Concordia Institute for Information System Engineering
(CIISE)

Concordia University

INSE 6150 – Security Methodology Evaluations

Project Report:

Evaluation of Internet Banking Security

Submitted to:

Professor Jeremy Clark

Submitted By:

Nithish Reddy Yalaka – 40164619
Leela Gopinath Yadlapalli – 40162978

Abstract:

The Internet has its own intrinsic security issues as far as Integrity, confidentiality, and privacy. The principal effect of these sorts of issues is explicitly on the financial business as they have expanded their Internet banking offices to diminish costs and offer better types of assistance and banking accommodation to their Internet banking. Internet Banking has turned into the essential method of getting to banking administrations for most clients, yet its security is yet a consistent worry since millions of dollars are lost each year because of fraud and attacks. Over the long run, banks and clients conquer the underlying technological distrusts and figure out how to get their tasks done. In any case, there are yet numerous illustrations to learn, importantly when checking out the upcoming technological advancements. Online banking is perhaps the most delicate task performed by broad Internet users. Most traditional banks presently offer internet banking services, and firmly urge clients to do online banking with comfort and trust .' Although banks intensely publicize an obvious '100% web-based security ensure,' commonly the fine print makes this contingent on clients satisfying specific security necessities.

Online banking is progressively famous, and banks have effectively supported this expense saving trend by convincing clients to join. Customers, drawn in by internet banking's accommodation, appear to be generally uninterested regarding fraud and phishing email tricks. Indeed, most clients appear to accept that Internet banking is very protected just on the grounds that their banks told them so. Truly, this feeling of safety may be bogus. Notwithstanding, banking clients have not had a decision of Internet banking fundamentally because of the way that they have currently attached to whatever type of Internet banking that their present existing bank provides. we have gone through the literature of internet banking security systems employed in current banks in the world and came up with the internet banking security checklist which can benefit both existing potential internet banking customers as well as for the banks providing internet banking services to enhance their security standards with the proposed guidelines. we have also discussed possible vulnerabilities in the current web with banking system possible attacks defense mechanisms. Our examination shows that authentication was often feeble, offering straightforward—however incredible—attack possibilities. Here, we talk about the authentication strategies and the attacks they made conceivable. Our synopsis is based entirely on openly accessible Internet data. We argue that the technical aspects of security for ensuring internet-based banking systems can give adequate protection against threats. The issue is the discrepancy of assumptions between the customers and the banking system. There is a huge gap between the system's assumptions for customers and how customers can really manage with respect to security – customers don't have a single model of security. We mean to find design principles that address these dissimilar internet banking security framework assumptions together for a solid and usable framework. **[8]**

Introduction (Online Banking System):

Internet banking, otherwise called e-banking or online banking, is the service given by banking establishments to empower bank customers to go through with banking exchanges over the web. Internet banking can be led through an assortment of different devices and mediums. At the point when a user utilizes a mobile phone or other cell phone, the terms are explicitly called as mobile banking, m-banking, or cellphone banking. Internet security is a subset of computer security, and it is significant because specialized reports ordered by insurance organizations, risk and security associations based on their analysis show that online attackers and hackers target internet firms. The worry is generally with internet banking, which includes a user visiting a web-based banking site to sign in and direct banking-related operations. The customer can utilize any kind of device, be it a cell phone or a PC. Internet banking customers can go through with a diversity of transactions, for example, checking the account records, reserves move between accounts, bill payments, prepaid service payment and installments (power, broadcast appointment, and so forth), traffic fines installments.

With the approach of Internet advancements, the internet has turned into a huge component in pretty much every business and One of the main improvements in this area is the banking business. The Internet has the capacity to coordinate and change a customary business into a model of online business in giving financial other options and working with accommodation to their Internet banking users. Truth be told, most of the banks all over the planet have changed their business methodology to achieve serious advantages, lessen functional expenses and improve their exhibition by offering an Internet banking framework to their Internet banking clients. Thus, Internet banking clients have the choice of getting to their accounts and making exchanges whenever and anyplace. In any case, Internet banking frameworks have related data security vulnerabilities and dangers which can be evaluated as low, medium, and high. Security and privacy of Internet banking exchanges and confidentiality of individual information data are among the greatest worries for both the financial business and Internet banking clients .While liking the advantages that go with internet banking, customers neglect to understand that there are likewise liabilities that are a vital for this service. There is by all accounts an absence of lucidity on precisely what are the obligations of the customers and banks in the event of an internet security breach.

