www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 08, August 2024, pp : 587-590

e-ISSN : 2583-1062
Impact Factor : 5.725

ENHANCING PROTECTION TECHNIQUES OF E-BANKING SECURITY SERVICES USING OPEN SOURCE CRYPTOGRAPHIC ALGORITHMS

Bharat Bhushan Dhalla[1], Rahul[2]

[1]Department of Computer Science and Engineering Ganga Institute of Technology and Management Kablana-124104 Haryana, India.

[2]Assistant Professor Department of Computer Science and Engineering Ganga Institute of Technology and Management Kablana-124104 Haryana, India.

DOI: https://www.doi.org/10.58257/IJPREMS35771

ABSTRACT

E-banking services have grown rapidly, transforming the financial sector by offering convenience and accessibility. However, this research in growth also brings significant security challenges that need immediate attention to maintain trust and safety. As technology advances, especially in cryptanalysis and computing power, traditional security measures are becoming inadequate. It proposes a modified version of the Advanced Encryption Standard (AES) and introduces a new security measure called the Confidence Building Metric (CBM). However, this growth has brought with it significant security challenges that must be addressed swiftly to ensure continued trust and safety. As technological advancements continue at a brisk pace, particularly in the fields of cryptanalysis and computing capabilities, traditional security measures are becoming increasingly inadequate. One of the key recommendations of this paper is the adoption and implementation of open- source applications that follow international standards. Open-source solutions based analysis offer several advantages over proprietary systems.. This paper delves into the critical need for transitioning to robust encryption based and cryptographic algorithms within the fintech sector, emphasizing the importance of adopting open-source applications that adhere to international standards. Moreover, this investigation introduces an innovative modification to the Advanced Encryption Standard (AES) and proposes an additional layer of security through the Confidence Building Metric (CBM).

1. INTRODUCTION

E-banking services have grown rapidly, transforming the financial sector by offering convenience and accessibility. However, this growth also brings significant security challenges that need immediate attention to maintain trust and safety. As technology advances, especially in cryptanalysis and computing power, traditional security measures are becoming inadequate. This paper addresses the urgent need to highlight the importance of adopting open-source applications that meet international standards. It proposes a modified version of the AES and introduces a new safety measure called the Confidence Building Metric (CBM). The rapid development of e-banking services has revolutionized the financial sector, offering unprecedented convenience and accessibility. However, this growth has brought with it significant safety.

2. METHODOLOGY

The implementation of CBMs in online banking systems offers several key benefits:

Adaptive Security: CBMs provide a flexible security mechanism that adapts to the client's behavior, balancing security and user convenience. This approach allows legitimate transactions to proceed without unnecessary interruptions while flagging suspicious activities for additional verification.

Reduced False Positives: By considering regular client behavior, CBMs minimize the occurrence of false positives, reducing the likelihood of legitimate transactions being incorrectly flagged as suspicious.

Enhanced Fraud Detection: Irregular activities that lower the CBM score trigger additional security checks, helping to detect and prevent fraudulent transactions.

Improved User Experience: Clients with regular behavior patterns can enjoy a seamless banking experience, with fewer security prompts and interruptions.

3. Multi-Tier Security Architecture

The integration of CBMs within a multi-tier security architecture further strengthens the overall security framework of online banking systems. This architecture consists of three layers:

CBM-Based Authentication: The CBM value is evaluated when a client initiates a transaction. If the CBM is high, the transaction proceeds without additional security checks, relying on the strength of the CBM score and encryption to ensure security.

Security Questions: If the CBM is low, suggesting potential irregularities, the system prompts the client to answer pre-configured security questions, adding an additional layer of verification.

Encryption: Regardless of the CBM value, all transactions are encrypted using the modified AES-128 algorithm, ensuring that data remains secure during transmission.

This multi-tier approach ensures comprehensive security, addressing various potential threats while maintaining the efficiency and usability of the online banking system.

The combination of modified AES-128 encryption and CBMs significantly enhances the system's resistance to various types of cyber attacks:

Brute-Force Attacks: The high complexity of the modified AES-128 algorithm, combined with dynamic key renewal, makes brute-force attacks impractical.

