ISSN: 2755-0214

Journal of Economics & Management Research

SCIENTIFIC Research and Community

Review Article

Open Access

Securing Payments and Banking Systems from Cybersecurity Threats

Vandana Sharma

Leading Technology Organization, SF Bay Area, US

ABSTRACT

Countering cyber threats to the payment and banking system has emerged as a global challenge. This trend has compelled financial establishments to integrate risk into their operational models. Consequently, there is a pressing need to invest in advanced technologies and security protocols to counteract potential substantial financial losses and the compromising of sensitive information due to cyber assaults. The escalating prevalence of cybercrime poses a significant apprehension for various stakeholders within the financial realm. Typically, cyber-attacks are orchestrated through software systems operating within the digital domain. Thus, it is imperative to identify entities within the digital sphere and subsequently isolate threats to application security. This entails scrutinizing vulnerabilities and formulating defensive strategies. This study aims to explore diverse methodologies that identify digital assets, categorize cyber threats, establish security countermeasures, and align security strategies with different types and functionalities. By selecting suitable approaches to address security threats and defenses, IT professionals and users can collaboratively make informed choices to fortify a robust defense mechanism.

***Corresponding author**

Vandana Sharma, Leading Technology Organization, SF Bay Area, US.

Received: October 06, 2021; **Accepted:** October 13, 2021; **Published:** October 20, 2021

Keywords: Threat, Risk, Cyber-Attack, Financial Institution

Introduction

In the dynamic realm of modern banking and payment systems, the surge in technological innovations has revolutionized financial services. However, this progress has unveiled a parallel surge in sophisticated cyber threats targeting these vital sectors. The combination of delicate financial information, complex transaction procedures, and interconnected networks has amplified the landscape of vulnerabilities. As financial operations increasingly digitize, the urgency for robust cybersecurity measures intensifies. The potential fallout of a successful cyber breach in banking and payments is profound, encompassing data breaches, financial harm, service interruptions, and erosion of public confidence. Consequently, a comprehensive cybersecurity approach is imperative, transcending conventional practices. Effective defense within banking and payments demands proactive strategies that address technical loopholes, human behavior, and compliance with regulations. As finance becomes more digitized and interconnected, safeguarding against cyber risks is critical to uphold the trust, stability, and credibility of these systems.

Cybersecurity and the Financial Institution

If treated as a country, the realm of cyber-crime, anticipated to result in a staggering $6 trillion USD worth of global damages in 2021, would stand as the third-largest economy internationally, trailing only the United States and China. Prominent cyberattacks often encompass activities like denial of service, infrastructure breaches, phishing, and other data protection challenges [1]. The capital market and banks have encountered multiple instances of CEO whaling attacks, which pose a significant threat to the industry's cybersecurity. The financial services sector has faced a disproportionately higher number of cybersecurity incidents compared to other industries. Notably, 33% of major attacks are directed at the financial services domain. Given these circumstances, it is imperative to establish robust security protocols to counter cyber threats within the banking sector. Financial institutions have notably been impacted by ransomware attacks in recent times. Artificial intelligence and machine learning are currently utilized to thwart the efforts of hackers.

Threats to Security in Banking and Payments

The transition from traditional paper-based banking to digital transactions via computers, mobile devices, and gadgets has introduced both opportunities and threats to the system, jeopardizing both institutions and individuals. This study focuses on the escalating cybersecurity challenge in payment and banking systems. The evolving landscape of technological progress offers advantages alongside emerging complexities. Traditional problems like fraud and theft have metamorphosed into novel cybercrime through information technology [2]. The scope of cybercrime is continuously expanding, facilitated by information technology, transcending geographical boundaries and constituting a transnational menace. This dynamic renders monitoring, detection, prevention, and control more intricate. Notably, ransomware, denial of service attacks, and phishing directly impact commercial networks, complicating identification due to varying behavioral patterns across accounts. Alzoubi et al. identifies five key security concerns capable of undermining these systems. These are as follows

- **Unencrypted Data:** Clients trust systems for their data, such as PIN codes and credit card details, they think that the data is safe. However, due to limited awareness about data security, vulnerabilities persist. Often, data remains exposed, enabling malicious actors to exploit it for unauthorized account access and financial theft.