Online security is a main pressing issue for associations and their customers who lead business on the internet. Banking organizations observed that internet security is quite difficult and challenging for online organizations. Absence of trust and security risks are main pressing issues for customers embracing internet buying and doing web-based banking. Security configurations assumes a significant part, particularly in applications where security isn't the essential task. Specifically, overlooking human limits in the plan of safety frameworks brings non-compliance towards security prerequisites. Human feelings assume a part in how clients collaborate with information system and frameworks, and architects of those systems need to think about the importance of human emotions. In this way it is prescribed to take human limits, for example, restricted memory-load capacity and human feelings into account in system design plan, since the substance of individuals' knowledge, including their speculations and convictions, can be a significant logical idea for understanding customers conduct corresponding to system. Accomplishing complete security is not possible. Humans have for quite some time been viewed as the most vulnerable connection in the security chain of Information Security Systems. Be that as it may, even with the best specialized security components, a security framework's most vulnerable connection will in general be the human. The primary test is acquiring the client get tied up with perform security errands and implanting their conduct into a safe culture and climate.

Adware, keylogger, malware, phishing, spyware, Trojans, and the viruses are the most widely recognized Internet banking security dangers and threats. Moreover, there are some extra Internet banking security dangers and risks that sway both the banks and the Internet banking users. These incorporate security familiarity with the Internet banking users and the banks, Internet banking clients' web-based behavior, risks (both validation and authorization), openness to new possible dangers, Internet banking users confidence in the Internet banking framework, the versatile financial security issue, secured against man-in-the-middle attack and man-in-the-web browser attack, identity or information data theft obtained from social media platforms, healthcare services and government gateways utilizing just a single factor authentication. These elements can possibly impact conventional baking clients from changing to online banking.

Hence, the fundamental motivation behind this report was to examine the security of Internet banking frameworks by utilizing a comparative analysis approach in creating a proposed online banking security checklist. This agenda could then be possibly used to assess their online banking security frameworks dependent on the online banking data. Accordingly, the potential Internet banking clients can be equipped with a security foundation and a thought of online banking security before picking a bank to initiate online banking. Then again, the current banking customers can utilize this checklist to distinguish their own security shortcomings and better secure their online banking experience.

Attacks on Internet Banking System:

Innovative threat evaluation techniques for systems and software are needed, relating to security trends and developments over the last decade, where reported vulnerabilities and incidents have increased significantly, and attacks are constantly becoming more sophisticated while requiring less intruder knowledge. Several novel techniques for threat modelling have emerged in recent years. Online banking is being used more frequently to support and improve the operations and management of the banking industry. We have simple access to banking services thanks to online banking systems. People can connect to the bank's computer system through the Internet using a more sophisticated and user-friendly interface, a browser, or a specific standalone application. As a result of this growing tendency, security issues such as confidentiality, integrity, and privacy have become increasingly important in online banking systems for both banks and users.

The study of risk assessment and threat mining in the online banking system has gotten a lot of attention. The security of today's online banking systems is discussed in this report. The STRIDE threat model in a system threat analysis method. We developed the online banking system threat model by using this threat analysis method to the threats analysis of the online banking system. We begin by analyzing the important business online banking system data flow diagram, followed by the construction of a STRIDE threat model to detect threats, reduce the complexity of online banking system threat analysis**[6]**. It is critical to the security analysis and risk evaluation of online banking systems, as well as the deep mining of their vulnerabilities and threats. Some of the common attacks on the banking system are:

1. **Man in the Middle Attack (MITM)**:

The Man in the Middle Attack occurs when an attacker blocks messages in key exchange and then retransmits them, substituting his own key for the specified one, so that the two distinct parties appear to be communicating with one another.

E.g.: Let's pretend you get an email from your bank asking you to log in to your account and confirm your contact details. You open the email and follow the link to what looks to be your bank's website, where you log in and complete the task. The man in the middle (MITM) sent you the email in this case, making it appear legitimate. (Phishing is used in this assault to get you to click on an email that appears to come from your bank.) He also built a website that appears exactly like your banks, so you won't hesitate to enter your login details after clicking the email's link. However, you are passing up your credentials to the attacker rather than logging into your bank account.

MITM attacks can be launched from any point along the communication path between a client and a server, from the customer's PC to adjacent system gadgets, such as remote passageways to distant switches, for example, by using forged IP addresses. MITM attacks can be passive, in which the attacker just listens in on the traffic flowing between the customer and the server to use the information later, or dynamic, in which the attacker can limit or alter the communication. Public key infrastructure is used in this system.

