International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 6 No. 22 March - April - 2025

Hidden Cyber Security Threats Targeting Virtual Banks in 2025

Gurunath S. Deshmukh
Assistant Professor, Smt Sushiladevi Deshmukh Senior College, Latur
Corresponding Author – Gurunath S. Deshmukh

DOI - 10.5281/zenodo.15532391

Abstract:

The banking sector is expected to pass primarily online through 2025, leading to an increase in interaction between cybersecurity and banking. In response to the escalation of the threat, financial institutions increased their cybersecurity budget by 89% in 2024. The key incident involving a virtual Chinese bank on the early days affected by the DDOS attack highlights the weaknesses online banks are facing only online banks. Advanced cybercrime tactics using ransomware and social engineering aimed at both employees and customers and virtual banks that rely on digital platforms. Risk situations will likely develop due to hidden cybersecurity threats, such as AI-controlled attacks and quantum computer risks. Cyberattacks in the financial sector have been rising dramatically since 2019, with 333% violations increasing by 333%, and ransomware attacks attack 59% of financial institutions in 2024. To combat these threats, banks are leveraging security measures such as realtime transaction monitoring, biometric authentication, and AI- based fraud detection systems. The weaknesses and misconceptions of cloud infrastructures offer additional challenges. This will surprise you with the exploitation accidents discovered between 2021 and 2022. Insider threats are also increasing due to remote work environments, requiring effective monitoring solutions. While cyber threats develop, virtual banking systems need a comprehensive approach that includes zero trust architecture, AI-enabled anomaly detection, and continuous safety verification frames to improve defense against sophisticated attacks and at the same time ensure compliance with regulatory standards.

Keyword: ***Virtual Bank Zero Trust Architecture Cyber Attack Advanced Persistent Threats Security Information And Event Management.***

Introduction:

The banking sector will shift almost entirely online by 2025. This change makes cybersecurity and banking more connected than ever. Financial institutions know the risks. Their cybersecurity budgets jumped up 89% in 2024 to curb rising threats.

Security risks pose a major challenge to virtual banks because they rely completely on digital platforms. A Chinese virtual bank learned this lesson the hard way. Their launch day turned into a nightmare after a devastating DDoS attack. Cybercriminals have become smarter. They now target both employees and customers through advanced ransomware and social engineering tactics.

The virtual banking landscape will face hidden cybersecurity threats in 2025. Our team scrutinizes ground attack scenarios and provides expert solutions to protect sensitive financial data. The analysis covers AI-powered threats and quantum computing challenges. These insights help build stronger virtual banking systems that can withstand future attacks.

The Evolving Landscape of Virtual Banking Security in 2025:

Virtual banking has changed how financial services handle security. Cyber attacks have led to data breaches that jumped by 333% since 2019. Financial services reported 744 cases in 2024, up from 172 cases in 2019 [1].

The Move from Traditional to Virtual Banking Security Models:

Virtual banks work through digital channels and offer their services only through internet and mobile apps. Traditional banks use technology to support their operations. Virtual banks, however, are tech companies that provide financial services [2]. This basic difference means they need a complete security overhaul.

Europe's Open Banking initiative and PSD2 started this change. These allowed other companies to access customer's banking data through APIs [3]. This created new security needs, especially since virtual banks must protect their only way to reach customers - the digital platform.

Banks now work to add better security through:

- Real-time transaction monitoring systems
- Biometric authentication methods
- AI-powered fraud detection mechanisms
- Cloud-native security frameworks

Key Statistics: Virtual Bank Cyber Attacks in 2024-2025:

New data shows cyber threats against banks are rising fast. A ransomware attack now costs INR 153.57 million to fix, without counting the ransom payment [1]. Phishing attacks have grown by 4,151% since late 2022 [1].

Early 2024 saw about 8 million DDoS attacks [1]. Ransomware hit 59% of financial institutions [1]. On top of that, IoT malware attacks grew by 107% in 2024 [1], which suggests criminals are finding new ways to attack.

