World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Analyzing the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs

Samuel Omokhafe Yusuf [1,*], Amarachi Zita Echere [2], Godbless Ocran [3], Justina Eweala Abubakar [4], Adedamola Hadassah Paul-Adeleye [5] and Peprah Owusu [3]

[1] *Independent Researcher, Massachusetts, USA.*
[2] *The Global School, Worcester Polytechnic Institute, Massachusetts, USA.*
[3] *WPI School of Business, Worcester Polytechnic Institute, Massachusetts, USA.*
[4] *Independent Researcher, Federal Capital Territories, Nigeria.*
[5] *Independent Researcher, Alimosho, Lagos, Nigeria.*

World Journal of Advanced Research and Reviews, 2024, 23(03), 2138–2147

Publication history: Received 31 July 2024; revised on 08 September 2024; accepted on 10 September 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.3.2753

Abstract

The study explores the significance of artificial intelligence (AI) in advancing encryption technologies, focusing on small and medium-sized businesses (SMBs) and their financial data security needs. As cyber threats evolve and quantum computing looms on the horizon, traditional encryption methods—such as symmetric encryption (AES) and asymmetric encryption (RSA)—are increasingly challenged. The study assesses how AI-driven encryption solutions address these challenges and enhance data protection.

Key objectives include reviewing the effectiveness of traditional encryption methods and comparing them with cutting-edge AI-powered approaches. The methods reviewed encompass homomorphic encryption, which allows for computations on encrypted data without decryption, quantum-resistant algorithms designed to withstand quantum computing threats, and adaptive encryption that adjusts security measures based on real-time risk assessments.

Major findings indicate that while traditional encryption methods remain foundational, they are often insufficient to address modern threats and future uncertainties. AI-enhanced solutions offer significant improvements, such as real-time threat detection, scalability, and adaptive security. In particular, homomorphic encryption and quantum-resistant algorithms present promising advancements for protecting sensitive financial data against emerging threats.

The study highlights the practical implications of integrating AI into existing encryption infrastructures, including potential cost implications, scalability challenges, and the need for compatibility with legacy systems. It underscores the importance of a hybrid approach, combining traditional and AI-driven encryption methods, to build a resilient and future-proof security framework for SMBs. This approach ensures robust financial data protection in a rapidly evolving digital landscape.

Keywords: AI-powered encryption; Financial data security; SMBS; Homomorphic encryption; Symmetric encryption; Asymmetric encryption; Cybersecurity

1. Introduction

In today's increasingly digital economy, data security has become paramount for small and medium-sized businesses (SMBs) (Kallmuenzer et al., 2024). These businesses, which often operate with limited resources and infrastructure,

* Corresponding author: Samuel Omokhafe Yusuf

face significant risks from cyber threats that can compromise sensitive information such as customer data, transaction records, and financial statements. A breach in security can not only lead to substantial financial losses but can also damage the trust of customers and stakeholders, potentially resulting in long-term reputational harm (Seh et al.,2024). In this context, encryption has emerged as a crucial tool for protecting sensitive information, ensuring that even if data is intercepted, it remains inaccessible to unauthorized parties.

Traditionally, encryption methods have relied on symmetric and asymmetric encryption algorithms, where the former uses the same key for both encryption and decryption and later uses a pair of public and private keys (Al-Dhabi, 2019). While efficient and fast, symmetric encryption presents challenges in key management, especially when data is transmitted across different systems (Bani et al., 2017). On the other hand, asymmetric encryption offers enhanced security by using two different keys, but it is computationally more intensive and slower, making it less suitable for large-scale applications (Bani et al., 2017). Despite their effectiveness, these traditional methods have limitations, particularly in the face of increasingly sophisticated cyber threats.

The advent of artificial intelligence (AI) has introduced a new dimension to data encryption, enhancing data protection measures. This review aims to analyze the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs, contrasting them with traditional encryption methods. Specifically, it explores the strengths and weaknesses of symmetric and asymmetric encryption and how AI is transforming these approaches. By examining the current state of AI in encryption and its potential future developments, the review seeks to provide a comprehensive understanding of how SMBs can better protect their financial data in an increasingly digital world. The objective is to assess whether AI-powered solutions offer a significant advantage over traditional methods and identify the key factors SMBs should consider when choosing an encryption strategy.

2. Literature Review

2.1. Symmetric Encryption: AES and its Role in Financial Data Protection

Symmetric encryption is one of the earliest and most used types of encryption, which encrypts and decrypts data using the same key (Shallal & Bokhari, 2016). The Advanced Encryption Standard (AES) is the most widely used symmetric encryption technique for safeguarding financial data. (Smid, 2021). Developed by the U.S. National Institute of Standards and Technology (NIST) in 2001, AES has become the accepted standard for securing sensitive information due to its robustness and efficiency.

AES operates on block ciphers, using 128, 192, or 256 bits of keys to encrypt data in fixed-size blocks, usually 128 bits. (Sousi et al., 2020). The security of AES lies in its ability to perform multiple rounds of transformation on the data block, including substitution, permutation, and mixing of the plaintext. Depending on the key size, there are ten rounds of transformation for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys (Sousi et al., 2020). This layered approach makes AES highly resistant to brute-force attacks, where an attacker attempts to decrypt data by systematically trying all possible keys (Zodpe & Shaikh, 2021).