With the MITM attack, the affected STRIDE categories are Spoofing and Escalation of Privilege resulting in the violation of Authentication and Authorization property respectively. Attackers can utilize the MITM attack to gain control of devices and then exploit the system in a variety of ways such as IP Spoofing, Stealing browser cookies, SSL Hijacking, Wi-fi eavesdropping, Email Hijacking, HTTPS Spoofing, DNS Spoofing.

2. Credential Stuffing Attack:

Credential stuffing is one of the most popular methods of credential theft. Credential stuffing is an automated attack that uses bots to test millions of stolen login and password combinations on a targeted website or application. It is a sub-vector of brute force attacks. Because many users' login information has been stolen due to breaches over the years, the security sector is experiencing an enormous spike in credential stuffing assaults. Attackers rely on the reuse of these credentials across various applications and websites, and they usually bring in a lot of money.

Stolen account credentials, such as usernames and passwords, are used in this sort of cyberattack to gain illegal access to accounts via large-scale automated login requests. These lists are made public because of data breaches and are frequently acquired on the dark web. This type of fraud does not require the use of password guessing software. Using typical online automation tools, a hacker can log thousands to millions of broken passwords and usernames in an automated process. Using various passwords for different accounts is the best approach to protect yourself from this type of attack. Even obsolete data must be carefully maintained since hackers can still discover methods to exploit it.

3. Phishing Attack:

Phishing is the illegal act of impersonating a trustworthy entity and employing social engineering techniques to obtain sensitive information such as usernames, passwords, and credit card information. With Phishing attacks, the affected STRIDE categories are Spoofing resulting in the violation of Authentication.

Phishing attacks utilize a combination of social engineering and technical methods to mislead users and acquire sensitive data and banking account passwords. A surge in phishing schemes targeting bank personnel in the hopes of obtaining sensitive information such as usernames and passwords." The main goal is to persuade bank personnel to open attachments or click on links that lead to fraudulent websites. They are urged to give their login passwords and other sensitive data there. With access to an employee's email account, cyber attackers can read a bank's essential information, write emails on the bank's behalf, hack into the employee's bank and social media accounts, and gain access to internal papers and client financial information.

Spear phishing, Phone phishing, clone phishing, whaling, and Pharming are some of the common phishing techniques.

Employee training is the most effective strategy to counteract phishing attacks, as it teaches employees how to recognize these communications and how to respond to them, which includes not clicking on any links and informing IT personnel.

Security Evaluation Metrics

Based on the existing literature, the security checklist proposed by Subsorn and Limwiriyakul are used as the best evaluation criteria when it was published in 2011 and a few years later Alsaleh, Alarifi, Alshaikh and Zarour used those as building blocks and improvised the security criteria according to a technology improvement, time, fixed vulnerabilities in banks, new security issues and large base of internet banking customers. According to our review the approach followed by **[2]** will be apt to consider for evaluating the existing real-world banks, this is because the customer base and number of banks is increased now, so the new vulnerabilities and using their approach of further narrowing down each security property into set of metrics will provide the better results than the security checklist that was proposed by Subsorn and Limwiriyakul **[1]**. According to our literature review the following properties proposed by [1] plays a major role in determining the security of the internet banking system. Banks provide and offer six major security feature categories to their Internet banking customers. These include (1) general online security and privacy information for Internet banking customers, (2) IT assistance, monitoring, and support, (3) software and system requirements and settings information, (4) bank site authentication technology, (5) user site authentication technology, and (6) Internet banking application security features. Each security category has different security properties take into consideration by Subsorn and Limwiriyakul.

Based on our literature review we found that this evaluation by **[1]** is the standard criteria used to evaluate the security issues, but there was an upgraded version of evaluation framework which was built upon this standard criterion of Subsorn and Limwiriyakul. We referred to that research of Alsaleh, Alarifi, Alshaikh and Zarour **[2]** and in our review we found that it was further narrow down into each of the security property with more metrics into consideration. So that when we evaluate the internet banking system security, we will get the better analysis on each metric using framework proposed by **[2]** instead of the generalized analysis for each property in the security criteria which is performed by **[1]** and Research of **[2]** helps us to get the better results in assessing both security and privacy features that are missing or incorrectly implemented and provide external validity for other related sectors or organizations to use as a guideline for improving their own Internet banking security system performances.

Each of these security feature categories with different security properties is explained in detail below and with metrics is shown in the Appendix.