Why Virtual Banks Face Unique Cybersecurity Challenges:

Virtual banks deal with special security problems because they run everything digitally. While cyber attacks hurt traditional banks, they could destroy virtual banks completely [2]. Here's why they're more vulnerable:

Virtual banks use more technology and work with many vendors. This bigger digital footprint makes them more open to internal problems and outside threats [2].

These banks must balance new features with strong security. To cite an instance, when they run promotions, unexpected customer traffic has caused system problems. This shows how hard it is to keep systems both accessible and secure [2].

Working with other companies creates another risk. Each connection to an outside system gives attackers a possible way in. Banks need to check these connections carefully and watch them all the time [2]. Even when they share responsibilities with others, the bank's leaders are still responsible.

Rules and regulations create special challenges for virtual banks. Some places, like Hong Kong, want virtual banks to have better cyber protection than traditional banks, which can adjust their security based on risk [2].

There's another reason to worry - personal responsibility. Board members and top managers could be personally liable if cyber attacks or data breaches happen [2]. Even though virtual banks hire skilled people, they still need to balance new ideas with security awareness.

Advanced Persistent Threats Targeting Banking Infrastructure:

Advanced persistent threats (APTs) have become sophisticated cyber attacks that target banking infrastructure. These attackers maintain unauthorized network access for long periods. Their covert operations focus on stealing data rather than causing system outages [4].

AI-Powered Attack Vectors Against Banking APIs:

AI has altered the map of cyber attacks against banking APIs. Recent data shows API attacks in India grew by 62% in the first half of 2024 [5]. APIs faced 68% more attacks than websites. DDoS attacks surged 94% quarter-over-quarter [5].

AI-powered attacks show five characteristics that make them dangerous:

- Attack automation for faster deployment
- Quick data gathering capabilities
- Advanced customization options
- Reinforcement learning abilities
- Precise employee targeting mechanisms [6]

These AI-enabled threats adapt to avoid detection patterns. Traditional security measures struggle to identify them [6]. Security researchers have found threat actors who utilize large language models to improve phishing campaigns and create convincing fake personas [6].

Quantum Computing Threats to Banking Encryption:

Quantum computing creates an unprecedented risk to banking encryption systems. Studies show 60% of organizations in Canada and 78% in the US believe quantum computers will become mainstream by 2030 [7]. About 60% of respondents think cybercriminals will use quantum capabilities to decrypt current security protocols [7].

Banking systems face these quantum threats:

1. Breaking asymmetric encryption through advanced algorithms
2. Compromising data integrity via forged digital signatures
3. Decrypting historically stored sensitive information
4. Undermining blockchain-based technologies [8]

Financial institutions that manage personal data must protect it for 5, 10, or 20 years [7]. Organizations need quantum-resistant cryptography now to protect against "harvest-now, decrypt-later" attacks. Adversaries store encrypted files until quantum computers can break current encryption methods [7].

Zero-Day Exploits in Banking Software: Case Studies:

Zero-day attacks pose one of the most dangerous threats to banking infrastructure. They exploit unknown vulnerabilities before developers can patch them. The finance sector remained a top target for these attacks in 2023 [9].

A Chrome zero-day vulnerability affected banking applications in 2021. The exploit came from a bug in the V8 JavaScript engine that could compromise financial transactions [10]. In 2020, attackers used a zero-day attack on Apple's iOS platform to remotely compromise banking applications on iPhones [10].

Zero-day attacks on banking systems lead to severe problems:

- Unauthorized access to sensitive customer data
- Extended periods of system compromise
- Major operational disruptions
- Substantial regulatory fines

- Long-term reputational damage [9]

Banks must adopt an integrated approach with zero trust architecture (ZTA) frameworks to curb these threats. These solutions help banks segment their networks into distinct zones. This creates roadblocks that stop malware from spreading through internal systems [9]. Banks can identify and respond to suspicious activities by monitoring network traffic, device activities, and user behavior [9].

Social Engineering Tactics Evolving for Virtual Bank Customers:

Social engineering attacks on virtual bank customers show new levels of sophistication. Bank fraud incidents rose by 56% in the last year [11]. These attacks now combine cutting-edge technologies with psychological manipulation to break through banking security.

