SECURITY FOR ONLINE BANKING AND TRANSACTIONS

Prof. Pushpa Nanasaheb Bhagawat
SBVP's Loknete Balasaheb Thorat Arts, Commerce and Science College,
Talegaon Dighe, Ahmednagar

Abstract

This study explores the safety measures used in online transactions and banking, highlighting the importance of robust security features for safeguarding bank and customer data. It examines unique threats like port scanning, password cracking, and social engineering, emphasizing the need for robust security features. Key security features include virtual keyboards, one-time passwords, browser safety, and virtual certificates. The study also explores tools like tool identity, SMS verification, device registration, and CAPTCHAs for enhanced user authentication. Private firewalls, transaction monitoring, training, and secure protocols like SSL are also highlighted as critical elements of online banking safety. The study uses correlation analysis to examine the relationship between online and traditional banking, revealing a negative correlation between demand drafts and online banking. The study also highlights the interdependence of protection elements, database, and transaction protection. Regression analysis shows a positive correlation between age and gender, while Hypothesis testing rejects the null hypothesis that there is no correlation between online and traditional banking or that safety affects customer use. The article concludes by emphasizing the growing dependence on online banking systems and the crucial role of robust security features in building customer confidence and ensuring consumer safety.

Introduction

In the past ten years, online banking systems have grown in popularity. Through the use of an online payment system, various clients can carry out financial transactions via a website. As long as there is an Internet connection, customers of an online bank can use their own personal devices to manage their accounts. Other names for online banking include e-banking, virtual banking, online banking, and others. Any online banking system has two basic phases: the registration phase and the login phase. Every bank has essentially a similar structure for their registration step. The two stages of password security used during the login phase include transaction password and user ID, as well as additional measures such as one-time password, QR code, grid authority card, biometric systems, security questions, and e-token, among other advanced systems. Every security mechanism is designed to safeguard customers' bank accounts from potential threats posed by members of the black-hat community. Expert criminal hackers have the ability to alter an online financial institution's information system, disseminate malicious viruses, damage data, and lower the performance quality of the information system, all of which can lead to the compromise of bank information. Therefore, banks use high-level password security systems to guard against these kinds of attacks. This survey will include a thorough analysis of the sophisticated password security measures employed by various banks as well as a comparison between nationalised and private sector banks from many angles.

The Value of Security Systems

Regarding Online Transactions and Banking Protecting customer and bank data and information requires integrating security solutions for online banking and transactions. Mujinga et al. (2018) claim that transactional activities and online banking have expanded dramatically and are now an essential part of peoples' daily lives. The sophistication of attacks has increased along with technological development. Both money and time are lost as a result of it. Sensitive and payment systems are also accessed as legitimate users, compromising personal information in addition to credentials and information of legitimate users being stolen. Salem et al. (2019) state that banks guarantee the transference of critical and sensitive financial information by implementing a dependable security mechanism. In addition, there have been cases where cybercriminals created phishing websites that mimic bank websites in an attempt to trick users into divulging private and sensitive information. It helps obtain data that will support expanding clientele for handling transactions and data, which raises financial risks and results in security lapses in institutions.

Cyberattacks on Online Banking Systems

The term "attacks on electronic banking systems" simply describes methods or strategies used to fraudulently access electronic banking transactions. examines assaults against online electronic banking, such as. a) Social engineering attacks: these involve deceiving victims into disclosing their true identities to scammers via social media. Customers' inadequate understanding of computer systems is exploited by fraudsters for their own fraudulent gain. In order to take advantage of their victims and scam them, they send texts, calls, or links (phishing and spooling) to clients demanding their private financial information.b.) Packet sniffers: To intercept sensitive data, such as passwords and credit card numbers, attackers set up surveillance on the link between the user's PC and the web server. Consequently, this makes it feasible to con these victims. c.) Port Scanners: Attackers employ a variety of strategies to obtain consumer information by identifying a system's entry points for customers through the use of port scanners. Here, software is installed to repeatedly scan data passing through the intended port until it detects customer banking information. d.) Trojans: A Trojan is a piece of software that poses as a host system and asks for a gateway before gaining access. Due to its capacity to connect covertly and transmit sensitive information about consumers' private information, Trojan is considered the most significant security threat to electronic transactions. The goal of Trojan development is anonymity. Data from a variety of clients, servers, and database systems can be filtered using them. They can be set up to monitor conversations using databases, online electronic mail, as well as additional sources. e.) Password Cracking: This entailed searching through hundreds of common keywords, words, activities, and names until a series of them was allowed access to a server. Brute Force and other vulnerability decrypting techniques were then used to crack the user name as well as password of a particular website for its clients.f.) Denial of Service Attacks: This type of attack overloads servers, making them susceptible. The method is to continuously load a large amount of work onto the server until it can no longer operate efficiently. The attacker then takes advantage of the server's current vulnerability to infect users' computers with malware or Trojan horses and gives them instructions on how to launch targeted attacks against the server. g.) Server defects: With millions of web servers in operation worldwide, server defects are utilised to fool the server intrusion detection system and provide attackers the chance to create threads. As a result, the server becomes more susceptible to threats and server defects. h.) Super User Exploits: Using this technique, attackers can take over the system and act as though they are the system administrator. This is accomplished by the attackers using scripts to alter the database or causing a buffer imbalance that renders the system unusable.