Security feature categories with different Security properties: -

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

This section includes the following security properties and these properties proposed by **[1]** are considered best amongst the other literatures as per our review:

a. Account aggregation or privacy and confidentiality:

This property investigates the current privacy and confidentiality policies that banks offer to their Internet banking customers. To ensure the integrity of Internet banking customers' confidential data, the policy must comply with privacy laws and incorporate the National Privacy Principles. Banks must also comply with any legal or regulatory obligations in their stipulation when it comes to use and disclosure.

b. Losses compensation guarantee:

This property investigates the banks' current guarantee policy, which requires the banks to cover any losses incurred because of unauthorized transactions made by someone other than the customer using the customers' Internet banking accounts.

c. Online/Internet banking security information:

This property examines the Internet security data which is given by the banks to their Internet banking clients. These cover significant and related Internet banking security data like threats, security rules and tips.

d. Bank security mechanism system:

This property attempts to determine whether banks provide information on their Internet banking security systems, such as firewalls and intrusion detection systems (IDS), which have the capability of enhancing Internet banking customers' privacy and confidentiality.

2. IT assistance, monitoring and support: -

This section includes the following security properties and **[1]** defined these better than **[2]**:

a. Hotline/helpdesk service availability:

This property tries to search the banks websites for information about an IT hotline or helpdesk support for Internet banking customers. Ideally, banks should offer several modes of communication to their Internet banking customers. Some of the most common communication methods are phone calls and secure email.

b. Internet banking transaction monitoring by the banks:

This property investigates whether banks have their own dedicated teams for monitoring potentially suspicious transactions on their Internet banking systems.

3. Software and system requirements and settings information: -

This section includes the following security properties and these properties proposed by **[1]** are no longer valid because at present as per our research all internet banking sites are compatible to almost all browsers and there aren't any browser settings need to be pre-configured neither screen resolution requirements:

a. Compatibility "best" with the popular Internet browsers:

Based on the information provided by the banks, this property determines whether the banks Internet banking systems support or are compatible with the world's most popular Internet browsers, including Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, and Apple Safari.

b. Internet banking user device system and browser setting requirement:

This property examines the operating systems, browser settings, and screen resolution requirements information provided by banks for optimal usage.

c. Free/paid security software/tool available to the Internet banking customers:

This property is considered in determining whether banks have provided optional Internet security software or tools to their customers to reduce any significant threats to the personal computers of Internet banking customers **[1]**.

4. Bank site authentication technology: -

This section identifies the bank authentication technology that is currently used to cover types of secure sockets layer (SSL) encryption, digital certificate technology, and certificate authority (CA). SSL encryption creates an encrypted link between the banks' web servers and the Internet banking customers' browsers, allowing both parties to communicate privately and securely. At present all banks are using Extended Validation SSL Certificates because it offers a high-security Internet browsers information to clearly identify a Web site organizational identity as defined by **[2]**.

5. User site authentication technology: -

This section is focused with determining the authentication mechanism that Internet banking customers use to authenticate with banks. The framework entails the determination of the implemented authentication technology in the web portal (e.g., login mechanism, login requirements, login procedures, failure restriction, and transaction verification) as well as the properties of the secure connection between a client's host and the bank server. The framework also checks to see if the bank supports multi-factor authentication and can provide a high degree of identity validation. It includes the following security properties:

These properties defined by **[1]** during 2011 are still up to the standards of current internet banking infrastructure and Metrics defined by **[2]** for each property will gives us the better results.

a. Two-factor authentication for logon and/or for transaction verification available
b. Logon requirements
c. Logon failure limitation
d. Logon user input type
e. Scramble an on-screen input keypad
f. Password restriction/requirement
g. Transaction verification

6. Internet banking application security features: -

Internet banking applications are also evaluated against a set of criteria designed to reduce the risk of security breaches and remote harmful assaults like worms and viruses. For example, one of the investigated security features is automatic timeout for inactivity, which establishes a default inactivity period after which the online client is signed out.

Session management is also assessed in terms of safeguarding transaction execution throughout online banking sessions, such as session tokens and page tokens technologies, as well as clearing the appropriate cookie information in the user browser once the client signs off or closes the Internet browser. To mitigate the threat of impersonation attacks, the default allowable transfer amount should be lowered and linked with two-factor authentication. It includes the following security properties:

These properties along with the metrics proposed by **[2]** will give us better results while evaluating this security feature when compared to **[1],[3]**.

a. Automatic timeout feature for inactivity
b. Limited default daily transfer amount to third party account/BPAY/international transactions
c. Logging information
d. Session management

Analysis and Findings of Security Evaluation Metrics on real world Banks

Based on the existing literature of **[1]**, **[2]** and **[3]** we have compared the security evaluation of internet banking on different banks in the world and gathered the important findings analysed from the evaluation framework and possible improvements for the banks to reduce the risk of security threats.