Deep Fake Voice Authentication Bypass Techniques:

Voice authentication systems serve as secure biometric methods for banking transactions but face major threats from deepfake technology. Tests show that audio samples sound fake to human ears yet successfully bypass voice biometric systems [12]. Deepfake attacks now succeed 75% of the time with just five minutes of setup [13].

A UK energy firm's case highlights these risks. Criminals used AI-generated audio to copy a chief executive's voice and transferred INR 20,504,449.55 without authorization [14]. These attacks target voice authentication systems through:

- AI algorithms that copy and analyze voice characteristics
- Speech generation that matches target voice patterns
- Poor audio quality in cellular networks [13]

Targeted Phishing Campaigns Using Banking App Clones:

Banking app clones mark a new phase in phishing tactics. Criminals create perfect copies of real banking applications and distribute them through trusted platforms like Google Play. These harmful apps wrap around genuine banking software, which makes them hard to detect [15].

The Criminal Investigation Department found cybercriminals selling cloned versions of major bank apps at INR 2,000 each [16]. These apps reach customers through:

1. Bulk SMS messages with phishing URLs
2. Malicious dashboard app installations
3. Automatic data theft systems [16]

These attacks work because they look exactly like real banking interfaces. The installed apps steal user credentials and often collect specific data points to plan future attacks [15].

Customer Data Harvesting Through Third-Party Financial Apps:

Third-party financial apps create privacy risks that most customers don't know about. A complete survey shows 80% of users don't know fintech apps use third-party providers to collect financial data [1]. About 76% remain unaware these apps might sell their personal information to marketing and research firms [1].

Data collection through these apps raises red flags:

- 77% of users don't know apps keep access after deletion
- 78% miss that apps access personal data even when closed
- 80% remain unaware of apps' limited security breach liability [1]

Risks grow as these applications rely on other third parties to get account information, which exposes sensitive data further [17]. Third-party apps store online user IDs and passwords forever, even for one-time transactions, and might collect data unrelated to the original transaction [17].

Current social engineering attacks focus on human psychology through AI-powered chatbots and voice assistants that act like humans [18]. These advanced techniques make it hard to tell real from fake communication, which makes standard security measures less effective.

Virtual banks must build strong defenses using behavioral analysis, biometrics, and transaction monitoring to curb these threats [18]. Customer education remains the best defense, yet 65% of fraud victims blame themselves when these schemes succeed [11].

Cloud Infrastructure Vulnerabilities in Banking Platforms:

Cloud infrastructure vulnerabilities create growing challenges for banking platforms. A 95% increase in cloud exploitation incidents occurred from 2021 to 2022 [2]. Gartner predicts that customer-side misconfigurations will cause 99% of cloud security failures through 2025 [19].

Misconfigured Cloud Security Settings: Common Pitfalls

Banking platforms often face critical security gaps due to misconfigured cloud settings. Studies show that 27% of organizations dealt with public cloud security incidents. Misconfigurations caused 23% of these breaches [19]. These vulnerabilities show up through:

- Unrestricted outbound access enabling data exfiltration
- Disabled logging systems hampering threat detection
- Excessive account permissions expanding attack surfaces
- Poor network segmentation allowing lateral movement [20]

Cloud misconfigurations in banking environments cost organizations an average of INR 375.49 million per incident [21]. Improper access controls, weak encryption protocols, and poor monitoring mechanisms are the main reasons behind these breaches [21].

Container Escape Attacks in Banking Microservices:

Container escape attacks pose a growing threat to banking microservices architectures. These attacks let malicious actors break free from containerized environments and potentially compromise entire banking systems [2]. Research shows that container escapes usually happen through:

1. Exploitation of high-privilege capabilities retained during container creation
2. Manipulation of runtime socket techniques granting access to host directories
3. Using misconfigured sensitive mounts within container settings [2]

Container escapes become more dangerous when threat actors access resources outside the container. This leads to data theft and privilege escalation [2]. Many containers exposed to the internet increase security risks as attackers use retained capabilities for various escape methods [2].

