International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||10||Pages||1631-1646||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i10.ec10

Cybersecurity Threats and Vulnerabilities in Online Banking Systems

FNU Jimmy

Senior Cloud Consultant, Deloitte, USA

Abstract

The rapid expansion of online banking has introduced significant convenience and accessibility for consumers and financial institutions alike. However, it also brings a substantial increase in cybersecurity threats, making online banking systems prime targets for cybercriminals. This paper provides a comprehensive examination of the prevalent cybersecurity threats that online banking faces, including phishing attacks, malware, ransomware, man-in-the-middle (MITM) attacks, insider threats, and distributed denial-of-service (DDoS) attacks. We analyze these threats in-depth, exploring how each tactic is deployed to compromise security and exploit vulnerabilities within online banking systems.

Moreover, this paper discusses specific vulnerabilities that exist in online banking platforms, such as weak authentication practices, insecure network connections, outdated software, and risks associated with third-party integrations. Through tables and graphical data, the paper offers a clear overview of the most common vulnerabilities and their prevalence, providing insights into how these weak points are exploited in the cyber landscape.

The impact of such cybersecurity breaches on financial institutions is also considered, highlighting the consequences that follow a security breach, such as financial losses, reputational damage, regulatory fines, and customer distrust. The findings reveal that these impacts not only affect individual financial institutions but can also undermine public confidence in digital banking as a whole.

Finally, the paper proposes several strategic defenses against these threats. Solutions include multi-factor authentication, end-to-end encryption, robust threat monitoring, regular security audits, and customer education initiatives, among others. Statistical data on the effectiveness of these strategies demonstrates their role in mitigating cyber risks and fortifying online banking systems against future attacks. This study concludes by emphasizing the critical need for continuous innovation in cybersecurity practices, as cyber threats continue to evolve in sophistication.

Keywords: Cybersecurity, Online Banking Security, Threat Detection, Cyber Threats, Network Vulnerabilities, Authentication Security, Two-Factor Authentication (2FA), Risk Management, Data Encryption, Firewall Security.

1.0 Introduction

In recent years, online banking has transformed the financial industry by offering customers convenient and efficient ways to manage their finances remotely. From checking account balances to transferring funds and making payments, online banking has become integral to daily financial activities. According to industry reports, over 60% of bank customers globally now rely on digital banking channels, highlighting the rapid adoption and growth of online banking services. However, as online banking becomes more prevalent, so too do the cybersecurity risks associated with it. Cybercriminals continuously seek vulnerabilities in these systems to