Google Chrome	✓	✓	✓	NI	✓
3.1.2	Firefox	✓	✓	NI	✓	✓
3.1.3	Internet Explorer	✓	✓	✓	✓	✓
3.1.4	Netscape	✓	NI	NI	NI	NI
3.1.5	Opera	✓	NI	NI	NI	NI
3.1.6	Safari	✓	✓	✓	✓	✓
3.1.7	No Information					
3.2	Internet banking user device system and browser setting requirement					
3.2.1	Operating System	✓	✓	✓	✓	
3.2.2	Type of Browser	✓	✓	✓	✓	✓
3.2.3	Browser setting (e.g. cookie, pop-up windows)	✓	✓	✓	✓	✓
3.2.4	Screen Resolution	✓	✓	✓	✓	NI
3.2.5	No Information					
3.3	Free/paid security software/tool available to the internet banking customers					
3.3.1	Antivirus/ Spyware	×	×	×	×	×
3.3.2	Internet security suite	×	×	×	×	×
3.3.3	Provides internet links/ information to security software vendor(s)	×	×	×	×	×
3.3.4	No Information					
4	Bank site authentication technology					

4.1	Employed encryption and digital certificate technologies					
4.1.1	SSL 128/168-bit encryption OR	A2	A2	E	E	R
4.1.2	SSL 256-bit encryption					
4.1.3	Extended validation SSL certificates	✓	✓	✓	✓	✓
4.1.4	Signing CA	✓	✓	✓	✓	✓
5	User site authentication technology					
5.1	Two-factor authentication for transaction verification available					
5.1.1	Token device (no. of digit pins) OR	×	×	×	×	×
5.1.2	SMS (no. of digit pins) OR	✓	✓	✓	✓	✓
5.1.3	Secure Access Image	×	✓	×	×	✓
5.1.4	Not in use					
5.2	Logon Requirement					
5.2.1	Bank/credit cards number or bank register/customer ID or email address	✓	✓	✓	✓	✓
5.2.2	Password/ personal code or security number	✓	✓	✓	✓	✓
5.2.3	Others (e.g. CAPTCHA, security question)	×	✓	×	×	✓
5.2.4	Two-factor authentication	×	✓	×	×	✓
5.3	Logon Failure Limitation					
5.3.1	Standard max. (3 times) OR	✓				
5.3.2	Max. more than 3 times OR		✓	✓	✓	
5.3.3	In use but does not specify maximum number of failure allowed			✓		
5.3.4	No Information					
5.4	Logon user input type					
5.4.1	Keyboard AND/OR	✓	✓	✓	✓	✓
5.4.2	Keypad	✓				
5.5	Scramble an on-screen input keypad					
5.5.1	Customer ID	✓				
5.5.2	Password	✓	✓	✓	✓	✓
5.6	Password restriction/requirement					
5.6.1	Enforce good password practice	✓	✓	✓	✓	✓
5.6.2	Password/pin length (minimum)	✓	✓	✓	✓	✓
5.6.3	Combination of numbers and letters	✓	✓	✓	✓	✓
5.6.4	Combination of upper and lower cases	✓	×	✓	✓	×
5.6.5	Special Characters	✓	✓	✓	✓	✓
5.6.6	Different passwords as compared to any of three previous used passwords	NI	NI	✓	NI	NI
5.6.7	Cannot have three or more of the same characters in a row (e.g. aaa, 111)	NI	NI	NI	NI	NI
5.6.8	Cannot have three or more of the consecutive characters in a row (e.g. abc, 123)	NI	NI	NI	NI	NI
5.6.9	Automatically check password strength when creating or changing password	✓	✓	✓	✓	✓
5.6.10	No Information					
5.7	Transaction verification					

