Challenges in Privacy and Security in Banking Sector and Related Countermeasures

Zarka Zahoor
Jamia Hamdard University
Jamia Hamdard
New Delhi 110062, India

Moin Ud-din
Jamia Hamdard University
Jamia Hamdard
New Delhi 110062, India

Karuna Sunami
Jamia Hamdard University
Jamia Hamdard
New Delhi 110062, India

ABSTRACT
With the extensive use of technology particularly internet by users, banking is becoming more dependent on technology. Unfortunately, with this the cyber-crimes related to banks are also increasing stupendously. The tendency of cyber security attacks aimed at financial sector is much high than any other sector. Some of the common cyber security attacks aimed at banks include Phishing, Cross site scripting, Cyber-squatting, Botnets, Spoofing, etc. This causes a tremendous loss of money to the customer and bank, declines bank's reputation and decreases the trust that users place in a bank.

Banks are obligated to provide a safe online banking environment to its users. Although banks have taken a lot of steps for safety and security of their assets, yet these conventional security mechanisms are no longer optimum as still attackers are able to bypass these security mechanisms. Thus banks should tighten their security mechanisms and take appropriate countermeasures to ensure safety and privacy to bank's most valuable assets.

In this paper, the emerging challenges in security and privacy faced by banks are analyzed. The security mechanisms used by banks have been identified. The security and privacy issues in financial sector have been recognized particularly the cyber security attacks aimed at banks. Lastly, the countermeasures that should be adopted by banks to provide protection against these attacks and ensure a safe banking environment to users have been suggested.

General Terms
Security, Bank, Authentication, Cyber-crime, Cyber-attacks, Privacy, Phishing, Botnets, Spoofing, Key-logging, Cyber squatting

Keywords
Phishing, Botnets, Spoofing, Key-logging, Cyber squatting MITM-Man In The Middle, MITB- Man In The Browser, MITPC- Man In The Personal Computer, OTP-One Time Password, ATM-Automated Teller Machine, DDOS-Distributed Denial Of service, SSL-Secure Sockets Layer, XSS-Cross Site Scripting, IDS-Intrusion Detection System, IPS-Intrusion Prevention System, DNS-Domain Name Server

1. INTRODUCTION
Today technology has become a part of almost every field especially the business sector and the banking sector. The dependence on technology is so much that the banking sector cannot be thought of without the use of technology. But technology has also brought a whole set of challenges to be dealt with which include external threats leading to cyber frauds, higher impact due to intentional or unintentional acts of internal employees, new social engineering techniques used to gain confidential credentials [1].

Given the competitive nature of banking environment, along with the significant value of the resources they manage, business and technology organizations must take all steps necessary to protect their assets. A compromise of these information assets could have a severe impact on the bank, bank customers, form a violation of laws and regulations and negatively affect the reputation and financial stability of the bank.

The Banking industry has been exposed to a large number of cyber-attacks on their data privacy and security such as frauds with online payments, ATM machines, electronic cards, net banking transactions, etc. The average number of attacks aimed at financial services institutions is four times than that of companies in other industries according to a new report from Websense Security Labs [2].The main reason behind these intrusions is to gain confidential data or steal money from banks. Although tight security measures in transactions have been implemented, yet every year these attacks are successful in breaching the security and causing huge financial loss to individuals and banks. Thus there is a high need of implementing countermeasures to protect the most valuable assets of banks against these attacks.

The aim of this paper is to analyse security and privacy challenges faced by banks that are emerging with time. In first section, a survey of the existing literature related to the banking privacy and security challenges has been done. In second section, the security mechanisms employed by banks to provide security and privacy to customer data have been identified. In the next section, the security and privacy challenges in financial sector have been recognized and an analysis of the recent and most common cyber-attacks that are attempted on data security and privacy in banking sector has been done. Lastly, countermeasures have been suggested that could be taken to ensure that such attacks don't happen in future or how to minimise their effect and eventually improve security and privacy perspective of banks.

2. LITERATURE REVIEW
Some specific literature has been assessed in order to find out the work done by research professionals, scholars and organizations in this area. The number of cyber-attacks directed at financial institutions of all sizes is growing. And to address this new threat a lot of effort is required by the financial institutions. More et al. [3] showed that the IT usage and online banking related cybercrime are on the rise particularly in India and young people in the age group 18-30 form the major part of cyber criminals and are of male gender. There is a high need for our law enforcement agencies to be able to overcome and prevent the cyber-crime.

R.R and Neena [4] showed a bigger share of private and foreign banks in frauds related to online banking, ATM, cards and other digital banking transactions. Even with the reducing

number of cases, the value of such cases did not come down proportionately. Ahmad et al. [5] have recognised the intrusions in banking security which include DDOS Attack, Data Breach, Malware, TCP/IP Spoofing, etc. There is a multifaceted threat to Online Banking [6] which include Threats to using PCs, Threats to personal Data Input, Threat to Web Browser, Threats to SSL Communications (SSL MITM), etc. Apart from this, Kaur [7] and Bendovschi [6] have also identified the threats to online banking which include Social engineering Phishing, MITB, MITM, etc. A hacking method to bypass OTP using the MITM and MITPC techniques can easily be developed in the near future and has been discovered by Yoo et al. [9]. The new attack method was tested on Korean internet banking services, and it was empirically proved that it could effectively bypass all of the currently implemented OTP security systems in Korea.

RBI has also published a Report on online banking and cyber frauds [1] in which it identifies the emerging Information Security Attacks and issues of increasing concern in bank security. Angelakopoulos and Mihiotis [10] examined the opportunities and challenges of e-banking for the banking sector in Greece, during the e-commerce era and the study revealed that the low response rate from customers and the implementation of security and data protection mechanisms are the main problems faced by banks.

Banks are also trying their best to tighten their security mechanisms and fill the gaps in them. Bhatt and Pant [11] have described the various cyber-crime safety mechanisms used by banks which include password encryption, virtual keyboard, Secured Socket Layer, SMS Alerts and User Awareness Programs and they found that banks use the latest technology for online security but User Awareness Programs were given least importance due to which users lacked the knowledge of the various security setups of the bank.