- **Malware:** Malware, an abbreviation for malicious software, refers to software crafted with the intention of infiltrating, harming, or obtaining unauthorized entry to computer systems and networks [3]. This category encompasses a range of manifestations, including viruses, worms, Trojans, ransomware, and spyware. Malware can cause a range of harmful effects, including data theft, system disruption, financial losses, and privacy breaches. It may compromise personal information, disrupt critical services, or render systems unusable. Ransomware can encrypt valuable data, demanding payment for its release. Spyware can clandestinely monitor online activities, compromising user privacy. Worms can spread across networks, consuming resources and causing network congestion. Overall, malware poses a significant threat to cybersecurity, requiring robust preventive measures like antivirus software, regular updates, and user vigilance to mitigate its impact.
- **Unreliable Third-Party Services:** Banks utilize external third-party providers that furnish improved services for payment and banking systems. Nonetheless, should these external systems be vulnerable to unauthorized access, it becomes straightforward for them to be breached. Such a situation could potentially lead to theft via the compromised third-party platform, with the ultimate consequence being severe damage to the bank's reputation.
- **Spoofing:** This is like pretending to be someone else, often called impersonation. Hackers do this to act as if they're the real account owner. To do this, they get someone's login details and use them to unlawfully access and steal from the victim [4]. This harms the individual more than the banks.
- **Altered Information:** When hackers modify data pertaining to cybersecurity systems, they gain an advantage in deceiving people into giving them money under false pretexts stated that this could lead to financial losses for both the bank and the payment system. These points reveal issues about security in banks and similar financial institutions. It also shows how problems in the banking industry and how things work affect consumers and are exploited by bad actors. In summary, this gives a basic idea of why strengthening and using cybersecurity measures should be thought about, especially by those using such systems.

Risks to Banking and Payment Systems

Risks to banking and payment systems include ransomware, denial of service, race condition, phishing, data breach and watering hole attacks.

- **Ransomware**
  Ransomware, categorized as a form of malicious software (malware), is created to encrypt a target's files or block their access to their computer system. This restrictive state persists until a payment, or ransom, is remitted to the perpetrator. When a system becomes infected by ransomware, critical files are encrypted, rendering them off-limits to the rightful owner. The attacker subsequently requests payment, frequently in the form of cryptocurrency, in return for furnishing the decryption key necessary to regain access to the files or restore system privileges. The ramifications of ransomware attacks can be dire, leading to data loss, disruptions in business operations, and financial setbacks. They may target individuals, businesses, or even critical infrastructure. Those who fall victim are confronted with a challenging choice: either comply with the ransom demand and trust that the attacker will furnish the decryption key, or decline payment and potentially forfeit access to crucial data. Preventing ransomware involves regular software updates, robust cybersecurity practices, backup solutions, and user education to avoid falling victim to phishing and other attack vectors that distribute ransomware. Figure 1 demonstrates Ransomware.

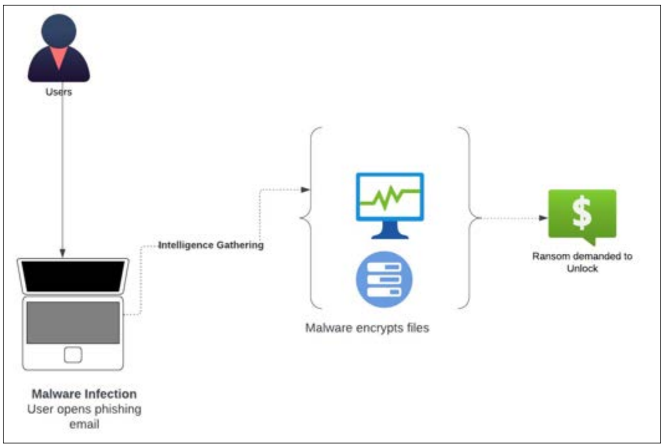

Figure 1: Ransomware

- **DDoS Attacks**
  The frequency and magnitude of DDoS attacks are surging. In fact, these attacks have surged almost 300% annually and the trend is set to worsen. In a distributed denial-of-service (DDoS) attack, hackers attempt to infect a network of devices, such as your computer, to create a bot army for assaulting major targets. Their aim isn't your personal data—it's much bigger. They seek to include your device in their vast bot army to disrupt giants like Google and Amazon. These incidents have made headlines, caused service disruptions and prompted the creation of cybercrime legislation. Figure 2 demonstrates DDoS Attack.