Techniques for securing electronic banking

The advances in technology, such as super-fast broadcast broadband connections for real-time transmission, the high definition of 3D and 4D video content in personal homes, the emergence of cloud computing, and the complemented physical network infrastructure such as WiFi, 3G, 4G, Wimax, etc., have enhanced and encouraged the application of technology in information processing and online businesses. On identical technology, electronic banking finds its functioning. Due to the sensitive nature of electronic banking, the following security precautions have been put in place:

I. Digital Certificate: A digital certificate needs a trusted third-party who ascertains the legitimacy of the transaction by signing the authentication certificates attesting to their validity. The authentication relies on a public key transaction (PKI) and certificate authority (CA). A digital certificate is used to authenticate both the user and the bank.

II. One-Time Password Tokens: A one-time password token is a second authentication factor that is a code in the form of a password required in a specified or random scenario created by the application and delivered to the registered device of the user. The operation is authenticated and proceeds if the password is entered as necessary within the set time frame. This safeguard makes acquired authentication data by fraudsters unusable for subsequent attempts; consequently, the password is updated dynamically and used once within the authorised time range.

III. One-Time Password Cards: A one-time password card is a card used in generating passwords that are used for a second authentication factor, like one-time password tokens. The difficulty with a one-time password card is that certain banks allow for the reuse of passwords produced over time, which makes them susceptible to assault.

IV. Browser Protection: Browser protection is a security model that is safeguarded at the internet browser level used to access the banking system. In browser protection, the user and their browser are safeguarded against known malware. This is performed by monitoring the memory region allotted by the browser with the purpose of identifying such malware as well as limiting credential theft and the collection of sensitive information.

V. Virtual Keyboard: In recent times, the virtual keyboard has been replaced by a more efficient technology that uses less computing power and has a slower transmission rate. A virtual keyboard is a gadget generally based on Java and software cryptography that permits mobility across various machines. A virtual keyboard hinders the effective use of key loggers, which collect information input into the device.

VI. Device Registering: in the event of registering with the banking system for an online transaction, the device to be used by the client is registered with the bank database (particularly in mobile banking). The bank will, in the event of a transaction, assure that the registered device is the one used for such a transaction; otherwise, such a transaction is rejected. For enhanced authentication, hardware fingerprinting methods are employed in combination with user identification using secret credentials.

VII. CAPTCHA: The CAPTCHA solution is an automated test intended to identify and render ineffective automated assaults against legitimate services. The CAPTCHA solution helps to shield the consumer from password-guessing assaults on their identity. The strategy sends information to the user in the form of jumbled pictures, which automated robots find tough to detect and process. When the user is able to input the scrambled picture properly, it makes him or her a valid user.

VIII. Short Message Service (SMS). SMS is used to send brief messages to a dedicated phone number of the owner of the account, asking consent to go forward with such a transaction.

IX. Device Identification: This approach is used jointly with device registration. The approach employs the physical properties of the user's device to identify the original and historical information about the user.

X. Positive Identification: In positive identification, the user is asked to offer some secret information only known to him as a means of identification. This information must have been given and recorded in the banking database against the customer's session at the first time of using the banking application.

XI. Passphrase: A passphrase is compared to a password, except that it is a phrase. Passphrase is a second authentication element that demands that a consumer identify himself by supplying a phrase owned by him as a gateway.

XII. Transaction Monitoring: Transaction monitoring needs the use of a business auditing model to monitor activities such as payment processing. The logs are monitored and examined to discover a trend of improper transactions at the business process level.

