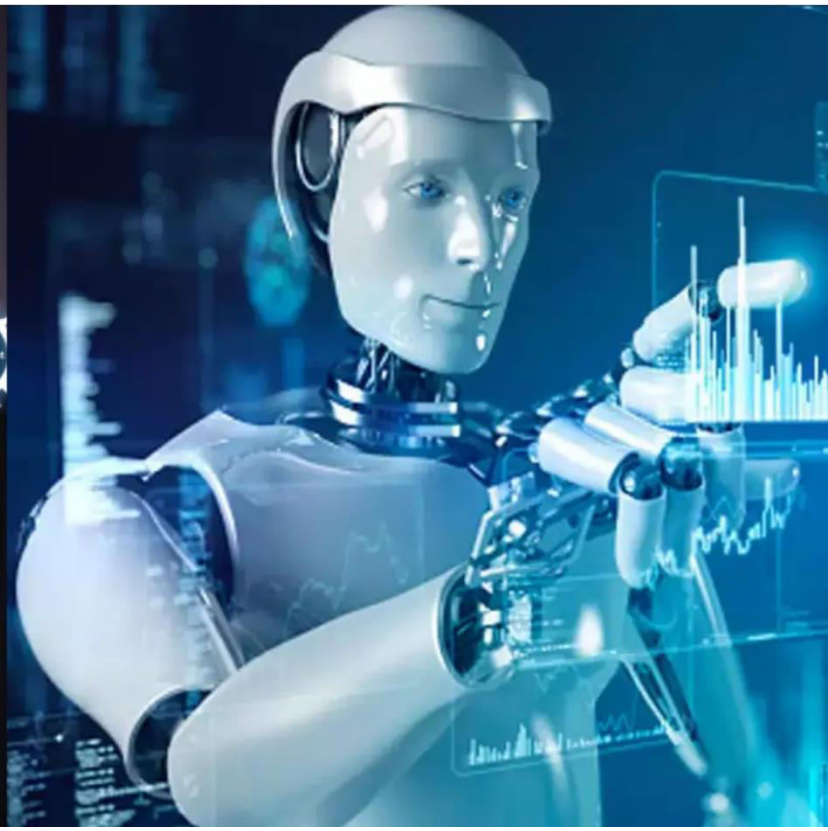
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.935

Volume 15, Issue 6, June 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506114|

Enhanced Security for Accounts using Visual Cryptography Techniques

Borude Sharayu Ram, Lashkare Sakshi Babasaheb , Shaikh Umair Inayatulla,

Kulakarni Vijay Padmakar, Prof. Chandane P.B.

Department of Computer Engineering, Adsul's Technical Campus, Chas, Ahilyanagar, Maharashtra, India

ABSTRACT: Online banking has become an essential component of modern financial systems, providing fast and convenient access to financial services. However, this rapid digital transformation has also increased exposure to cyber threats such as phishing, identity theft, malware attacks, and data breaches. The increasing complexity of banking systems demands an integrated cybersecurity risk management framework that can effectively detect, analyze, and mitigate potential threats.

This project proposes a comprehensive framework that combines risk identification, risk assessment, and mitigation strategies with advanced technologies such as encryption, machine learning, and continuous monitoring. The framework aims to provide a proactive, systematic approach to managing cybersecurity risks, enhancing the security posture of online banking platforms while ensuring compliance, customer trust, and resilience against evolving cyberattacks.

KEYWORDS: Online Banking, Cybersecurity, Risk Management, Phishing, Identity Theft, Malware, Data Breach.

I. INTRODUCTION

Online banking has become an integral part of modern financial systems, offering users fast and convenient access to various financial services. With the digital transformation of banking, there is an increased reliance on electronic platforms, which has also elevated the risks associated with cyber threats. Attackers increasingly target online banking systems to exploit sensitive data, such as account credentials, balances, and transaction histories. Traditional security measures such as firewalls and antivirus software are no longer sufficient to handle sophisticated and evolving cyberattacks.

This project proposes a comprehensive cybersecurity framework for online banking that integrates risk identification, assessment, and mitigation strategies, leveraging advanced technologies such as encryption, machine learning, and continuous monitoring. The framework aims to strengthen security, ensure compliance with standards, and maintain customer trust by proactively addressing potential threats.

II. BACKGROUND

Online banking platforms facilitate the management of financial transactions through digital interfaces, providing convenience to users. However, this convenience comes with significant cybersecurity challenges. Cyber threats such as phishing, malware attacks, identity theft, and data breaches have become increasingly common.

Traditional security approaches mainly rely on static defenses like firewalls and antivirus software. While these measures provide a first line of defense, they are inadequate against adaptive and sophisticated threats. The complexity of modern banking systems and the high value of financial data necessitate an intelligent and dynamic cybersecurity approach that can anticipate, detect, and mitigate threats in real-time.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506114|

III. LITERATURE REVIEW

LSB is the most common concealment algorithm where a secret image is concealed in the least significant bit (LSB) of cover image pixels. A new LSB based system where they use a secret key to determine the cover image layer for secret image concealment [1].