- Based on the banks involved in the case study done by **[1],[2],[3]**. We have analysed that almost all banks have shown compliance with the national privacy principles and laws as well as the customer protection code; when it comes to encryption and digital certificate, only half of the banks are deployed the extended validation SSL certificates. According to VeriSign Authentication Services, extended validation SSL certificate offers a high-security Internet browsers information to clearly identify a Web site organizational identity. While some banks still deploy SSL certificates with 256-bit encryption and the others with 168-bit encryption and 128-bit encryption. Upgrading to an extended validation SSL certificate and 256-bit encryption can give optimum security for bank site authentication while also increasing the security confidentiality of possible new Internet banking users. Almost All banks are not liable for any claim, loss, expenditure, delay, cost, or damage resulting from or related to any instruction, request, inquiry, or transaction made or effected where any user identity or password has been or is alleged to have been used by unauthorised people. An exception is when the bank's website is hacked or is viewed by an unauthorised user, in which case the bank is compelled to pay the clients after investigating the associated incident. Almost half of the banks do not fully provide 24/7 IT helpdesk via telephone support regarding Internet banking system issues. However, all the selected banks involved in case study provide online, FAQ and secured email supports **[1]**.

- For inputting a user ID, a bank registration ID, a bank card number, or an email address, all chosen banks require a keyboard as their primary input method. Some banks on their keypad, use a scramble mechanism. This implies that the keypad is reset each time the webpage is accessed. This strategy can help to limit the threats of unauthorized keystroke recording. We notice that only a few banks give enough information on threats, assaults, general internet security standards, security alert issues, and password security tips. However, there are certain technical phrases on the webpages that are solely intended for advanced users. Furthermore, all banks did not give their clients with information regarding key loggers, which may be used to obtain user identity and passwords.
- To prevent unauthorized users from undertaking online password guessing assaults, majority of the banks-imposed limits on the number of unsuccessful logins. Majority banks require customers to use a minimum of 8 digits that comprise both characters and numbers to increase password strength in terms of length, complexity, and unpredictability against online password guessing attacks. Users, however, were not subjected to rigorous password composition policies. In terms of session management, after logging out or closing the Internet browser, all banks delete the cookie information. In addition, all banks have a daily transfer limit to third-party accounts to mitigate the impact of fraudulent transactions. Furthermore, with certain banks, the international transfer limit is substantially lower than the national transfer limit **[2]**.
- There were similarities in the Internet banking systems based on simple information audits on the websites of the selected institutions. This might be because some banks function as subsidiaries of other parent banks. This explains that Internet banking technology is comparable. This has the advantage of reducing the difficulty of managing and maintaining two independent Internet banking systems. However, there may be a little risk to both banks if one of their partners Internet banking systems is compromised, exposing the other bank to infiltration.
- When a user loses or forgets her password, the banks password recovery processes differ widely. Although most banks require users to enter their ATM card number, ATM PIN number, and/or national ID number to change their passwords online, other banks need more stringent verification measures for password recovery. One bank sends an SMS with an automatically produced verification code to the customer's registered mobile number, and the user enters this verification code into the password reset form on the online banking site.
- Some banks even provide links to free and commercial antivirus and antimalware software to its customers. So that those tools mitigate against malware attacks **[1,2]**.

Recommendations to improve Internet Banking Security: -

Based on our literature review **[1]** has provided the mandatory improvements that banks should consider to be secured against possible attacks during 2011. Best of them are listed here as follows. But if **[1]** has done the same research now, they will notice that most of these recommendations won’t be applicable after looking into literature review of fellow researchers based on their topic and by analyzing the internet banking sites, **[1]** can understand most of these improvements stated below are already incorporated in the current internet banking and in this regard **[2]** gives us the current accurate research results when compared to **[1]**,**[3]** and it’s clear that all of these are implemented in most of the banks as per research conducted by **[2]**.