Accepting the fact that challenges in bank security are becoming more and more complex with time, there is high time for banks to tighten and improve their security mechanisms. According to NIST's cybersecurity framework [12], there are five core cybersecurity functions that organisations need to implement for providing better protection against cyber threats. These five functions include: Identify, Protect, Detect, Respond and Recover.

A number of countermeasures that should be taken by financial institutions have been discussed [1] [9] [5] [6] [7]. Anti-key logging technology and Anti-Hacking and network security technology have been suggested by Kaur [7] as countermeasures for ensuring safety. Yoo et al. [9] suggested solutions based on the analysis of root cause of the OTP vulnerabilities.

RBI's report [1] has also suggested various security measures that should be taken by banks .Some of them are Risk assessment, direct back-end updates to database, use of cryptographic techniques, a minimum of 128-bit SSL encryption, implementation of Information Security Management System (ISMS) based on ISO 27001 by commercial banks, periodic Penetration Testing, etc.

Thus the cyber-crime in relation with banks is arising at a stupendous rate and is expected to high in near future. Although banks have adopted a number of security measures to protect their assets, yet a lot of effort needs to be still put in. For safeguarding their assets, banks need to analyze the cyber security attacks that are attempted or that can be possibly attempted to breach their security and take countermeasures that need to be taken to ensure these attacks don't happen in future.

3. CYBER-CRIME SAFETY MECHANISMS USED BY BANKS

Financial institutions employ a number of security mechanisms to secure their network and devices.

3.1 Security Safeguards Used In Internet Banking

Table 1: Security safeguards categorised according to the layer on which they are implemented from data process perspective [9]

LAYER	SECURITY SAFEGUARD
DATA LAYER	• Data encryption
DATABASE/APPLICATION LAYER	• Anti-phishing • Anti-reverse engineering • Second factor authentication (OTP, security card, outbound call service, SMS notification service)
OS/PLATFORM LAYER	• Firewall (PC based) • Anti-key logger • OS patch installation agent
NETWORK LAYER	• SSL (Secure Sockets Layer)
PHYSICAL LAYER	• Biometrics • Physical access control by smartcard

3.2 User Authentication Techniques

Based on the characteristics of authentication, these techniques can be categorised into four groups: simple password, second factor authentication, additional channel methods and others. Below tables summarises the key characteristics of each authentication technique from user convenience and security risk perspective.

Table 2: Summary of user authentication techniques and User Convenience

Class	Technique	User convenience		
		User inconvenience	**Installation Cost**	**User carelessness**
Simple Password Type	ID password type	Low	Low	Low
	Virtual keyboard	Normal	Low	Low
	Pre-inquiry response type	Normal	Normal	Normal

	Security card	Normal	High	Normal
	Image Verification Type	Normal	Normal	Normal
Second Factor Methods	Asymmetric key type	Normal	High	Low
	Symmetric key type	Normal	High	Low
Additional methods	One-way type	Low	High	Normal
	Two-way type	Normal	High	Normal
Others	Key board security	normal	Low	low

Table 3: Summary of user authentication techniques and security risk perspective (O: can counteract, X: cannot counteract, *: can counteract partially) [9]

Class	Technique	Security Risk		
		Sniffing	Keyboard logging/ Screen capture	Phishing
Simple Password Type	ID password type	X	X	X
	Virtual keyboard	O	*	X
	Pre-inquiry response type	X	O	X
	Security card	O	O	*
	Image Verification Type	O	X	*
Second Factor Methods	Asymmetric key type	O	O	X
	Symmetric key type	O	O	X
Additional methods	One-way type	O	O	X
	Two-way type	O	O	X
Others	Key board security	O	O	X

3.3 Secured Socket Layer (SSL)

SSL is a security protocol that establishes a secure connection between a server and a client. It creates an encrypted link between server and browser. Sensitive information such as credit card numbers are transmitted securely through SSL. It is used by millions of websites for securing their communications particularly banking websites for online transactions.

To establish an SSL communication, a web server needs an SSL certificate which is issued by a Certifying Authority (CA) [13]. SSL Certificates consist of a pair of keys: a public and a private key. Once the SSL certificate is received, it is installed on the server. An intermediate certificate that establishes the credibility of our SSL Certificate by tying it to our CA's root certificate is also installed. Using a "SSL handshake", the web browser and the SSL protected website establish a secure connection. There are three kinds of keys which are used in SSL protocol: public key, private key and a session key. First, using public and private key, the session key is exchanged between the server and the browser and then using the session key, further communication is secured. Nowadays banks use 128-bit or 256- bit SSL protocol.

3.4 Vulnerability Assessment And Penetration Testing

Security assurance of information needs to be obtained through periodic penetration testing and assessment of system vulnerabilities. The task needs to be done by well trained and independent information security experts in a bank. Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for evading the security features of an application, system, or network [14]. Banks should periodically carry out penetration tests so that they can find out the vulnerabilities in their systems, networks, network equipment, etc. and find out immediate solutions to these vulnerabilities before these are exploited by attackers.

3.5 Database Encryption

In order to secure the sensitive data at rest from internal users who have access to the database, database encryption should be done in banks. There are a number of ways in which database can be encrypted. One way is an inbuilt mechanism in database called Transparent Data Encryption [15] which involves encrypting the data in database using symmetric or asymmetric approach, then encrypting the encryption key using either a certificate stored in master database or an asymmetric key and storing the encryption.

3.6 Data Retention

In a banking institution, all the data that is no longer used for daily business purposes should be removed to avoid compromising of data security. Archiving and retention of data should be done to ensure data is kept as long as needed on a dedicated environment (back-up servers, dedicated archives, etc.), and removed from the company's network. This limits the risk of unauthorised access to sensitive information.