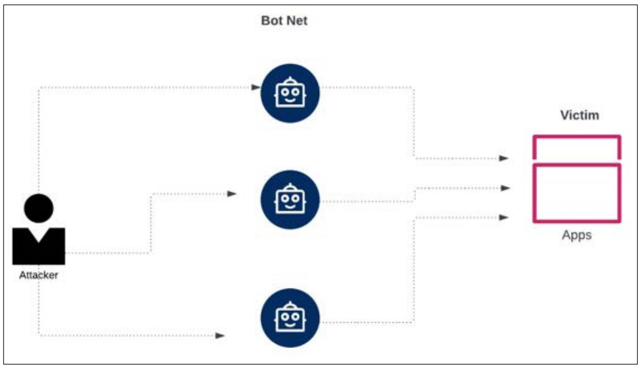

Figure 2: DDoS Attack

- **Race Condition**
  A race condition in cybersecurity refers to a situation where multiple processes or threads in a computer system attempt to access or manipulate shared resources simultaneously, potentially leading to unpredictable or unintended outcomes. This phenomenon arises when the timing and sequencing of these processes affect the final result, which can be exploited by attackers to manipulate the system's behavior. Within the realm of cybersecurity, malicious entities can leverage a race condition to circumvent security protocols or attain unauthorized entry to resources. For example, if a system is not properly synchronized, an attacker might execute

certain actions at precisely timed intervals to exploit the race condition and gain unauthorized access or privileges. To mitigate race conditions, robust programming practices, proper synchronization techniques, and careful design of multithreaded or multiprocessor applications are crucial. Failure to address race conditions can lead to vulnerabilities that attackers might exploit to compromise system integrity, confidentiality, or availability.

- **Phishing and Business Email Compromise**
  In a May 2017 FBI inquiry, it was revealed that over $5 billion had been illicitly taken from enterprises via email breaches, encompassing techniques like phishing. Phishing refers to the act of a criminal impersonating a trustworthy source to extract information or funds. Numerous variations of phishing exist, such as spear phishing and whaling. In spear phishing, the attacker assumes the identity of the CEO or a company representative to request money or sensitive data. If banks and payment systems fail to detect such attackers, they expose themselves to potential financial losses and the jeopardy of compromising customer data, as indicated by the recorded 37.3 million instances.

- **Data Breach**
  A data breach transpires when unauthorized individuals manage to penetrate an organization's systems and gain entry to confidential or sensitive information. This encompasses personal details, financial records, intellectual property, or any other kind of sensitive data. Data breaches can result from various cyberattacks, including hacking, phishing, malware infections, and more. The attackers seek to steal, expose, or manipulate the compromised data for financial gain or other malicious purposes.

- **Watering Hole Attacks**
  Watering hole attacks are gaining popularity due to employees becoming better at recognizing phishing emails. A watering hole attack is a cyberattack strategy where hackers compromise websites that their intended victims frequently visit. These victims are chosen based on their relevance to the hackers' goals, such as their industry or affiliations. Instead of directly targeting the victims' systems, hackers infect the compromised websites with malicious code. When the victims visit these sites, their devices become infected with malware without their knowledge. This tactic exploits the trust victims place in familiar websites, making detection harder. Watering hole attacks are particularly effective against targets with strong security measures, as they exploit human behavior rather than directly targeting system vulnerabilities. Once compromised, the attacker can gain access to sensitive information, launch further attacks, or potentially infiltrate a victim's network.