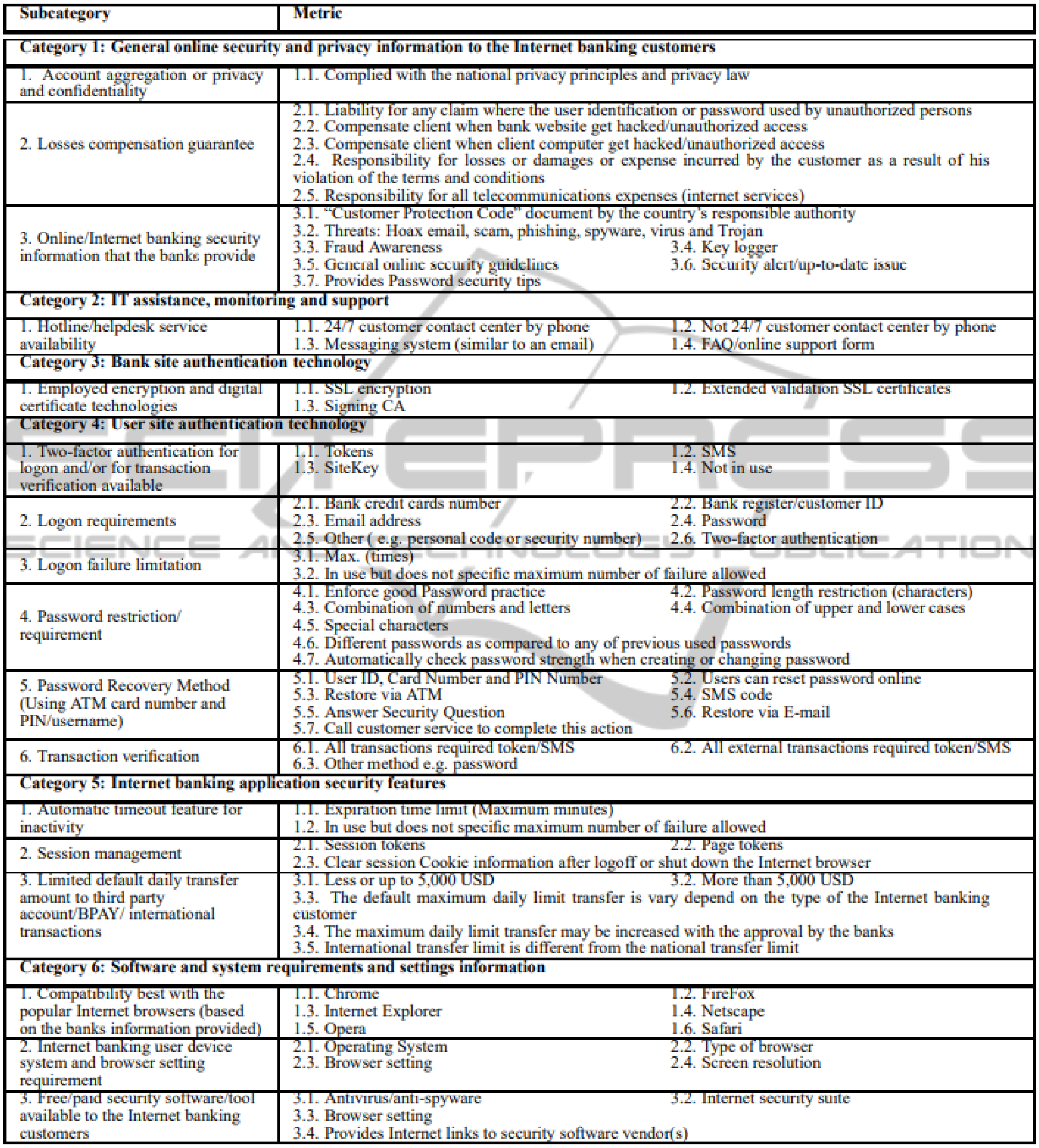
- All the banks have generally provided a standard Internet banking security system with certain optional security services to their Internet banking customers. However, these selected institutions should impose a required two-factor authentication mechanism for both login and transaction verification.