3.7 Network protection devices

3.7.1 Firewalls

Firewalls are devices or programs that control the flow of traffic between networks or hosts that have differing security postures [16]. The main goal of having a firewall is "access control". A firewall reduces various attack vectors by limiting inbound and outbound communications. Financial institutions have four primary firewall types: Packet Filtering, Stateful inspection, proxy servers and application level firewalls [1]. Any product may have characteristics of one or more firewall types.

3.7.2 Intrusion Detection Systems

According to NIST's definition, an Intrusion Detection System is "A hardware or software product that collects and analyses information from various areas within a computer or a network to identify possible cyber-attacks, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations)". Identification of network traffic in real time is the primary goal of an IDS.

Most IDSs detect port scans, malware, and other kinds of abnormal network communications by using signatures. The ideal placement of an IDS is external to the organization as well as internal to the organisation, just behind the firewall. This would enable a bank to view the traffic coming inside and going outside the organization through the firewall. This is particularly useful for situations where malicious activity originates from inside the firewall.

A banking institution should be aware of the detection capability and the effect of placement and other network defences on the detection capability for using a network IDS (NIDS) effectively. False positives (alerts where no attack exists) and false negatives (no alert when an attack does take place) are detected by all NIDS detection methods [1]. While false negatives are obviously a concern, false positives can also hinder detection.

3.7.3 Network Intrusion Prevention Systems

Network Intrusion Prevention Systems (NIPS) are devices that analyse packet headers and packet payloads and based on that allow or disallow access. A "white list" consisting of IP addresses that should not be blocked can also be used with an IPS unit which helps ensure that an attacker cannot carry out a DOS by spoofing the IP of a critical host.

3.7.4 Quarantine

When a device is quarantined, it protects the network from potentially malicious code or actions [1].
A device (connecting to a security domain) is queried for conformity to the domain's security policy. If the device does not conform, it is placed in a restricted part of the network until it conforms

3.7.5 DNS Placement

To maintain the security of the institution's communications, it is necessary to effectively protect the institution's DNS servers [1]. Much of the protection is provided by host security However, an important factor is the placement of the DNS . The optimal placement is split DNS, where one firewalled DNS server serves public domain information to the outside. It does not perform recursive queries. Another DNS server, in an internal security domain performs recursive queries for internal users.

3.8 Password Protection mechanisms

Passwords is one of the most important security feature used today. A number of password protection mechanisms can be used by banks to secure user passwords such as password encryption, password hashing. Further security of hashed digests can be improved using the concept of SALT and ITERATION COUNT.A salt is a sequence of bytes that is concatenated to the password before hashing and then the concatenated value is hashed. This gives the password protection against dictionary attacks. Iteration Count is the number of times the hashing function is applied again and again to get the final digest. This makes the task of an attacker more time consuming and eventually difficult.

3.9 SMS Alerts

SMS banking is a facility used by banks in which they send messages to customers by SMS messaging to notify them something important or to enable them perform transactions. There are two types of messages: Push and Pull messages [17]. Push messages are the messages sent by bank to the customer without initiation by the customer for providing the information. For example a large withdrawal of funds from an ATM. Pull messages are messages initiated by the customer using a mobile phone to get information or to perform a transaction such as an account balance enquiry. SMS uses insecure encryption and is easily spoofable, therefore there is a high risk of fraud where SMS banking is involved. As compared to conventional banking services like ATM or net banking, this technology is less secure so it should not be used for very high risk transactions.

4. CHALLENGES IN PRIVACY AND SECURITY IN BANKING SECTOR

With the increase in the use of online banking by customers, security threat to banking sector is increasing at an extraordinarily high rate. The Banking industry has been exposed to a large number of cyber-attacks on their privacy and security such as frauds with online payments, ATM machines, electronic cards, net banking transactions, etc. This section describes the challenges in privacy and security of banks. First the privacy issues are discussed, followed by the common cyber-attacks aimed at banks.

4.1 Privacy Issues

Banking is one of the most risky areas as far as privacy is concerned. There are a no. of ways in which violation of privacy can take place in the banking sector which include: sharing personal information with third parties or allowing them access for marketing purposes without approval from users, stolen or lost banking number or card, inadequate notification to an individual about what will be done with their personal data, collection of more personal data than is necessary, refusing in providing financial records when requested by client, incorrect recording of personal information, and loss of a client's personal data due to improper security measures. For example in Bank Of America, the Utility Consumers' Action Network reported a very common privacy violation by the bank in which the bank sold the personal information (bank account numbers, social security numbers, etc.) of thirty five million customers to marketers and third parties without informing individuals [18].

4.2 Cyber Security Attacks On Banks

Banks are exposed to a number of cyber security attacks. RBI in [1] identifies Phishing, Cross site scripting, Vishing, Cyber-Squatting, Bot networks, E-mail related crimes, Malware, SMS spoofing, Denial of service attacks, Pharming, Insider threats as the emerging information security attacks on banks.

4.2.1 Phishing

One of the most common cyber frauds is "Phishing". Phishing is an attack in which an attempt is made to obtain sensitive information of user such as usernames, passwords, credit card details, etc. by an attacker by pretending to be a reliable body in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging in which users are asked to click on a link usually for securing their accounts. The users are then directed to fraudulent websites which look alike the original banking website so that the user is deceived and is asked to enter his personal information such as usernames, passwords, credit card details, etc. Once the user enters his/her personal information, the fraudster then has access to the customer's online bank account and to the funds contained in that account. There are a variety of tools and techniques used by phishers which serve a variety of functions, including email delivery, phishing site hosting, and specialized malware. These tools include Botnets, Phishing Kits, Abuse of Domain Name Service (DNS) , Technical Deceit, Session Hijacking and Specialized Malware [19].

A phishing incident was reported in Hyderabad [20], which was in the name of India's central bank RBI in which the phishing email said that RBI had launched a new security system and asked users to click a link which redirected users to a fake website. It asked users to enter their online bank credentials including card numbers and the secret three digit CVV number, among others. RBI has cautioned people that it has not launched any such software as soon as it came to know about it.