XIII. Education: As a fundamental criteria for electronic banking security defence, the user (customer) should have a very strong understanding of electronic banking security trends. Thus, it becomes vital for the consumer to supply strong passwords and prevent all sorts of online habits that are security-sensitive.

XIV. Personal Firewalls: This is focused on the usage of firewalls to restrict the types of traffic launched and directed to your computer. XV. Secure Sockets Layer (SSL): The SSL model is a protocol that encrypts data between the customer’s system and the site’ Initiate a handshake to transfer encrypted information back and forth between the customer♣s server. The SSL monitors a request made from an SSL-secured website by identifying the server as a trustworthy entity. ’s machine and the site's server. The objective is to guarantee that information moving back and forth between the customer’s machine and the site’s server is encrypted to render it worthless in case hackers intercept and sniff the information.

XVI. Server Firewalls: A firewall houses the web server to guarantee that all requests made reach the system via specialised ports only, and in certain situations, it ensures that all access is from particular physical machines only. The demilitarised zone (DMZ) of employing two (2) firewalls is the usual strategy used in server firewall security, which are:

(a) the outer firewalls that monitor the ingoing and outgoing HTTP requests while the client browser connects with the server.

(b) The inner firewalls, which reside behind the e-commerce server. The two firewalls are equipped with intrusion detection software, which is employed to detect any unwanted access attempt. The server firewalls also employed the honeypot server approach in addition to the DMZ. The honey pot is a resource, such as a false payment server, that is put in the DMZ to trick the hackers into believing that he or she has obtained entry into the system. Surveillance is deployed on the servers and continuously watched to identify access by an intruder.

XVII. Intrusion Detection and Audit of the Security Log: A good security system is one that can detect and prevent assaults. The intrusion detection system monitors the actions of the users of the system and uses the intelligent build-in software to identify suspicious behaviours either based on role functions or tries to access resources outside of sites. The intrusion detection system, upon detecting anomalies in the activities of the user, will block the user or log him or her out, then create notifications to the system administrator for comprehensive investigation and apprehension when feasible.

Objectives of the study

1. To examine the performance of numerous high-stage password protection systems employed by diverse banks, evaluating safety protocols and features across nationalised and private regional banks.
2. To study the impact of safety on consumer use and self-assurance in online banking, make use of correlation evaluation to quantify the link between certain safety features and person adoption.
3. To discover feasible areas for development within online banking security, targeting weaknesses and threats that are not effectively handled with the aid of present solutions.
4. To contribute to the knowledge and information of user behaviour in on-line banking practices, especially with cognizance of safety features and variables affecting on-line transaction options.

Need of the study

The widespread use of net banking necessitates robust safety features to safeguard private records and promote confidence. Online transactions are easy, but in addition, they place non-public information and coins at risk from quite a few risks, which include malware, phishing, and hacking. This research looks at cutting-edge security protocols, evaluates how well they work towards new threats, and pinpoints viable regions for improvement. Designing safe, dependable, and clean-to-use online banking systems that empower people and guard monetary security in virtual technology requires an intensive know-how of person behaviour, a thorough analysis of safety efficacy, and an investigation of the effect of protection on adoption.

Hypothesis

H01 (Null Hypothesis): The use of traditional banking techniques and online banking does not statistically significantly

H1 (alternative hypothesis): The use of online banking and conventional banking are statistically significantly correlated.

H02 (Null Hypothesis): There isn't any statistically large difference between the use of online banking by way of clients and security features.

H2 (alternative hypothesis): The use of online banking by customers is statistically extensively impacted by safety features.

Data Collection / Analysis

Table 1: Relationship between Traditional and Online Banking [Vimala, V. (2016). An evaluative study on internet banking security among selected Indian bank customers. Amity Journal of Management Research, *1*(1), 63-79]

Explanation	Correlation Coefficient	p-value
Demand Draft and Online Banking	-0.261	0.067
Security Lockers and Online Banking	0.104	0.472
Online and 24/7 Banking	-0.203	0.158
Internet Banking and Accessibility	-0.212	0.139

Table 2: Relationship between the security of online banking and the elements that affect it

Explanation	Correlation Coefficient	p-value
File security and security codes	-0.280	0.049
Database and Transaction Security	-0.427	0.002
File and Database Security	-0.304	0.032

Table 3: Internet Banking Usage Regression using Demographic Variables

Variable	Coefficient	p-value
Age	0.152	0.013
Gender	-0.243	0.002
Income	0.061	0.142