Firstly, they convert stego key to 1D circular array bit stream and secret image to a 1D bit stream. Then the system performs XOR operation between the 1st pixel LSB of the red layer and the 1st bit of stego key. If the resultant bit is 1, the system chooses the green layer of the cover image and for 0, the system uses the blue layer for concealment of 1 bit of the secret image. For the next bit of secret image, the system points to the next red layer pixel and the next bit of stego key. This process continued until the whole secret image bit stream finished. If someone knows the decoding method with stego key, then it can be restored easily. Another LSB based steganography technique where it can hide only texts up to 1024 bytes [2]. steganography technique where it can hide only texts up to 1024 bytes [3].

This system used blue and green layer of the cover image respectively to hide data and a stego key to verify the intended recipient. The first few pixels are used for keeping stego key and the rest of the pixels are used for secret data of the cover image. For decoding, if stego key matches with the key provided by the recipient then the decoding procedure starts. In stego image, there is a terminating key after stego key and secret information which helps to decode. In this method, the security issue is not satisfactory. If the extraction method is revealed, anyone can easily extract the secret information from stego image. Gopi Krishnan S and Loganathan D used a method based on visual cryptography [4].

At first, they converted secret image to half toned image. Then used XOR operation between half toned and a certain randomly created binary image. The resultant image is called share2 and the binary randomly created image is called share1. They decrypted the half toned image by doing XOR operation between share2 and share1 images. Then they retrieve the secret image from half toned image. Their method was so good for security but only share2 image is suspicious to some extent. In addition, they did not use image steganography. Three steganography methods are proposed in paper [5].

They used a pixel's dependency on its neighborhood and psycho visual redundancy to estimate smooth areas and edged areas. In smooth areas, they embed 3 bits and in edged areas, they embed variable rate bits. Though their methods provide a good image quality but they did not provide any security procedure for their work. They used many bits to conceal hidden data in a certain pixel of cover image but a large number of pixels is unused. As a result, certain areas distorted too much. M. Mary Shanthi Rani and K.RosemaryEuphrasia in [6]

added a steganography method where it works only for text secret messages. They converted text message to QR code and conceal it to a cover image through a general LSB method. A steganography approach using visual cryptography on the JPEG image was used in this paper [7].

However, there it could only hide images but not texts. Visual cryptography is applied for the secured sharing of medical images [8]. But security could have been increased by adding the steganography technique

IV. RESEARCH GAPS

- Reliance on static security measures like firewalls and antivirus.
- Limited continuous risk assessment across digital channels.
- Minimal use of AI/ML for threat detection.
- Fragmented compliance with global standards.
- Lack of real-time threat mitigation.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506114|

V. CONCLUSION

In conclusion, The proposed integrated cybersecurity risk management framework provides a comprehensive and proactive approach to securing online banking systems. By combining risk assessment, real-time monitoring, and advanced technologies, it strengthens protection against evolving cyber threats. This framework not only safeguards customer data and financial assets but also enhances trust, compliance, and operational resilience in digital banking. Implementing such a unified model is essential for ensuring a secure and sustainable future in online financial services.

VI. FUTURE DIRECTIONS

- Implement AI/ML for real-time threat detection.
- Enhance encryption for sensitive data protection.
- Develop adaptive risk management frameworks.
- Continuous monitoring of transactions and user behavior.
- Ensure compliance with ISO 27001, NIST, and GDPR.
- Increase user awareness about cyber threats.

REFERENCES

1. A. Sharma, R. Mehta, and S. Verma, “An Integrated Cybersecurity Risk Management Framework for Online Banking Systems,” *International Journal of Computer Applications*, vol. 182, no. 15, pp. 25–31, 2023.
2. P. Kumar and S. Patel, “A Risk-Based Cybersecurity Approach for Secure Online Banking Transactions,” *IEEE Access*, vol. 10, pp. 15420–15429, 2022.
3. R. Gupta and M. Thomas, “Cyber Threat Detection and Risk Mitigation in Online Banking Using Machine Learning,” *Journal of Information Security Research*, vol. 8, no. 4, pp. 112–119, 2021.
4. S. Verma and L. Das, “Framework for Secure Online Banking Through Multi-Layer Cyber Risk Management,” *International Journal of Cybersecurity and Digital Trust*, vol. 5, no. 2, pp. 47–55, 2020.
5. National Institute of Standards and Technology (NIST), “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1, U.S. Department of Commerce, 2018.
6. M. Al-Hujran, A. Al-Debei, and H. Chatfield, “Improving Online Banking Security through Integrated Risk Management Practices,” *Computers & Security*, vol. 124, pp. 103027, 2023.
7. T. Nguyen and D. Kim, “AI-Driven Cybersecurity Framework for Financial Institutions,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 620–632, 2023.
8. L. Zhang and Y. Li, “Blockchain-Based Security Model for Online Banking Risk Management,” *Journal of Financial Technology and Innovation*, vol. 7, no. 1, pp. 88–97, 2022.
9. S. Bansal and R. Jain, “Enhancing Data Protection in E-Banking Systems Using Hybrid Encryption,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 10, pp. 55–61, 2021.
10. ISO/IEC 27005:2018, *Information Technology — Security Techniques — Information Security Risk Management*, International Organization for Standardization, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details