4.2.2 Cross site scripting

Cross-site scripting (XSS) is a kind of cyber security vulnerability usually found in web applications and they allow code injections by malicious web users into the web pages that are viewed by other users [1]. Examples of such code include client-side scripts, HTML code, etc. A cross-site scripting vulnerability can be exploited by attackers to bypass access controls. Their impact ranges from a petty nuisance to a significant security risk, depending on the sensitivity of the data that is handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

4.2.3 Vishing

Vishing is a cyber-attack in which social engineering and Voice over IP (VoIP) are used to access the private and financial information from the public for getting financial reward [1]. It combines "voice" and "phishing". Vishing is an illegal practice where an attacker calls a user and pretends to be from a bank in which the user has an account. He usually asks to verify the user's account information (stating that user's account has been suspended, etc.) and once the user gives his credentials such as username, password, credit card number, etc., the attacker has easy access to the user's account and the money in it. There has also been a theft of payment card data of the customers of U.S. banks by various vishing attacks. In an attack in 2014, customers of a midsize bank received SMS text messages which claimed their debit card was deactivated and asked users to provide the card and PIN numbers to reactivate it [21].

4.2.4 Cyber Squatting

Cyber-squatting is a process in which a famous domain name is registered and then it is sold for a fortune. Cyber Squatters register domain names which are similar to popular service providers' domains so as to attract their users and benefit from it. Some countries have specific laws against cyber-squatting that are beyond the normal rules of trademark law. For example, the United States has the U.S. Anticybers-quatting Consumer Protection Act (ACPA) of 1999 which provides protection against cybersquatting for individuals and also owners of distinctive trademarked names. The Washington Post reported in 2007 that Dell filed a lawsuit against BelgiumDomains, CapitolDomains, and DomainDoorman for cyber-squatting and typo-squatting and dellfinacncialservices.com was one of the domains that was cited [22].

4.2.5 Bot Networks (Botnet)

Bots are programs that infect a system to provide remote command and control access via a variety of protocols, such as HTTP, instant messaging, and peer-to-peer protocols. Several of bots under common control are commonly referred to as a "Botnet". Computers get associated with botnets when unaware users download malware such as a "Trojan Horse" which is sent as an e-mail attachment. The systems that are infected are termed as "zombies". Illicit activities can be carried out with bots by the controller that include relays for sending spam and phishing emails, updates for existing malware, DDOS ,etc. Bot Networks create unique problems for organizations because they can be upgraded very quickly remotely with new exploits, and this could help attackers prevent security efforts.

4.2.6 Malware

Malware is a maliciously crafted software program that accesses and alters the computer system without the consent of the user or owner. Malware includes viruses, Trojan horses, worms, etc. Malware can heavily influence the confidentiality, integrity and availability of the banking system. Malwares have the capability to compromise the information in the banking systems and may lead to a loss of worth millions to the bank. Malwares can target both the user's system and the bank itself. E.g; Zeus.

4.2.7 Denial of Service (DOS) Attack

A DOS is an attack in which a user or an organisation is prevented from accessing a resource online. While as in Distributed denial-of-service Attack (DDOS), a specific system is targeted by a large group of compromised systems (usually called a Botnet) and make the services of the targeted system unavailable to its users. Actually the targeted system is flooded with incoming messages which causes it to shut down and thus the system is unavailable to its users.

Although DOS attacks don't usually result in loss of information or security to a bank, it can cost the bank a great deal of time, money and customers and can also destroy programming and files in affected computer systems.

4.2.8 SMS Spoofing

It is a relatively new technology in which a user receives a SMS message on phone which appears to be coming from a legitimate bank. In this SMS the originating mobile number (Sender ID) is replaced by alphanumeric text. Here a user may be fooled to give his/her online credentials and his/her money may be at risk of theft.

4.2.9 TCP/IP Spoofing

It is one of the most common forms of online camouflage. In IP spoofing, illegal access is attempted on a system by sending an email message to a victim that appears to come from a trusted machine by "spoofing" the machines' IP address. IP address spoofing is a powerful technique as it can enable an attacker to send packets to a network without being blocked by a firewall. This is because usually firewalls filter packets based on sender's IP address and they would normally filter out any external IP address. However using IP spoofing, the attacker's data packet appears to come from legitimate IP address (internal network) and thus firewall is unable to intercept it. The main goal here is to obtain root access to the victim's server (here the banking system), allowing a backdoor entry path into the targeted systems [5].

4.2.10 Pharming

It is also called farming or DNS poisoning. In this attack whenever a user tries to access a website, he/ she will be redirected to a fake site. Pharming can be done in two possible ways: one is by changing host's files on a victim's computer and other way is by exploiting vulnerability in DNS server software. In January 2005, the domain name for a large New York ISP, Panix, was hijacked and legitimate traffic was redirected to a fake website in Australia [23]. No financial losses are known. In January 2008, a drive-by pharming incident was reported by Symantec that was directed against a Mexican bank and in which the DNS settings on a customer's home router were altered after receipt of an e-mail message

that appeared to be from a legitimate Spanish-language greeting-card company [24].

4.2.11 Insider Threats

With the increase in the use of information technology by banks, there is a high security risk to bank's data by insiders or employees of banks who can disclose, modify or access the information illegally. Also unintentional errors by employees can have devastating results. Robust security processes must be used by banks to mitigate such threats.

4.2.12 Attacks on OTP

OTP(one Time Password) is a two factor authentication method in which a password is created whenever the users attempts authentication and the password is disposed of after use. A no. of attacks can be launched on accounts that are OTP protected which are known as MIT-X methods (Man-In –The-X) [9]. These are as follows:

- ***Man-in –the-middle attack (MITM):*** Here the transmission paths of data are accessed and information is snatched in the middle of transactions.
- ***Man-in-the-Browser attack (MITB):*** Here malicious code exists in the web browser and it induces users to enter credentials and other important information into a fake form.
- ***Man-in-the-PC attack (MITPC):*** MITPC exploits the weaknesses in the hardware environment or operating system to steal OTP.