- To strengthen security in Internet banking systems, banks should implement and enforce a good and effective security strategy, as well as regulations enacted by local or state governments. Two-factor/multi-factor authentication systems, transaction verification, 256-bit encryption with extended validation SSL certificate, auto logout feature, suspicious activity monitoring, last login time display, account lockout, and audit trails are some examples of good and effective security policies that could be enacted.
- Banks can work with local and state government agencies to improve the confidentiality of online payment systems while also improving performance and providing better Internet banking security services such as personal information theft protection, personal financial information theft protection, identity fraud protection, and online crime protection.
- Banks that now use 128-bit encryption SSL should consider upgrading to 256-bit encryption. upgrading from a normal validation SSL certificate to an extended validation SSL certificate should be explored. These two enhancements have the potential to improve the secrecy of both present and prospective Internet banking consumers.
- Banks must be on the alert for emerging threats/risks such as phishing through SMS/text message, phishing over the phone, and SSL–evading Trojans. Furthermore, by conducting a survey and offering rewards for customer feedback, banks should be aware of their customers' demands, opinions, concerns, mistrusts, and/or expectations, such as their transaction activities monitoring, online and mobile threats concerns, and strong security methods for online activities. The responses to these surveys may be used to strengthen the confidentiality of both current and future Internet banking customers. Banks must also adequately educate and encourage their Internet banking consumers to become aware of the security threats/risks associated with Internet banking. Banks should also provide a link to download and/or update antivirus and Internet security software, as well as firewall measures.
- In the future, banks may consider deploying biological authentication tools such as finger and hand geometry, retinal scan, iris scan, fingerprint recognition, face recognition, voice recognition, keystroke recognition, and handwriting recognition to protect their Internet banking systems from attackers. Alternatively, banks may offer insurance to compensate clients for losses caused by possible Internet banking security threats/risks caused by unskilled Internet banking customers or a lack of their knowledge and/or awareness **[1]**.

Conclusion: -

Finally, based on our literature review we concluded that with in depth analysis of the each of the security property with set of metrics we can achieve better results in mitigating the security breaches, finding the existing vulnerabilities, find the defense mechanisms to possible attacks and finally developing a better evaluation framework to analyze the security of internet banking system so that customers can choose the secured banks and also useful for stake holders in banks to address the existing security issues and mitigate them with defense mechanisms and satisfy the customer requirements. Based on our comparative analysis most of the banks need to improve the security by performing the security evaluation using the proposed security checklist provided by the **[1],[2]** and getting the feedback by conducting a survey from the existing banking customers, stake holders and the operational entities. Using the effective evaluation framework there are no solutions, but we can always have the tradeoffs.

Appendix:-



Subcategory	Metric
Category 1: General online security and privacy information to the Internet banking customers	
1. Account aggregation or privacy and confidentiality	1.1. Complied with the national privacy principles and privacy law
2. Losses compensation guarantee	2.1. Liability for any claim where the user identification or password used by unauthorized persons 2.2. Compensate client when bank website get hacked/unauthorized access 2.3. Compensate client when client computer get hacked/unauthorized access 2.4. Responsibility for losses or damages or expense incurred by the customer as a result of his violation of the terms and conditions 2.5. Responsibility for all telecommunications expenses (internet services)
3. Online/Internet banking security information that the banks provide	3.1. "Customer Protection Code" document by the country's responsible authority 3.2. Threats: Hoax email, scam, phishing, spyware, virus and Trojan 3.3. Fraud Awareness 3.4. Key logger 3.5. General online security guidelines 3.6. Security alert/up-to-date issue 3.7. Provides Password security tips
Category 2: IT assistance, monitoring and support	
1. Hotline/helpdesk service availability	1.1. 24/7 customer contact center by phone 1.2. Not 24/7 customer contact center by phone 1.3. Messaging system (similar to an email) 1.4. FAQ/online support form
Category 3: Bank site authentication technology	
1. Employed encryption and digital certificate technologies	1.1. SSL encryption 1.2. Extended validation SSL certificates 1.3. Signing CA
Category 4: User site authentication technology	
1. Two-factor authentication for logon and/or for transaction verification available	1.1. Tokens 1.2. SMS 1.3. SiteKey 1.4. Not in use
2. Logon requirements	2.1. Bank credit cards number 2.2. Bank register/customer ID 2.3. Email address 2.4. Password 2.5. Other (e.g. personal code or security number) 2.6. Two-factor authentication
3. Logon failure limitation	3.1. Max. (times) 3.2. In use but does not specific maximum number of failure allowed
4. Password restriction/ requirement	4.1. Enforce good Password practice 4.2. Password length restriction (characters) 4.3. Combination of numbers and letters 4.4. Combination of upper and lower cases 4.5. Special characters 4.6. Different passwords as compared to any of previous used passwords 4.7. Automatically check password strength when creating or changing password
5. Password Recovery Method (Using ATM card number and PIN/username)	5.1. User ID, Card Number and PIN Number 5.2. Users can reset password online 5.3. Restore via ATM 5.4. SMS code 5.5. Answer Security Question 5.6. Restore via E-mail 5.7. Call customer service to complete this action
6. Transaction verification	6.1. All transactions required token/SMS 6.2. All external transactions required token/SMS 6.3. Other method e.g. password
Category 5: Internet banking application security features	
1. Automatic timeout feature for inactivity	1.1. Expiration time limit (Maximum minutes) 1.2. In use but does not specific maximum number of failure allowed
2. Session management	2.1. Session tokens 2.2. Page tokens 2.3. Clear session Cookie information after logoff or shut down the Internet browser
3. Limited default daily transfer amount to third party account/BPAY/ international transactions	3.1. Less or up to 5,000 USD 3.2. More than 5,000 USD 3.3. The default maximum daily limit transfer is vary depend on the type of the Internet banking customer 3.4. The maximum daily limit transfer may be increased with the approval by the banks 3.5. International transfer limit is different from the national transfer limit
Category 6: Software and system requirements and settings information	
1. Compatibility best with the popular Internet browsers (based on the banks information provided)	1.1. Chrome 1.2. FireFox 1.3. Internet Explorer 1.4. Netscape 1.5. Opera 1.6. Safari
2. Internet banking user device system and browser setting requirement	2.1. Operating System 2.2. Type of browser 2.3. Browser setting 2.4. Screen resolution
3. Free/paid security software/tool available to the Internet banking customers	3.1. Antivirus/anti-spyware 3.2. Internet security suite 3.3. Browser setting 3.4. Provides Internet links to security software vendor(s)

