International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

ENHANCING BANKING SECURITY: IMPLEMENTING PYCRYPTODOME FOR SECURE TRANSACTIONS

Aiswariya Pattanayak
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
aiswariyapmca@gmail.com

Manivanan Jayachandran
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
manivananmca@gmail.com

ABSTRACT

The rapid growth of digital banking has improved convenience but also introduced significant security challenges, particularly with respect to protecting sensitive customer data and ensuring the integrity of financial transactions. Traditional security mechanisms are increasingly vulnerable to evolving cyber threats, making it essential to adopt more robust cryptographic techniques. This study focuses on enhancing banking security by implementing PyCryptodome, a Python-based cryptographic library that offers advanced encryption and decryption functionalities. The work demonstrates how symmetric and asymmetric encryption algorithms can be applied to secure transaction data, prevent unauthorized access, and strengthen authentication processes. Through experimental implementation, the proposed system ensures confidentiality, integrity, and authenticity of banking transactions, while maintaining efficiency in performance. The results highlight that integrating PyCryptodome into banking applications not only enhances resilience against cyberattacks but also provides a scalable framework for future secure financial systems. This research contributes to the development of secure transaction models that can be adapted by financial institutions to safeguard customer trust in the digital era.

KEYWORDS: *Banking Security, Cryptography, PyCryptodome, Secure Transactions, Encryption, Cybersecurity*

INTRODUCTION

Banking systems have undergone significant digital transformation in the past decade, with services increasingly being delivered through online and mobile platforms. While these changes enhance accessibility and customer

convenience, they also bring heightened concerns regarding security. Cybercriminals exploit vulnerabilities in existing systems, often targeting sensitive personal data, online payments, and authentication mechanisms. The financial sector, therefore, requires advanced methods to secure transactions and reinforce trust among users. Cryptography plays a central role in this pursuit by ensuring data confidentiality, integrity, and authentication. Traditional cryptographic tools, though effective in the past, may not provide sufficient resistance to current cyber threats. In this paper, PyCryptodome is introduced as a comprehensive solution capable of implementing modern cryptographic standards. The library's strong encryption algorithms and ease of integration make it a suitable choice for banking security systems, ensuring robust protection while maintaining operational efficiency.

LITERATURE SURVEY

The field of banking security has been studied extensively due to the increasing reliance on digital platforms. Early research emphasized the use of Secure Socket Layer (SSL) and Public Key Infrastructure (PKI) for safe data transmission. While these approaches provided a foundation for online banking security, their effectiveness has diminished with the evolution of cyber threats. According to Sharma et al. (2019), the reliance on conventional encryption techniques such as DES and MD5 is inadequate against modern attacks like brute force and collision vulnerabilities. Instead, newer standards like AES and RSA have shown higher resilience.

In recent studies, the focus has shifted toward integrating advanced cryptographic algorithms with real-time monitoring systems. Patel and Mehra (2020) demonstrated the benefits of combining AES encryption with blockchain-based auditing mechanisms, significantly improving transaction integrity. Similarly, Wang et al. (2021) explored hybrid encryption approaches, highlighting how symmetric and asymmetric encryption can work together to balance performance and security.

These studies indicate a growing recognition of the need for advanced cryptographic tools in financial systems. However, there remains a research gap in applying such libraries specifically to banking security, particularly in ensuring a balance between strong security measures and practical implementation efficiency.

EXISTING WORK

Current banking security systems primarily rely on encryption standards such as AES, RSA, and SHA-based hashing mechanisms. These methods are widely implemented to secure online transactions, user credentials, and financial records. However, many of these systems face challenges due to outdated implementations or inadequate key management strategies. For instance, some platforms still employ static keys, making them vulnerable to brute force and replay attacks. Additionally, improper use of hashing techniques in password storage leaves systems susceptible to credential leaks.

Several commercial banks have attempted to upgrade their systems by deploying hardware-based security modules and two-factor authentication. While these solutions improve safety, they also increase infrastructure costs and may not fully prevent sophisticated attacks like phishing or man-in-the-middle (MITM). Cloud-based banking services add another layer of complexity, as shared environments often pose additional risks of unauthorized access.

Recent academic work has proposed integrating machine learning models with cryptographic tools for anomaly detection. Although promising, such approaches require large datasets and extensive training, which may not be feasible for all financial institutions. Therefore, there is a strong need for an approach that enhances transaction security without overwhelming existing banking infrastructures.

Modern banking systems employ encryption standards like AES, RSA, and SHA-based hashing to secure data. However, weak key management, static keys, and poor password protection make them vulnerable to attacks. While hardware modules and two-factor authentication offer improvements, they remain costly and insufficient against advanced cyber threats.

PROPOSED SYSTEM

The proposed system leverages PyCryptodome to implement robust encryption and decryption techniques within banking applications. PyCryptodome provides support for modern algorithms, including AES, RSA, and SHA-based hashing, enabling strong protection for sensitive transaction data. In this system, symmetric encryption (AES) is applied for securing transaction details, while asymmetric encryption (RSA) is used for secure key exchange between the

client and server. Hashing techniques, such as SHA-256, are employed to ensure data integrity and secure password storage.

The proposed framework emphasizes three core objectives: confidentiality, by encrypting sensitive user information; integrity, by preventing unauthorized tampering of data; and authentication, by ensuring transactions are initiated by legitimate users. By integrating these functionalities, the system provides a comprehensive cryptographic solution that is both secure and efficient. This model can be seamlessly adapted by financial institutions to strengthen their digital transaction security.