5. COUNTERMEASURES FOR SECURING SECURITY ARCHITECTURE IN BANKS

Banks should tighten up their defence methods for safeguarding the data of customers and adopt countermeasures to make the banking system more immune to these attacks. In this section, we are attempting to suggest some countermeasures that banks should take up to mitigate the cyber security attacks and enhance the banking security infrastructure.

5.1 Continuous Risk Assessment

There are no two banks alike. Thus each financial company has its own risk profile depending on its size, geographical setup, business operating sector, etc. Each company should perform a series of steps to put into effect security controls, identify threats, loopholes, risks and design and implement security controls that address these risks.

5.2 Countermeasures For Key Logging Attacks

Financial institutions have become the target of key-loggers, especially those ones in which advanced security features such as PIN pads, screen keyboards are not yet used. There are two methods that can be adopted for withstanding key-logging attacks:

5.2.1 Anti-key logger

Anti-key logger is a software application which detects keystroke logger software present in a system and then deletes or immobilises the hidden keystroke logger software. Any system on which banking or client information is accessed is scanned by Anti-key loggers and banking information, and credit card numbers are protected from identity thieves.

5.2.2 Anti-key logging Technology

In order to protect keyboard input values, every portion of the entire system needs to be protected (Fig 5.1) and this protection starts from the end user's keyboard inputting to what is saved in the memory of the web browser and finally what is reported on the user's screen. In order to provide keyboard security, everything needs to be detected in both the kernel level keylogging and the user level keylogging.

At the kernel level, if the input values from port to IDT, from port to driver are codified, then only the input values can be protected. At the user level, each stage of the process should be detected for hooking and the memory should be protected. Moreover, if data is captured through BHO or API of the browser, it should be protected by using a sophisticated technology that shows only dummy data that would be meaningless.

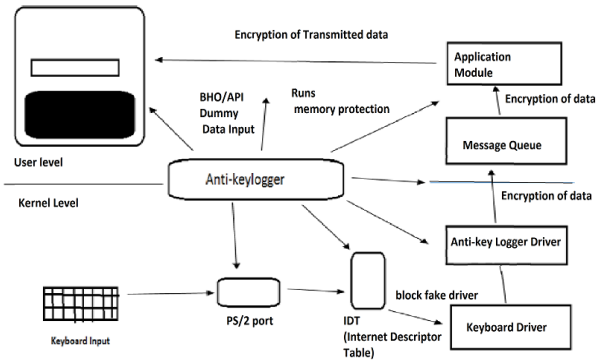

Figure 1: Anti-key logger that provides protection at every stage of the transaction carried out by keyboard inputting (PS/2 illustrated) [6]

5.3 Countermeasures Against Web Browser Attacks

The web browser is the commonest target of most of the attackers. For safe online banking, we need a web browser technology that is able to protect itself against reverse engineering and debugging by attackers and should be able to block any attempt to access or modify its memory. It should obstruct COM (Component Object Model) Hooking and Cross Site Scripting as well as screen capture to prevent inputting the image type password. By falsifying host files or DNS, it should hinder Phishing and Pharming attacks.

Some security countermeasures for deterring a Man-in-the-Browser Attack [25] are as under:

Table 4: Active safeguards against MITB

METHOD	DESCRIPTION	EFFECTIVE AGAINST MITB?	REASON
Hardened Browser on a USB Drive	A hardened browser is shipped to en.d-users on a USB drive that is hard-coded to only connect to the target bank's website;	Yes, but inconvenient	Attacking this browser is difficult for Malware, but it cannot be ruled out since the malware and secure browser are

	sometimes a PKI credential stored on the USB device is used for authenticati on purposes.		running on the same computer; many organizatio ns have disabled USB drives or have at least disabled "autorun" capability for external media, making deployment of this browser more challenging; browser updates can also be difficult
OTP token with signature	We can amplify on the OTP token method and some kinds of OTP tokens can be used to sign transaction details electronicall y, if they are equipped with a small numeric keypad. Here user is prompted to enter transaction details on the small keypad and then a signature code is computed by the token.	Yes, but inconvenie nt	User is aware of the specifics as user enters the transaction details, and if malware attempts to change them, the banking site can detect it; usability on the token screen and keyboard is weak, and the user can be confused; deployment of special hardware must be done.
OTP token with signature	We can amplify on the OTP token method and some kinds of OTP tokens can be used to sign transaction details electronicall y, if they are equipped with a small numeric keypad. Here user is prompted to enter transaction details on the small keypad and then a signature code is computed by the token.	Yes, but inconvenie nt	User is aware of the specifics as user enters the transaction details, and if malware attempts to change them, the banking site can detect it; usability on the token screen and keyboard is weak, and the user can be confused; deployment of special hardware must be done.
Out-of-Band Transactio n Detail Confirmati on with OTP	Here the user is not only sent a one-time passcode via out-of-band communicat ion (e.g., Voice or SMS channel), as well as a summary of the transaction that's about to occur; user can then review the details, and only proceed if they recognize the details	Yes	User will be able to view transaction details in a separate communicat ion channel; Bank must be cautious to protect against easy reset of the out-of-band contact details or the malware will do this first then attack successfully ; reset is inherently a more elaborate and protected process if out-of-band confirmatio n is sent to an initialized mobile application (vs. simply SMS to a phone).

Table 5: Passive Safeguards against MITB

Method:	Explanation:	Effective against MITB?	Reason:
Fraud Detection that Monitors User Behaviour	From the moment users log on till the moment they complete their session, this method will capture and analyse all of the user's Web traffic data; best-of-breed examples of this type of fraud detection use a "zero-touch" approach for achieving this, eliminating the need to change the online application, streamlining deployment and also increase the ability to react to changes in fraud	Yes	The advantage of this solution is that aberrations in behaviour can be highlighted before an actual transaction is undertaken, including the detection of IP changes mid-session, navigating through a site too quickly, or navigating in an unusual way for a given user's profiled data "Zero-touch" fraud detection application accesses information at all levels of the communication stack, including source IP address, user-agent type, activity dynamics, etc. A 360 degree view of how the banking application is being used and abused is given to the system by analysing from a single user session, multiple sessions for the same user and multiple sessions for multiple users.