5.7.1	External transactions required token/SMS/extra password	✓	✓	✓	✓	✓
5.7.2	Not Required					
5.7.3	No information					
6	Internet banking application security features					
6.1	Automatic timeout feature for inactivity					
6.1.1	Max. (mins) OR					
6.1.2	In use but does not specify timeout length	✓	✓	✓	✓	✓
6.1.3	No Information					
6.2	Limited default daily transfer amount to third party account/BPAY/international transactions					
6.2.1	Less or up to 2,00,000 INR					
6.2.2	More than 2,00,000 INR	✓	✓	✓	✓	✓
6.2.3	The default maximum daily limit transfer is vary depend on the type of the internet banking customer	✓	✓	✓	✓	✓
6.2.4	The default maximum daily limit transfer may be increased with the approval by the banks	✓	✓	✓	✓	✓
6.2.5	No Information					
6.3	Logging information and alert					
6.3.1	Last Login	✓	✓	✓	✓	✓
6.3.2	Activity Log	×	×	×	×	×
6.3.3	Alert available via E-Mail and/or SMS	×	×	×	×	×
6.3.4	No Information					
6.4	Session Management					
6.4.1	Use cookies	✓	✓	✓	✓	✓
6.4.2	Use Page Tokens OR	NI	NI	NI	NI	NI
6.4.3	Use Session Tokens					
6.4.4	Use cookies for other purposes (e.g. marketing)	×	NI	NI	NI	NI
6.4.5	No Information					
7	Mobile Application Technology					
7.1	Application availability	✓	✓	✓	✓	✓
7.2	Login requirements for app	✓	✓	✓	✓	✓
7.3	Registered Mobile number on login device	✓	×	×	✓	✓
7.4	Parallel login sessions on mobile app and desktop	NI	NI	NI	NI	NI
7.5	Biometric authentication/fingerprint sensors on supported devices	×	×	✓	×	×
7.6	Session Management	✓	✓	✓	✓	✓

✓ represents yes
* represents optional
NA represents not applicable
NI represents no information
A1 represents AES 256-bit encryption
R represents RC4 128-bit encryption
A2 represents AES 128-bit encryption
D represents 3DES-EDE-CBC 168-bit encryption
E 128 bit encryption(no other information)
V represents VeriSign Authentication Services

REFERENCES

1. C. Wueest, "Internet Security Threat Report", *Symantec.com*, 2017. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf
2. P. Subsorn and S. Limwiriyakul, ""A comparative analysis of the security of internet banking in Australia: A Customer Prespective"", *Ro.ecu.edu.au*, 2011. [Online]. Available: http://ro.ecu.edu.au/icr/25/
3. P. Subsorn and S. Limwiriyakul, "A Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective", 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877705812012970
4. G. Sharma, "Study of Internet Banking Scenario in India", *Ermt.net*, 2016. [Online]. Available: https://www.ermt.net/docs/papers/Volume_5/5_May2016/V5N5-138.pdf.
5. V. Chauhan and V. Choudhary, "Internet Banking : Challenges and Opportunities in Indian Context", *Apeejay.edu*, 2015. [Online]. Available: http://apeejay.edu/aitsm/journal/docs/issue-june-2015/ajmst020305.pdf.
6. R. Lal and R. Saluja, "E-BANKING: THE INDIAN SCENARIO", *Indianresearchjournals.com*, 2012. [Online]. Available: http://indianresearchjournals.com/pdf/apjmmr/2012/december/2.pdf.
7. "RRBs - Operation of bank accounts & money mules", *Rbi.org.in*, 2010. [Online]. Available: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=6167&Mode=0.
8. C. Wueest, "Financial threats 2015", *Symantec.com*, 2015. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/financial-threats-15-en.pdf.
9. https://scroll.in/article/809228/three-charts-show-how-mobile-wallets-are-exploding-in-india-but-plastic-cards-are-still-ahead
10. http://www.financialexpress.com/industry/banking-finance/online-banking-users-in-india-to-reach-150-billion-by-2020-according-to-a-study/731048/
11. R. Jassal and R. Sehgal, "Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example", *Iosrjournals.org*, 2013. [Online]. Available: http://www.iosrjournals.org/iosr-jce/papers/Vol13-issue1/R0131114121.pdf?id=7416.