The security evaluation part of the framework extracted from (Subsorn and Limwiriyakul, 2011) **[2]**

References:-

1. Subsorn, P., & Limwiriyakul, S. (2011, August 2). *A comparative analysis of the security of internet banking in Australia:a customer perspective Panida Subsorn*. A comparative analysis of the security of internet banking in Australia:a customer perspective. Retrieved December 8, 2021, from http://docshare04.docshare.tips/files/30258/302583632.pdf.
2. Alsaleh, M., Alarifi, A., Alshaikh, Z., & Zarour, M. (n.d.). *Online banking security and usability towards an Effective Evaluation Framework*. Online Banking Security and Usability Towards an Effective Evaluation Framework. Retrieved December 8, 2021, from https://pdfs.semanticscholar.org/8abe/ff8851cf96a27f121a99c4b0de4c51b46360.pdf.
3. Subsorn, P., & Limwiriyakul, S. (2011, November 25). *A Comparative Analysis of Internet Banking Security in Thailand: A Customer PerspectiveA Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective*. A Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective. Retrieved December 8, 2021, from https://www.researchgate.net/publication/257724372_A_Comparative_Analysis_of_Internet_Banking_Security_in_Thailand_A_Customer_Perspective.
4. Mannan, M., & van Oorschot, P. C. (n.d.). Security and Usability: The Gap in Real-World Online Banking. Retrieved December 8, 2021, from https://www.nspw.org/papers/2007/nspw2007-mannan.pdf.
5. Moh'd Qasem, M. (2014, November 20). *Developing a robust evaluation framework to evaluate security for online banking services*. Developing a Robust Evaluation Framework to Evaluate Security for Online Banking Services. Retrieved December 8, 2021, from https://www.academia.edu/9421398/Developing_a_Robust_Evaluation_Framework_to_Evaluate_Security_for_Online_Banking_Services.
6. Xin, T., & Xiaofang, B. (n.d.). Online banking security analysis based on stride threat model. Retrieved December 8, 2021, from https://www.researchgate.net/publication/290034127_Online_Banking_Security_Analysis_based_on_STRIDE_Threat_Model.
7. Hole, K.J. & Moen, V. & Tjostheim, T.. (2006). Case study: Online banking security. Security & Privacy, IEEE. 4. 14 - 20. 10.1109/MSP.2006.36.
8. Mujinga, Mathias & Eloff, Mm & Kroeze, Jan. (2013). Towards a heuristic model for usable and secure online banking. Proceedings of the 24th Australasian Conference on Information Systems. 1-12.
9. Botacin, Marcus & Kalysch, Anatoli & Grégio, André. (2019). The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study. ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security. 1-10. 10.1145/3339252.3340103.
10. Hao, Chen & Corriveau, Jean-Pierre. (2009). Security Testing and Compliance for Online Banking in Real-World. Lecture Notes in Engineering and Computer Science. 2174.