5.4 Countermeasures Against Attacks On OTP

Table 6: OTP related countermeasures

TYPE OF ATTACK ON OTP:	RELATED COUNTERMEASURE:
MITM(Man In The Middle) Attack	• Using encrypted channel between the user and the bank's server provided by HTTPS, VPN or SSL. • Proper authentication of the server with which users establish an SSL/TLS session by user. • Make user authentication depend on the user's (secret) credentials as well as on state information related to the SSL/TLS session in which the credentials are being sent to the server [26].
MITPC(Man In The PC) Attack	• Regularly fixing the vulnerabilities of hardware and operating system • Securing every Data access path in the OS including the Key input, screen, mouse movement and also memories
OTP attack by using MITM and MITPC	• **Technological solution [9]:** Mutual certifying in server: Multiple login requests from different IP's within 60 s can be regarded as an attack attempt Protection Of certificate: A hardware certifying function be included in the certificate for an internet banking service. E2E (End to End Encryption): It allows Direct encryption from web browser to the authentication server. Code Integrity Checking: A Code Integrity Check before authentication can't be the ultimate solution but can enhance OTP security level at a low cost • **Policy perspective solution [9]:** Technology can't be the ultimate solution and flexible policies should be followed to minimize the loss and risk ,for example; setting up a transaction delay of 10 minutes for transactions greater than a thousand dollar or a transaction notification system for transactions over a certain amount of money

5.5 Countermeasures Against Phishing And Spear Phishing

The countermeasures against phishing can be categorised into two approaches:

5.5.1 Approaches that mitigate the phishing attack without modifying the traditional authentication and authorisation method (PIN/TAN) [27]

This group can further be categorised into two classes: User dependent approach and user independent approach.

User dependent approach is in the form of a guideline to users and describe correct usage of service. For example, Spam filters and Filters for Outgoing Data in which already known phishing mails and faked hyperlinks are identified and corresponding email can be classified as spam. It can also scan outgoing data for sensitive information, block it and immediately notify the user. Also Browser Plug-ins fall under this category in which some (SpoofStick) plug-ins verify the URL of the currently visited website while some (Phish Net) use blacklists with well-known phishing sites.

User independent approaches are implemented solely by the service provider. For example Spam Trap and Domain Watch which inform the service provider at an early stage of an attack so that they can issue an early warning to users. In Spam trap, email addresses are dropped in numerous newsgroups, websites, etc. so as to get as many spams as possible on that address. These emails are analysed for a phishing attack and the effected service provider is notified accordingly. Domain Watch monitors registration of new domain names that are similar to an existing service provider and the service provider is notified accordingly. Another user independent approach is Validation of sender information in which the real originator of spam and phishing mails is identified using Sender-Validation techniques.

5.5.2 Approaches that modify the traditional authentication and authorisation method (PIN/TAN) [27]

- **Hardware Tokens**

The PIN/TAN procedure is substituted by a piece of hardware (hardware token) given to all users that is used to generate One time passwords.

- **PKI and Digital Certificate:**

In PKI, user gets a key pair and a certificate that guarantees its public keys authenticity. A timestamp and a certificate is put together with every request sent to the service provider who can verify the request using user's public key.

5.6 Countermeasures Against Cross Site Scrippting

There are two main measures [28] to prevent XSS attacks: Filtering and escaping. In FILTERING FOR XSS, all XSS attacks infect websites through some user input which could be a simple <form> submitted by the user, an exploited cookie, etc. all this data is coming from external sources and shouldn't be trusted. The simplest way for XSS protection is to pass all external data through a filter which would remove all dangerous keywords, such as the <SCRIPT> tag, JavaScript commands and other dangerous HTML mark-up. ESCAPING FROM XSS method effectively disables an XSS attack. In Escaping, the browser is effectively instructed that the data sent by website should be treated as data and should not be interpreted in any other way. Even if an attacker manages to put a script on website's page, the victim will not be affected because the script will not executed by the browser if it is properly escaped.

5.7 Countermeasures Against Attacks From Botnets

These fall under two categories [29]:

5.7.1 Classical Countermeasures

- **Take down the Command-and-Control server**

The base of a botnet (Command-and-Control server) is removed which extinguishes the whole botnet in one go. But this is possible only if three conditions are met. First, the botnet uses a centralised structure. Second, Command-and-Control server's location is known. Third, the provider cooperates. Usually all of these conditions are difficult to meet.

- **Sinkholing Malicious Traffic**

If Command-and-Control server cannot be put down, another option is redirection of malicious traffic to Sinkholes (a special purpose server) either locally or globally. The sinkholes record, analyse and drop malicious traffic so that it is unable to reach the target it was intended for.eg; DDOS Null Routing.

- **Clean Infected Systems**

All the systems infected are cleaned by removing the bots installed.

5.7.2 Offensive Measures

These fall under three categories: Mitigation, Manipulation and Exploitation.

"Mitigation strategies" slows down botnets for instance by consumption of their resources. "Manipulation Strategies" use command layer. Possible manipulation can be the altering or removing of DDoS or Spam commands as well as commands to download and execute programs, which allows a remote clean-up of infected machine. Among the less invasive options are dropping collected personal data, like credit card or banking details and replacing them by fake information, or to issue commands to make bots stop the collection. Lastly in "Exploitation", bugs found in bots are used and can be used to perform specific actions on infected machines.

5.8 Countermeasures Against DOS And DDOS Attacks

These fall under the following categories [30]:

5.8.1 Defense Mechanisms For DDOS Based On Deployment

This classification is based on the location where the defence mechanism is implemented and can be further categorised as:

- **Source based**

These mechanisms are implemented near sources of attacks and basically restrict the network customers from generating DDOs attacks.

- **Destination Based**

These mechanisms are employed near the victim i.e. either at the access router or the edge router of the destination. Some of these are IP Traceback mechanisms and Packet marking and filtering mechanisms.