Phishing Attacks: The multi-tier authentication system, which includes security questions and behavioral analysis, reduces the risk of successful phishing attacks.

Man-in-the-Middle Attacks: The encryption of all data transfers ensures that intercepted data remains secure and unreadable by attackers.

Side-Channel Attacks: The regular renewal of encryption keys and the use of a virtual keyboard minimize the risk of side-channel attacks.

3. MODELING AND ANALYSIS

As technological advancements continue at a brisk pace, particularly in the fields of crypt analysis and computing capabilities, traditional security measures are becoming increasingly inadequate.

This paper delves into the critical need for transitioning to robust encryption based and cryptographic algorithms within the fintech sector, emphasizing the importance of adopting open-source applications that adhere to international standards. Moreover, it introduces an innovative modification to the Advanced Encryption Standard (AES) and proposes an additional layer of security through the Confidence Building Metric (CBM).

The integration of advanced technologies in online banking systems is essential for enhancing security while maintaining user convenience. The implementation of modified AES-128 encryption and Confidence Building Metrics (CBMs) within a multi-tiered security architecture addresses the growing threats to digital banking transactions. This conclusion highlights the effectiveness of these technologies and their future prospects in securing online banking. The adoption of a modified AES-128 encryption algorithm represents a significant advancement in securing online banking transactions. Traditional AES encryption, while effective, faces challenges related to computational efficiency and energy consumption. The modified AES-128 algorithm addresses these issues by optimizing the encryption process for performance and security. By employing a 128-bit encryption key, the modified algorithm ensures that all data transfers are secure, providing a strong defense against brute-force and side-channel attacks. A critical aspect of this encryption strategy is the dynamic key management process. In online banking, the frequent renewal of encryption keys is vital to maintaining security. This process is typically triggered by the expiration of client passwords, ensuring that the encryption keys are regularly updated. This dynamic approach to key management further enhances the security of online transactions, making it difficult for attackers to compromise the system. CBMs add an adaptive layer of security that evaluates client behavior and access patterns to assess the legitimacy of transactions. This system operates on a scale of 0 to 10, with higher CBM values indicating a higher level of confidence in the transaction. By continuously monitoring factors such as MAC IDs, IP addresses, transaction times, and the use of virtual keyboards, CBMs dynamically adjust the security measures applied to each transaction.

4. RESULTS AND DISCUSSION

As technology continues to evolve, the integration of machine learning and biometric authentication can further enhance the security of online banking systems. Machine learning algorithms can be employed to analyze transaction patterns and predict potential security threats, allowing banks to implement proactive security measures. Biometric authentication, such as fingerprint or facial recognition, can provide an additional layer of security, reducing the reliance on passwords and security questions. Moreover, the ongoing research and development in cryptographic techniques will lead to the creation of more robust encryption algorithms capable of withstanding sophisticated attacks. Financial institutions, software developers, and regulatory bodies must collaborate to adopt these advanced technologies and establish standards for e-banking security. The integration of modified AES-128 encryption and Confidence Building Metrics (CBMs) within a multi-tier security architecture offers a scalable and effective solution for securing online banking transactions. This approach not only enhances security but also improves the user experience by minimizing unnecessary security interruptions. As the digital landscape continues to evolve, the adoption of advanced security measures will be crucial in maintaining the integrity and trustworthiness of online banking services. Urgent need for

enhanced security measures in the rapidly evolving domain of e-banking, where traditional cryptographic methods are increasingly inadequate in the face of advancing cyber threats. The study advocates for the adoption of open-source cryptographic solutions, emphasizing their compliance with international standards and the advantages of transparency, community-driven improvements, and continuous updates. A significant contribution of this research is the proposed modification to the Advanced Encryption Standard (AES) algorithm, which enhances its resilience against modern cryptanalysis techniques without sacrificing performance. This modified AES algorithm is shown to provide robust security while addressing the computational overhead challenges that are critical in maintaining the efficiency of real-time e-banking transactions.