Data Residency Challenges Across Global Cloud Providers:

Data residency creates complex challenges for virtual banks operating in multiple jurisdictions. Financial institutions must follow different regulatory requirements. Some nations require strict data localization within their borders [3]. Countries worldwide have created laws to control cross-border data movement to prevent security breaches [3].

Banks must deal with:

- Different regulatory frameworks across regions
- Varying data transfer restrictions between jurisdictions

- Requirements for local infrastructure investment
- Evolving privacy laws impacting data storage [3]

Global financial institutions face major operational disruptions and heavy financial penalties for not complying with data residency requirements [3]. The internet's mesh architecture makes compliance harder by making it difficult to restrict traffic paths between international locations [22].

Banks must implement complete cloud security posture management (CSPM) strategies to strengthen cloud infrastructure security [20]. This requires constant monitoring of cloud configurations, regular security audits, and automated compliance tools [21]. Cloud environments change rapidly and need careful oversight. Even small misconfigurations can expose critical banking systems to major risks [23].

Insider Threats in Remote-First Banking Operations:

Remote-first operations in virtual banking have led to more insider threats. Financial institutions saw a 20.3% jump in internal security breaches [24]. Distributed workforces accessing sensitive banking systems created a bigger attack surface.

Privileged Access Misuse in Virtual Banking Environments:

Banking operations face substantial risks from credential theft through privileged access misuse. Bad actors with privileged account credentials can wreak havoc - from deleting databases to installing malware on critical systems [25]. Data breaches happen most often due to privilege misuse, making it the third highest security threat [26].

A worrying pattern shows administrators often use high-level accounts for everyday tasks. This lets privileged users give others expanded access, which makes the number of high-standing privileges grow beyond control [26]. The danger grows when hackers target stored credentials, especially those of privileged administrators.

Monitoring Solutions for Distributed Banking Teams:

Remote work creates new challenges for monitoring teams. IT resources often struggle with the flood of traffic logs and event data [6]. Banks use layered monitoring approaches to tackle these challenges:

- Real-time tracking of privileged session activities
- Advanced behavioral monitoring systems
- Complete activity logs for compliance audits
- Automated anomaly detection tools [25]

Monitoring solutions work best when they can spot irregular logins, strange data transfers, and unusual behavior [6]. Banks can spot threats early through security information and event management (SIEM) and user entity behavior analytics (UEBA) before they become serious breaches [5].

Psychological Factors Behind Banking Insider Attacks:

Learning about what drives insider threats is vital for prevention. Research shows two types of insider threats: intentional (malicious) and unintentional (accidental) [27]. Several factors drive malicious threats:

1. Money problems leading to data theft
2. Personal beliefs that clash with company values
3. Grudges against management
4. Thrill-seeking without wanting money [28]

Remote work adds new stress that can trigger insider incidents. Workers who feel isolated might disconnect from their jobs and become unhappy [5]. The lack of face-to-face contact makes it harder to get quick help, which leads to more accidental security breaches [5].

Studies show that 27% of insiders showed warning signs before security incidents [7]. These signs showed up as more complaints about pay, strange cell phone use at work, outbursts at coworkers, and keeping away from team members [7].

Banks need both technical controls and mental health support to reduce these risks. They should offer employee assistance programs, keep communication open, and provide regular security training [5]. But harsh punishment for honest mistakes should be avoided. Strict penalties can make people feel treated unfairly, hurt morale, and even cause revenge actions [27].

Expert Solutions: Building Resilient Virtual Banking Systems:

Virtual banking systems need a comprehensive approach to handle the growing number of cyber threats. Cyber attacks grow more sophisticated each day, and financial institutions must find new ways to protect their digital assets and keep their customers' trust.

Zero-Trust Architecture Implementation for Banking Platforms:

Zero Trust Architecture (ZTA) has become a vital framework to boost cybersecurity in virtual banking environments. This approach follows the principle of "never trust, always verify." Users, devices, and applications must go through continuous authentication and authorization to access the network [8]. Banks that use ZTA can substantially reduce unauthorized access and system breaches.