- **Network Based**

These mechanisms are mainly implemented inside networks and on the routers of the autonomous systems. Some of the network based defense mechanisms include detecting and filtering malicious routers, route based packet filtering, etc.

5.8.2 Defense Mechanisms For DDOS Based On Protocol

These are further classified as:

5.8.2.1 Mechanisms to defend against the TCP/IP NETWORK level DDOS attacks:

5.8.2.2 TCP level defense mechanism [31]:

- ***Increasing Backlog:*** In this technique large backlogs are used so that in case TCB buffers are exhausted, backlogs can be used.

- ***Reducing SYN-RECEIVED Timer:*** Another quickly implementable measure is to reduce the timeout period between receiving a SYN and reaping the created TCB for lack of progress. A shorter timer will keep bogus connection attempts from persisting for as long in the backlog and thus it frees up space for legitimate connections sooner.

- ***SYN Cookies:***

  SYN cookies carry out modification of the TCP protocol handling of the server by delaying resource allocation until the client address has been verified. This technique guards against SYN flood attacks and also allows a server to avoid dropping connections in case the SYN queue fills up. Instead, server behaves as if the SYN queue had been enlarged and the appropriate SYN+ACK is sent back by the server.

5.8.2.1.2 IP level defense mechanism:

- ***SIP defender:*** VoIP Defender is an open security architecture in which the traffic flow is monitored between SIP servers and external users and proxies to detect attacks directed at the protected SIP server and a framework for attack prevention/mitigation is provided [32],[33].
- ***Push back:*** DDoS attacks at IP level are defended by Pushback mechanism by allowing a router to request adjacent upstream routers to limit the rate of traffic [34], [35].

5.8.2.2 Mechanisms to defend against APPLICATION level DDOS attacks:

These defense mechanisms can be:

- ***HTTP-flooding*** can be defended based on page access behaviour, [36].

- ***DDOS shield:*** Here use of statistical methods is done to detect HTTP level DDOS attacks [37].

- ***Defense against tilt DDOS attacks:*** Throughout a connection session, a user's features (e.g. request volume, instant and long-term behaviour) are examined in order to determine whether he is a malicious user or not [38].

5.8.3 DDOS Defense Mechanisms Based On Time Of Action:

Based on the time of action, defense mechanisms can be of following types:

- ***Before the attack:***

These attack mechanisms are basically deployed to prevent the attack from happening and are mostly focused on fixing the bugs such as protocol exploits system vulnerabilities, etc.

- ***During the attack:***

Mechanisms in this category are employed to detect the attack when it happens. There are various methods to detect the attack such as IDPS systems or firewalls can be used under this category.

- ***After the attack:***

These mechanisms are deployed to act once the DDOS is detected and the source of attack is traced back.

5.9 USER AWARENESS PROGRAMS

User is the key of any field and in some cases may be the weakest link in the chain. A bank can employ the latest security technologies but all are a waste if the customer does not know how to use them. Banks should frequently run some user awareness program for end users to inform them about the latest security features introduced by bank and how the customers can use them to secure their accounts.

6. CONCLUSION

As the dependency of banks on technology is increasing, Banks are facing an exponentially increasing privacy and security risk to their valuable assets. With this the cyber-crimes related to banks are also increasing stupendously. The security mechanisms employed by banks are no longer optimum. Thus banks should tighten up their security mechanisms and take appropriate countermeasures particularly the ones suggested in this paper to ensure safety and privacy to bank's most valuable assets. Thus it is finally concluded that with advancements in technology around the world, banks should not be left behind in terms of security systems, a sharp eye should be kept on vulnerabilities present in banking networks and emerging tricks and techniques used by hackers to bypass banking security and launch attacks should be continually monitored. A tight security architecture should be implemented to provide a safe banking environment to users.

7. FUTURE SCOPE

All of the above stated countermeasures target a particular attack and even some of them are able to provide protection only in a limited way or work under certain circumstances. For example, the classical countermeasures against Botnets where the command-and-Control is brought down can work only if three conditions are met. First, the botnet should use a centralised structure. Second, Command-and-Control server's location should be known. Third, the provider should cooperate. Usually all of these conditions are difficult to meet. Also the proactive countermeasures against these botnets are technically feasible but have legal and ethical aspects that need to be considered for implementing them. Thus the future scope of this study would be to devise an approach or an algorithm that would provide an all-round solution to mitigate the majority of the threats faced by banks. A solution can be thought of that fills in the gaps left by the currently used strategies, mitigates an attack under all circumstances and in the best possible way.

8. REFERENCES

[1] G.Gopalakrishna "Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds", RBI, Mumbai, Maharashtra, January 2011 Available: https://rbi.org.in/ scripts/ NotificationUser.aspx?Mode=0&Id=6366

[2] Maria Korolov. (Jun 23, 2015). Banks get attacked four times more than other industries [Online]. Available: http://www.csoonline.com/article/2938767/advanced-persistent-threats/report-banks-get-attacked-four-times-more-than-other-industries.html

[3] Dr. Manisha M.More, Meenakshi P.Jadhav and Dr. K.M.Nalawade, "Online Banking and Cyber Attacks: The current Scenario", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 12, pp. 743-749, 2015 ISSN: 2277 128X

[4] Soni R.R and Soni Neena, "An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks", Research Journal Of management Sciences, vol. 2,no.7,pp. 22-27, 2013 ISSN 2319–1171

[5] Mohd Khairul Ahmad, Rayvieana Vera Rosalim, Leau YU Beng and Tan Soo Fun, "Security issues on Banking Systems", International Journal of Computer Science and Information Technologies, vol. 1, no.4, pp. 268-272, 2010 ISSN: 0975-9646

[6] "Online Banking: Threats and Countermeasures", Ahnlab Online Security Available: https://sqnetworks.com/ downloads/AhnLab_AOS_WhitePaper.pdf

[7] Navjeet Kaur, "A Survey on Online Banking System Attacks and its Countermeasures", International Journal of Computer Science and Network Security, vol.15, no.3, pp. 57-61, 2015