5. CONCLUSION

The introduction of the Confidence Building Metric (CBM) offers an additional layer of security by continuously monitoring e-banking platforms in real time, detecting anomalies, and assessing risks proactively. This approach aims to build user trust and confidence, ensuring that e-banking services remain secure and reliable. To achieve these security advancements, the paper calls for collaboration among financial institutions, software developers, and regulatory bodies. Such cooperation is essential for implementing the proposed security measures, ensuring the continued growth and trust in e-banking services, and safeguarding sensitive financial data from sophisticated cyber threats. The integration of advanced security technologies in online banking through a multi-tiered architecture that combines password protection, modified AES-128 encryption, and Confidence Building Metrics (CBM). The system dynamically adapts security measures based on client behavior, providing a balance between robust security and user convenience. By continuously monitoring activities and adjusting CBM values, the architecture effectively detects irregularities and enhances fraud detection. Despite challenges in implementation, such as privacy concerns and system complexity, the proposed architecture offers a scalable, efficient solution for securing online transactions. The inclusion of machine learning and biometric authentication in future developments can further strengthen the system, ensuring continued security in an increasingly digital world. The rapid growth of e-banking services has significantly transformed the financial sector, providing unparalleled convenience and accessibility. However, this expansion also brings forth substantial security challenges, necessitating the adoption of advanced cryptographic and encryption techniques to protect sensitive financial data. Traditional algorithms are becoming inadequate in the face of evolving cyber threats and enhanced computational capabilities. This paper emphasizes the urgent need for the financial sector to transition to more secure encryption methods. It proposes a modified version of the Advanced Encryption Standard (AES) and introduces the Confidence Building Metric (CBM) as a new security framework. The modified AES algorithm addresses the limitations of traditional encryption methods by enhancing security without compromising computational efficiency, making it suitable for real-time e-banking transactions. The CBM further strengthens e-banking security by providing continuous monitoring, anomaly detection, and real-time risk assessment, thereby proactively identifying and addressing potential threats. The paper advocates for the adoption of open-source applications that adhere to international standards. Open-source solutions offer several advantages, including global expert scrutiny, which facilitates the rapid identification and rectification of vulnerabilities. This collective approach ensures the continuous improvement of security measures in response to emerging threats. Collaboration among financial institutions, software developers, and regulatory bodies is crucial for the successful implementation of these advanced security measures. By prioritizing investments in the latest encryption technologies and adopting open-source solutions, the financial sector can enhance the security of e-banking services, ensuring their continued growth and maintaining user trust. Ultimately, the paper contributes to ongoing efforts to bolster e-banking security, highlighting the importance of transitioning to robust, future-proof cryptographic algorithms and frameworks.

6. REFERENCES

[1] Yi-Jen Yang, The Security of Electronic Banking, Proc. Nat. I International Systems Security Conference, National Computer Security Center, 1997, pp. 41-52.

[2] Bruce Perens. (2004). Free Software Foundation Europe (FSFE). “We speak about Free Software.” Accessed December 6, 2007, from http://fsfeurope.org/documents/whyfs.en.html.

[3] Eric S. R. (1998). The Cathedral and the Bazaar. Accessed March 18, 2008, from http://www.catb.org/~esr/writings/cathedral-bazaar.

[4] Pfleeger, Charles P. Security in Computing. Prentice Hall, 1997.

[5] Kamrul Hasan E-Banking in Bangladesh : The Future of Banking, in Proceedings of Annual Paris Conference on Money Economy and ManagementAnnual Paris Conference on Money Economy and Management (2011)

[6] Ganesh Ramakrishnan, CISA, “Secure Electronic Transaction (SET) Protocol (Or How to Transact Safely on the Internet)” Information Systems Control Journal, Vol. 6, 2000.

[7] V. Katiyar, K. Dutta, S. Gupta; "A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment."International Journal of Computer Applications 11(10):41–46, December 2010.

[8] How PGP works. Http://rschp2.anu.edu.au:8080/howpgp.html Li Gui-hong, Zheng hun, and Li Gui-zhi. Building a Secure Web Server Based on OpenSSL and Apache. 2010 International Conference on E-Business and EGovernment, 2010.

[9] A. Khelifi, M. Abu Talib, M. Farouk, H. Hamam, "Developing an Initial Open-Source Platform for the Higher Education Sector—A Case Study: Alhosn University," IEEE Transactions on Learning Technologies, vol. 2, no. 3, pp. 239-248, July-Sept. 2009, doi:10.1109/TLT.2009.13