Key components of ZTA implementation in banking platforms include:

1. Granular access controls based on user identity, device health, and context
2. Micro-segmentation of network resources to limit potential damage from breaches
3. Continuous monitoring and real-time threat detection
4. Strong encryption protocols for data in transit and at rest

About 60% of organizations in Canada and 78% in the US believe quantum computers will become mainstream by 2030. This development poses major risks to current encryption methods [29]. Banks must act now to use quantum-resistant cryptography that protects against "harvest-now, decrypt-later" attacks [29].

AI-Based Anomaly Detection for Transaction Monitoring:

AI and Machine Learning have transformed how virtual banking systems monitor transactions. These technologies help financial institutions analyze huge amounts of data in real-time. They can spot suspicious patterns and potential fraud with remarkable accuracy.

AI-powered anomaly detection systems provide several benefits:

- Better pattern recognition capabilities
- Fewer false positives, which lets security teams focus on real threats
- Smart algorithms that adapt to new attack methods
- Better analysis of user behavior and transaction history

A newer study, published in [30], shows that AI-based fraud detection systems can handle massive amounts of transaction data better than traditional systems. These systems adapt faster to new fraud strategies and stay ahead of cybercriminals [30].

Regulatory Compliance Automation Tools for Virtual Banks:

Virtual banks face growing pressure to follow complex regulatory requirements. Automation tools have become essential to manage these challenges well.

Regulatory compliance automation brings several advantages:

1. Simpler reporting processes
2. Real-time monitoring of regulatory changes
3. Less risk of human error in compliance tasks

4. Better audit trails for regulatory inspections

To cite an instance, Quantivate Compliance Management Software offers a central platform to track regulatory and legal changes, organize compliance documents, and manage processes [31]. Banks can watch their compliance costs by linking changes to affected business units, processes, policies, and controls [31].

LexisNexis Legal & Professional® provides compliance alert services that watch regulatory changes from 13,000 agencies. These cover 52,000 measures and 600 document types [31]. Banks can create custom alerts that match their specific needs.

Continuous Security Validation Frameworks

Continuous Security Validation (CSV) helps ensure banking security measures work effectively. Companies must verify that their security controls perform as intended [32].

Key components of CSV frameworks include:

- Automated attack simulations based on real-life scenarios
- Regular checks of security control effectiveness
- Finding vulnerabilities and misconfigurations
- Setting priorities for fixes based on risk assessment

BAS (Breach and Attack Simulation) tools are crucial for CSV. They help banks copy cybercriminal tactics throughout the entire kill chain [32]. These simulations run around the clock to find potential security gaps.

Without doubt, CSV helps virtual banking systems in many ways:

1. Finding security weaknesses early
2. Better incident response capabilities
3. Meeting regulatory requirements
4. Making security investment decisions based on data

ISACA's research highlights CSV's importance. Threats and systems change daily, making traditional testing methods inadequate [9]. Banks that use CSV maintain strong security against evolving threats.

Banks must encourage security awareness throughout their organizations to make these solutions work. The core team needs regular training programs, clear security policies, and teamwork between IT, security, and business groups.

Financial institutions should also use advanced technologies like cloud-native security frameworks and biometric authentication. These innovative approaches, combined with the solutions above, help virtual banks build strong systems that can handle complex cyber threats in 2025 and beyond.

Results:

The results show that virtual banks face significant cybersecurity risks, including advanced ransomware, social engineering tactics, AI-powered threats, and quantum computing challenges.

The study found that Zero Trust Architecture, AI-based anomaly detection, and continuous security validation frameworks are effective in boosting cybersecurity in virtual banking environments. The study also found that regulatory compliance automation can simplify reporting processes and reduce the risk of human error. Additionally, the study highlights the importance of mental health support, technical controls, and employee training in reducing cybersecurity risks.

Conclusion:

Virtual banks face unprecedented cybersecurity challenges as we move toward 2025. Data violations have jumped by 333% since 2019. These numbers reveal why banks just need strong security measures now.