Table 4: Hypothesis Testing Results

Hypothesis	Test Statistic	p-value	Result
H01: No association between internet banking and traditional banking	F=2.46	0.034	Reject Null
H02: No impact of security on customer usage	t=-2.15	0.018	Reject Null

Future Suggestions

Future hints include a number of crucial regions on the way to ensuring a safe and wealthy online banking ecosystem: First and foremost, it's crucial to foster ongoing innovation in safety protocols, with a specific emphasis on sturdy information encryption, state-of-the-art threat detection, and the incorporation of present-day technologies like blockchain. Second, encouraging consumer training and awareness via centred projects and interactive marketing may additionally permit humans to recognise possible dangers and undertake secure online behaviours. Thirdly, so that it will alternate high-quality practices, jointly counter developing threats, and create standardised security frameworks, banks, IT companies, and regulatory companies ought to work together more intently. Ultimately, putting the desires of the person first while growing security features, which can be easy to apply and intuitive, will lead to broader adoption and increase confidence in online banking structures. We can control the continuously converting digital terrain and guarantee a safe and convenient destiny for online monetary transactions by adopting these ideas.

Conclusion

As a result, this study emphasises how vital strong security features are to secure the unexpectedly increasing online banking industry. It analyses distinctive dangers and modern security strategies, but it also highlights the need for ongoing innovation, personnel education, and teamwork to deal with changing issues. The documented hyperlinks between person adoption and security emphasise how essential it's to sell confidence and accept it as true with in-person transactions. Prioritising thorough safety techniques in addition to person-centric techniques will stay important in ensuring a secure, dependable, and on-hand destiny for online banking, empowering humans, and selling financial boom inside the virtual age as the technology progresses and cyber threats trade.

References

1. Mujinga, M., Eloff, M., & Kroeze, J. (2018). The internet of things: The security challenges for online banking. In Proceedings of the 2018 IST-Africa Week Conference (IST-Africa). IEEE.
2. Salem, O., Abdo, J., & Aljarallah, S. (2019). From threats to countermeasures: Dealing with the main security threats facing E-banking authentication. International Journal of Advanced Computer Science and Applications, 10(5).
3. Vimala, V. (2016). An evaluative study on internet banking security among selected Indian bank customers. Amity Journal of Management Research, 1(1), 63-79.
4. Cheney, J. S. (2008). An examination of the adoption of electronic banking: An integration of the technology acceptance model and theory of planned behavior (Doctoral dissertation, Auburn University).
5. AbuShanab, E., Pearson, J. M., & Setterstrom, A. J. (2010). Internet banking and customers' acceptance in Jordan: the unified model's perspective. Communications of the Association for information systems, 26(1), 23.
6. Aladwani, A. M. (2001). Online banking: a field study of drivers, development challenges, and expectations. International journal of information management, 21(3), 213-225.

7. Liao, Z., & Cheung, M. T. (2002). Internet-based e-banking and consumer attitudes: an empirical study. Information & management, 39(4), 283-295.
8. Grabner-Kräuter, S., & Faullant, R. (2008). Consumer acceptance of internet banking: the influence of internet trust. International journal of bank marketing.
9. Linck, K., Pousttchi, K., & Wiedemann, D. G. (2006). Security issues in mobile payment from the customer viewpoint.
10. Maditinos, D., Chatzoudes, D., & Sarigiannidis, L. (2013). An examination of the critical factors affecting consumer acceptance of online banking. Journal of Systems and Information Technology.
11. Rasiah, D. (2010). Theoretical framework of internet banking adoption in Vietnam. Journal of Global Business and Economics, 1(1), 57-75.
12. Lallmahomed, M. Z., Lallmahomed, N., & Lallmahomed, G. M. (2017). Factors influencing the adoption of e-banking in Mauritius. Telematics and Informatics, 34(4), 57-72.
13. Alkhowaiter, W. A. (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review. International Journal of Information Management, 53, 102103.
14. Hanafizadeh, P., Behboudi, M., Koshksaray, A. A., & Tabar, M. J. S. (2014). Mobile-banking adoption by Iranian bank clients. Telematics and Informatics, 31(1), 62-78.
15. Sarmah, B., Rahman, Z., & Kamboj, S. (2021). Customer's adoption of mobile banking services: an integration of UTAUT and trustworthiness. International Journal of Bank Marketing.