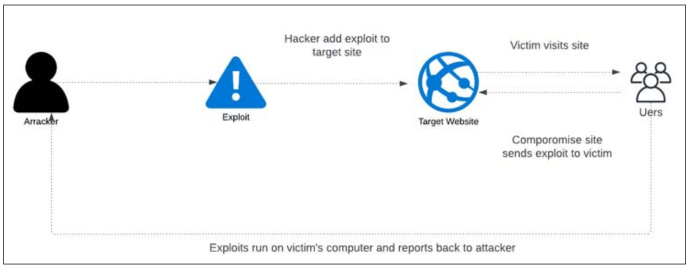
Arracker
Exploit
Hacker add exploit to target site
Target Website
Victim visits site
Uers
Comporomise site sends exploit to victim
Exploits run on victim's computer and reports back to attacker

Figure demonstrates Ransomware

Legal Regulations, Ethical Norms and Cybersecurity

Laws establish clear boundaries for business activities. Cybercrime exploits open networks and diverse devices to gain rewards. Information remains a prized internet asset. Therefore, laws define online legality, detailing offenses and penalties. Legislative bodies create necessary laws to safeguard information systems and assets within their jurisdiction [5]. Solely the legislature shapes cyber law and policy. In financial sectors, violating laws results in significant fines and penalties, with culprits facing prosecution by the criminal justice system. Different countries around the globe have put in place the subsequent legislations to protect banking systems [6].

- **Bank Secrecy Act (BSA), United States:** This law mandates that financial establishments maintain records and disclose specific transactions to aid in the prevention of money laundering and other financial illicit activities.
- **Payment Services Directive (PSD2), EU:** This law regulates payment services and enhances security for electronic payments and transactions within the European Union.
- **Financial Services and Markets Act (FSMA), UK:** This law establishes a regulatory framework for financial services and markets in the UK, including banking and investment activities.
- **Banking Act, Singapore:** Governs banking activities and provides regulatory measures to maintain the stability and integrity of the financial system.
- **Banking Regulation Act, India:** This law regulates and supervises banks in India to ensure their proper functioning and maintain monetary stability.
- **Basel III Framework:** An international set of banking regulations aimed at improving the banking sector's resilience by setting higher capital requirements and risk management standards.
- **Bank of Japan Law, Japan:** This law governs the functions and operations of the Bank of Japan, the country's central bank, and ensures the stability of the financial system.
- **Financial Institutions Act, Canada:** This act provides regulatory oversight for banks, credit unions, and other financial institutions to protect consumers and maintain financial stability.
- **Australian Prudential Regulation Authority (APRA) Act, Australia:** This act establishes the APRA's regulatory powers over banks, insurers, and superannuation funds to ensure their safety and stability.
- **Banking Act, South Africa:** This act regulates banking institutions and provides guidelines for their operations, promoting financial stability and consumer protection [7].

Steps to Secure Information and Banking Systems

Securing online banking payment systems relies heavily on safeguarding information. This means protecting data as it moves within the financial system and resides in the bank's database, ensuring it remains private. The need to address this arises from risks like unauthorized access, data changes, and disruptions. Therefore, it's crucial to use specific technological tools to bolster defenses against attackers and create a secure banking network environment. Within the operational realm of the bank, the subsequent procedures are executed to guarantee the protection of confidential and delicate data owned by both the bank and its customers. The subsequent section outlines the procedure and security precautions that financial institutions should adhere to.

- **Authentication**
  It involves the procedure of confirming the identity of an individual, system, or device to ensure their claimed identity is accurate. In banking systems, authentication plays a pivotal role in safeguarding sensitive financial information and transactions. Authentication in banking systems is typically implemented through multifactor authentication (MFA) methods to enhance security [8]. MFA involves combining two or more different authentication factors to establish identity: Something You Know: This includes traditional password or PIN-based authentication. Users provide a secret piece of information that only they should know. Something You Have: This entails having a physical item like a smart card, token, or a registered mobile device that produces time-sensitive codes. Something You Are: This involves biometric authentication, where physical characteristics like fingerprints, retina scans, or facial features are used to verify identity. Somewhere You Are: Occasionally, geolocation data is used as an additional factor, confirming that the user's physical location matches their expected location. In banking systems, during login or transaction authorization, users are required to provide multiple factors for verification. As an illustration, a user could input a password, receive a unique code on their mobile device, and offer a fingerprint scan. This stratified technique notably bolsters security, as even if one factor is compromised, an attacker would still require access to the other factor(s) to achieve entry. By implementing multifactor authentication, banking systems bolster their defenses against unauthorized access and fraudulent activities, ensuring the confidentiality and integrity of customers' financial data [9].