Financial institutions must tackle multiple threats at once. AI-powered attacks target banking APIs. Quantum computing puts current encryption standards at risk.

Social engineering tactics have grown more sophisticated. Criminals now use deepfake voice authentication bypasses and create convincing banking app clones to trick users.

Cloud infrastructure weaknesses create more problems, especially when you have misconfigured settings and container escape attacks. Remote work has made insider threats worse. Banks need improved monitoring solutions and psychological support systems.

Building resilient virtual banking systems needs an all-encompassing approach to security. Zero-trust architecture, AI-based anomaly detection, and continuous security validation frameworks are the most important components. Banks that use these expert solutions and automate their compliance checks stand stronger against new cyber threats.

Virtual banking security's future relies on quick threat detection, employee training, and advanced technological solutions. Organizations must stay alert as cybercriminals develop new attack methods. Success in this changing digital world depends on how well banks evaluate and improve their security measures to protect sensitive financial data and keep customer trust.

References:

1. https://www.prnewswire.com/news-releases/new-research-reveals-consumers-remain-uninformed-of-fintech-app-data-collection-practices-301434520.html
2. https://unit42.paloaltonetworks.com/container-escape-techniques/
3. https://incountry.com/blog/data-residency-for-financial-services-companies/
4. https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html
5. https://www.securonix.com/blog/technical-solutions-remote-working-and-insider-threats/
6. https://bfsi.eletsonline.com/managing-insider-threats-at-financial-institutions-during-remote-work/
7. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1094&context=jss
8. https://cloudsecurityalliance.org/blog/2023/09/27/putting-zero-trust-architecture-into-financial-institutions
9. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/continuous-security-validation
10. https://www.kaspersky.com/resource-center/definitions/zero-day-exploit
11. https://www.pymnts.com/fraud-prevention/2024/fraudsters-shift-tactics-to-customers-challenging-financial-institutions-to-innovate/
12. https://www.netspi.com/blog/technical-blog/adversary-simulation/using-deep-fakes-to-bypass-voice-biometrics/
13. https://www.securing.pl/en/voice-biometrics-how-easy-is-it-to-hack-them-with-ai-deepfake/
14. https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for
15. https://threatpost.com/cloned-android-banking-app-hides-phishing-scheme/106867/
16. https://www.the420.in/alert-new-phishing-attack-scammers-creating-clone-of-banking-apps-to-steal-your-money/
17. https://www.financialexpress.com/life/technology-how-safe-are-third-party-financial-mobile-apps-understanding-security-risks-and-ways-to-safeguard-your-personal-data-2960162/
18. https://www.cleafy.com/insights/social-engineering-attacks-in-online-banking-how-to-identify-and-fight-them

19. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/what-is-a-cloud-security-misconfiguration/
20. https://www.crowdstrike.com/en-us/blog/common-cloud-security-misconfigurations/
21. https://etedge-insights.com/technology/cloud/common-cloud-security-misconfigurations-and-how-to-prevent-them/
22. http://www.omg.org/cloud/deliverables/CSCC-Data-Residency-Challenges.pdf
23. https://vulcan.io/blog/cloud-misconfiguration/
24. https://www.proofpoint.com/sites/default/files/e-books/pfpt-au-eb-managing-insider-threats-in-financial-services.pdf
25. https://www.microsoft.com/en-in/security/business/security-101/what-is-privileged-access-management-pam
26. https://www.oneidentity.com/community/blogs/b/privileged-access-management/posts/staying-ahead-of-privileged-access-management-security-risks-success-strategies
27. https://pmc.ncbi.nlm.nih.gov/articles/PMC8550909/
28. https://www.linkedin.com/pulse/psychology-behind-insider-threats-understanding-mindset-shadowsight-y2qgc
29. https://www.techmagic.co/blog/ai-anomaly-detection/
30. https://www.tookitaki.com/compliance-hub/innovating-transaction-monitoring-with-ai-for-real-time-compliance
31. https://quantivate.com/industries/banks/bank-regulatory-compliance-manager-software/
32. https://cymulate.com/blog/what-is-continuous-security-validation/