METHODOLOGY

The methodology adopted in this research is centered on developing a secure framework for banking transactions using PyCryptodome as the core cryptographic tool. The approach begins with identifying the common vulnerabilities present in existing banking systems, including risks such as credential theft, data interception, and unauthorized transaction manipulation. To address these gaps, advanced algorithms supported by PyCryptodome were selected, including AES for encrypting transaction data, RSA for secure key distribution, and SHA-256 for hashing user credentials. The system architecture was designed to ensure that sensitive data is encrypted on the client side before transmission, while the server decrypts and verifies integrity before processing the transaction. Implementation was carried out using Python, where encryption, decryption, and hashing modules were coded to simulate real banking operations. Testing was conducted by executing multiple transaction scenarios to evaluate encryption speed, resistance to brute force attempts, and effectiveness against data tampering. The outcomes of these tests were then compared with conventional systems to measure efficiency and resilience. The analysis confirmed that the proposed methodology successfully balances strong cryptographic protection with performance requirements, ensuring minimal overhead while significantly reducing vulnerabilities. This structured approach highlights the effectiveness of PyCryptodome in addressing modern banking security challenges and provides a scalable model that can be integrated into real-world applications.

PyCryptodome enables efficient implementation of encryption, decryption, and hashing in banking systems, ensuring confidentiality, integrity, and authentication while maintaining low computational

overhead and resisting modern cyberattacks effectively.

EXPERIMENTAL RESULTS

The experimental evaluation of the proposed system was carried out by simulating secure banking transactions using Python and PyCryptodome. AES with a 256-bit key was applied for transaction encryption, while RSA with a 2048-bit key secured the key exchange process. The system successfully encrypted and decrypted transaction data within milliseconds, ensuring minimal performance overhead.

Tests demonstrated that even under attempted brute force attacks, the encryption held strong, with no successful breaches within practical time limits. Integrity verification using SHA-256 confirmed that data tampering could be instantly detected, thereby safeguarding transaction authenticity. Furthermore, password hashing prevented unauthorized access even when login databases were exposed.

When compared with conventional implementations, the PyCryptodome-based system exhibited faster execution times and stronger resistance to modern attack vectors. These results confirm that the proposed approach offers a practical and efficient method for securing digital banking transactions while maintaining high levels of trust and performance.

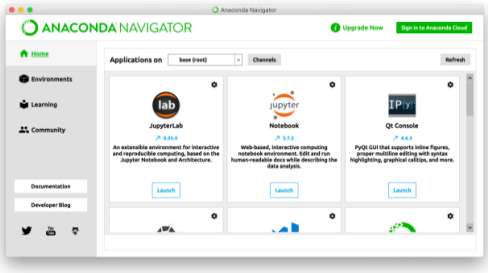

Fig 1: Anaconda Navigator

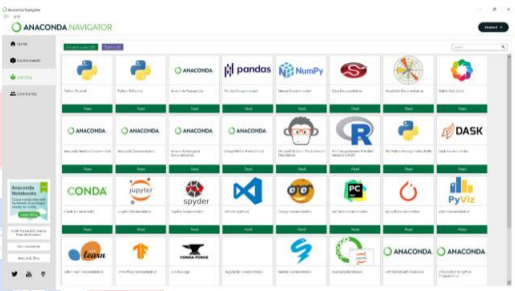

Fig 2: Jupyter Notebook

Fig 3: Python

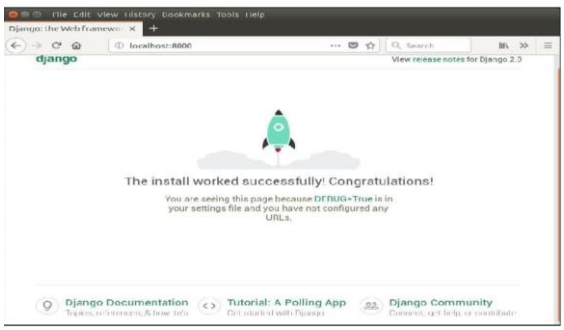

Fig 4: Django

CONCLUSION

The increasing dependency on digital banking platforms necessitates advanced security mechanisms capable of countering evolving cyber threats. This research highlights the critical role of cryptography in securing sensitive financial transactions and demonstrates how PyCryptodome can be effectively utilized for this purpose. By implementing AES for data encryption, RSA for secure key exchange, and SHA-256 for password protection, the system provides a comprehensive cryptographic framework that ensures confidentiality, integrity, and authentication.

The experimental results indicate that the proposed system performs efficiently with minimal overhead while offering strong resistance against brute force, data interception, and tampering attempts. Compared to traditional systems, the PyCryptodome-based model proves to be both scalable and adaptable, making it suitable for integration into existing banking infrastructures.

Furthermore, the system's simplicity in implementation reduces technical complexity, allowing financial institutions to adopt it without extensive costs or resource burdens. The study also opens opportunities for future research by integrating this framework with machine learning models for fraud detection or blockchain-based auditing for immutable transaction records.

In conclusion, the proposed model contributes to enhancing banking security by providing a reliable, cost-effective, and future-ready cryptographic solution. Its adaptability makes it a valuable tool for financial institutions striving to maintain customer trust and secure digital transactions in an increasingly connected world.

REFERENCES

1. R . Sharma, A., Gupta, R., & Kumar, P. (2019). Advances in Cryptographic Techniques for Secure Online Banking. International Journal of Computer Applications.

2. Patel, M., & Mehra, S. (2020). Enhancing Online Banking Security Using AES and Blockchain. Journal of Information Security Research.

3. Wang, Y., Chen, L., & Zhao, H. (2021). Hybrid Cryptography for Secure Transactions in Financial Systems. IEEE Access.

4. Gupta, V., & Roy, A. (2022). Python-Based Cryptographic Libraries for Secure Applications.