- **Authorization**
  This is the procedure of granting or denying entry to particular resources contingent on the authenticated privileges of a user. In banking systems, this ensures users can only access permitted information and transactions, preventing unauthorized actions. Banking systems execute authorization by employing role-based access control (RBAC) and meticulous fine-grained access control mechanisms. RBAC assigns roles with predefined permissions, while fine-grained control defines specific permissions for users or groups. After authentication, a user's identity and permissions are verified. When accessing data or functions, the system checks if their permissions match the request. If authorized, access is granted; if not, it's denied. Effective authorization limits data breaches, maintains compliance, and secures financial information, protecting both customers and the banking system.

- **Audit Requirements**
  Legal mandates compel financial institutions to conduct audits. Thus, it's incumbent on authorized personnel to regularly audit all activities on the bank's servers and database. Audit records are cross-referenced with backed-up data containing the bank's pre- and post-transaction values. This process logs transaction specifics such as date, terminal ID, user ID, name, bank domain, timestamp, and transaction outcome.

- **Integrity**
  The cornerstone of the banking and payment system is data integrity. In essence, it entails ensuring that all user data remains unchanged upon reaching the recipient. During transmission over the internet, data can be tampered with by external parties within an unsecured system before it reaches its destination. Additionally, stored data in the database must be protected against malicious alterations. Techniques such as digital signatures and Message Authentication Codes (MAC) are frequently utilized to maintain the integrity of data. This assurance of data accuracy from the source is pivotal for the success of the banking system.

Conclusion

This study examines factors impacting financial institutions' threat awareness and solutions, offering applicable insights to banks, payment systems, and organizations globally. As online banking rises, post-COVID-19, cybersecurity gains importance. Major banks employ security policies and insurances despite escalating cyberattacks. Limited security studies exist despite threats' significance and awareness, laws, human aspects, and adherence to standards being crucial. Cybercrime's borderless growth demands safeguarding banks, economic pillars. Banks prioritize security, defending against fraud and hackers, protecting assets and customer data. This study advocates fortified defense for Banking and Payment systems, aligned with prevailing cyber threats. Attackers target financial gains, underscoring the need for vigilant protection. Institutions must anticipate attackers using cybersecurity tactics for data theft and online fraud, ensuring secure financial services. Without such measures, disruptions, economic decay, and national instability loom.

References

1. Vieira A, Sehgal A (2018) How banks can better serve their customers through artificial techniques. In Digital marketplaces unleashed. Springer, Berlin, Heidelberg pp: 311-326.
2. Siddiqui MZ, Yadav S, Husain MS (2018) Application of artificial intelligence in fighting against cyber-crimes: A REVIEW. International Journal of Advanced Research in Computer Science 9: 118.
3. Giri S, Shakya S (2019) Cloud computing and data security challenges: A Nepal case. International Journal of Engineering Trends and Technology 67: 146-150.
4. Wewege L, Lee J, Thomsett MC (2020) Disruptions and digital banking trends. Journal of Applied Finance and Banking 10: 15-56.
5. Bose R, Chakraborty S, Roy S (2019) Explaining the workings principle of cloud-based multifactor authentication architecture on banking sectors. Amity International Conference on Artificial Intelligence 764-768.
6. Antrosio JV, Fulp EW (2005) Malware Defense Using Network Security Authentication: 3rd IEEE International Workshop on Information Assurance 43-54.
7. Iguer H, Medromi H, Sayouti A, Elhasnaoui S, Faris S (2014) The Impact of Cyber Security issues on Business and Governments: A framework for implementing a Cyber Security Plan. International Conference on Future Internet of Things and Cloud 316-321.
8. Goh J, Kang MH, Koh ZX, Lim JW, Ng CW, et al. (2020) Cyber Risk Surveillance: A Case STUDY of Singapore. International Monetary Fund 1-30.
9. B von Solms (2015) Improving South Africa's Cyber Security by cyber securing its small Companies: IST-Africa Conference 1-8.