[8] Andreea Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures", Procedia Economics and Finance, vol. 28, pp. 24-31, 2015

[9] Changsok Yoo, Byung-Tak Kang and Huy Kang Kim, "Case study of the vulnerability of OTP implemented in internet banking systems of South Korea", Multimed Tools Appl ,vol. 74, pp. 3289–3303, 2015

[10] Georgios Angelakopoulos and Athanassios Mihiotis "E-banking: challenges and opportunities in the Greek banking sector", Electron Commer Res, vol. 11, pp. 297–319, 2011

[11] Susheel Chandra Bhatt and Durgesh Pant, "Study of Indian Banks Websites for Cyber Crime Safety Mechanism", International Journal of Advanced Computer Science and Applications, vol. 2, no.10,pp. 87-90, 2011

[12] "Executive Leadership of Cybersecurity", CSBS [Online] Available: https://www.csbs.org/CyberSecurity/Documents/ CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf

[13] "What Is SSL (Secure Sockets Layer) and What AreSSL Certificates?", Digi cert Available:https://www.digicert.com /ssl.htm

[14] "Technical Guide to Information Security Testing and Assessment", NIST Available: http://csrc.nist.gov/ publications/nistpubs/800-115/SP800-115.pdf

[15] Vibhore K Jain, "Database Encryption", Banking Security Magazine, vol.1, no.1, 2011

[16] "Guidelines on Firewalls and Firewall Policy", NIST Available: http://csrc.nist.gov/publications/ nistpubs/800-41-Rev1/sp800-41-rev1.pdf

[17] "SMS Banking", Wikipedia Available: https://en.wikipedia.org/wiki/SMS_banking

[18] "Privacy and Banking: Do Indian Banking Standards Provide Enough Privacy Protection?", The Centre for Internet and society Available:http://cis-india.org/internet-governance/blog/privacy/privacy-banking

[19] Jason Milletary, "Technical Trends in Phishing Attacks", US-CERT

[20] R.P.Kaur, "Statistics Of Cyber Crime In India: An Overview", International Journal of Engineering and Computer Science, vol.2, no. 8, pp. 2555-2559,2013

[21] John La Cour (April 29, 2014) Vishing campaign steals card data from customers of dozens of banks [Online] Available: http://blog.phishlabs.com/vishing-campaign-steals-card-data-from-customers-of-dozens-of-banks

[22] Top Ten Cyber Squatter Cases Available: http://www.computerweekly.com/photostory /2240107807/Photos-Top-ten-cybersquatter-cases/1/ Cybersquatting-cases-Number-10-Dell

[23] "Pharming",Wikipedia Available: https://en.wikipedia.org / wiki/Pharming#cite_note-3

[24] Ellen Messmer (Jan 22, 2008). "First case of drive-by pharming identified in the wild" [Online] Available: http://www.networkworld.com/article/2282527/lan-wan/first-case-of--drive-by pharming--identified-in-the-wild.html

[25] "Defeating Man in the browser Malware" Available: https://www.entrust.com/wp-content/uploads/2014/03/WP_Entrust-MITB_March2014.pdf

[26] "SSL/TLS Session-Aware User Authentication—Or How to Effectively Thwart the Man-in-the-Middle" Available: http://people.inf.ethz.ch/basin/pubs/mitm-cc.pdf

[27] Klaus Plossl, Hannes Federrath and Thomas Nowey,"Protection Mechanisms against Phishing Attacks"in Proc. 2nd International Conference on Trust, Privacy and Security in Digital Business (TrustBus '05). LNCS 3592, Springer-Verlag, Heidelberg, 2005, pp.20-29.

[28] "Preventing XSS Attacks" Available: http://www.acunetix.com/blog/articles/preventing-xss-attacks

[29] "Proactive Botnet Countermeasures an Offensive Approach", NATO Available: https://ccdcoe.org /publications/

virtualbattlefield/15_LEDER_Proactive_Coutnermeasures.pdf

[30] Rajkumar, Manisha Jitendra Nene, "A Survey on Latest DoS Attacks: Classification and Defence Mechanisms", International Journal of Innovative Research in Computer and Communication Engineering,vol. 1,no. 8, pp. 1847-1860,2013

[31] ietf: tcp syn flooding attacks and common mitigations Available:http://tools.ietf.org/html/rfc4987

[32] "VoIP Defender: Highly Scalable SIP-based Security Architecture",Iptel Available: http://www.iptel.org/~dor/papers/Fied0707_voip.pdf

[33] "Protecting SIP against Very Large Flooding DoS Attacks", NEC Europe Ltd. Available: http://startrinity.com/VoIP/Resources/sip362.pdf

[34] John Ioannidis, Steven M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks", *In Proc. of Network and Distributed System Security Symposium*, 2002 Available: http://citeseer.ist.psu.edu/viewdoc/ download?doi=10.1.1.16.2012 &rep=rep1&type=pdf

[35] Tao Peng, Christopher Leckie and Kotagiri Ramamohana rao, "Defending Against Distributed Denial of Service Attacks Using Selective Pushback", *In Proc. of the Ninth IEEE International Conference on Telecommunications (ICT)*, 2002 Available: http://citeseerx.ist.psu.edu /viewdoc /download?doi=10.1.1.11.8639&rep=rep1&type=pdf

[36] Lei Zhang, Shui Yu, Di Wu and Paul Watters, "A Survey on Latest Botnet Attack and Defense", *International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11*,2011 Available: https://pdfs.semanticscholar.org/e4fa/1e3c305ce738da86bc43458e19faf62323d5.pdf

[37] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal and Edward Knightly, "DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection", *In Proc. Of IEEE Infocom*,2006, pp.23-29 Available: http://citeseerx.ist.psu.edu/viewdoc/versions ?doi=10.1.1.68.8279

[38] Huey-Ing Liu and Kuo-Chao Chang, "Defending Systems Against Tilt DDoS Attacks", *The 6th International Conference on Telecommunication Systems, Services, and Applications*, Bali, 2011, pp.22-27