In the context of financial data protection, AES is particularly valued for its speed and efficiency, which are critical in environments where large volumes of transactions occur rapidly (Tawfiq et al., 2021). Banks, payment processors, and other financial institutions rely on AES to secure transaction data, customer information, and communications. (Orucho et al., 2023). For instance, AES encrypts data at rest, such as customer account details stored in databases, and data in transit, such as credit card information being processed during an online purchase. The strength of AES ensures that even if encrypted data is intercepted, the decryption key is required to make it readable., providing a robust layer of security for financial exchanges (Prashant et al., 2024).

2.2. Asymmetric Encryption: RSA and Its Application in Financial Transactions

Asymmetric encryption, sometimes called public-key cryptography, entails using two unique keys: a private key for decryption and a public key for encrypting (Khan et al., 2018). One of the most widely recognized algorithms in this category is the Rivest-Shamir-Adleman (RSA) algorithm, named after its inventors. (Isaad et al., 2020) In contrast to symmetric encryption, which encrypts and decrypts data using the same key, RSA allows for more secure communication by enabling the distribution of a public key while keeping the private key secret.

The mathematical difficulty of factoring huge prime numbers forms the foundation of RSA's security, a problem that becomes exponentially harder as the key size increases (Rowland, 2016). Typically, RSA keys are 1024 or 2048 bits long, with 4096-bit keys used for more critical applications. In financial transactions, RSA is commonly employed to

protect the exchange of sensitive information over the internet. For instance, it is integral to the functioning of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, which secure online communications between web browsers and servers (Satapathy & Livingston, 2016). When a customer initiates a transaction on a banking website, RSA establishes a secure connection, encrypting the data transmitted between the user's browser and the bank's server (Ruman & Phaneendra, 2015). This ensures that private data, such as passwords and credit card numbers, is protected from malicious actors' interference.

Moreover, RSA is also utilized in digital signatures, a crucial feature in financial transactions where authenticity and integrity are paramount (Iwasokun et al., 2019). A digital signature generated using RSA verifies the sender's identity and ensures that no tampering has occurred with the data during transmission. This application is particularly important in online banking, electronic fund transfers, and other financial services where trust and data integrity are essential.

2.3. Public Key Infrastructure (PKI) and Its Role in Securing SMB Communications

Public Key Infrastructure (PKI) is a comprehensive system that supports asymmetric encryption by managing digital certificates' creation, distribution, and revocation (Danquah & Kwabena-Adabe, 2020). PKI is vital in securing communications and financial exchanges for small and medium-sized businesses (SMBs), which often face challenges in implementing robust security measures due to limited resources. PKI issues digital certificates through trusted entities known as Certificate Authorities (CAs) (Tanwan & Kumar, 2017). These certificates bind a public key to an individual or organization, allowing users to verify the identity of the party they are communicating with. For SMBs, PKI is crucial in ensuring the secure exchange of information with partners, customers, and suppliers (Danquah & Kwabena, 2020). In secure email communications, PKI encrypts email content and attachments, guaranteeing that the intended recipient can only decrypt and read the message with the matching private key. This is particularly important for SMBs that handle sensitive financial data, such as invoices, contracts, and payment details, where confidentiality and integrity must be maintained.

In financial exchanges, PKI underpins the security of electronic transactions, including e-commerce payments, online banking, and digital signatures. By leveraging PKI, SMBs can establish secure connections with customers and other businesses, safeguarding the exchange of sensitive information. Additionally, PKI supports multi-factor authentication, enhancing security by requesting that users utilize several methods, like a password, to confirm their identity and a digital certificate (Trzupik, 2020). This added layer of security is especially beneficial for SMBs, which are increasingly targeted by cybercriminals due to their often less sophisticated security infrastructures.

Hence, symmetric encryption, asymmetric encryption, and PKI each play crucial roles in protecting financial data for SMBs. While AES provides robust and efficient protection for large volumes of data, RSA ensures secure communication and transaction verification. PKI, meanwhile, offers a framework for managing the secure exchange of information and maintaining trust in digital interactions, making it an essential tool for SMBs navigating the complex landscape of data security.

3. Comparison of Traditional vs. AI-Powered Encryption Methods

AI's integration into encryption methods has garnered significant attention in recent literature, particularly due to its potential to revolutionize data security. AI-enhanced homomorphic encryption is one of the most noteworthy developments; it enables computations on encrypted data without decryption (Su et al., 2024). This capability is vital for preserving privacy in data processing, especially in sensitive fields like finance and healthcare. AI optimizes this process by dynamically adjusting encryption based on data complexity, improving both security and efficiency.

Another area where artificial intelligence is vital is quantum-resistant encryption. With the advent of quantum computing, traditional encryption methods like RSA are becoming increasingly vulnerable (Emmanni, 2023). AI-driven research has led to the development of lattice-based cryptography and other quantum-resistant algorithms designed to withstand quantum computers' power (Singh & Kumar, 2018). AI assists in identifying and refining these algorithms, ensuring they are robust against future threats.

Adaptive encryption represents a significant leap forward, with AI enabling real-time adjustments to encryption protocols based on the current threat landscape. Unlike static traditional methods, AI-driven adaptive encryption continuously assesses risk levels, dynamically enhancing security where necessary (Farooq & Mubashir, 2024). This innovation is particularly beneficial for SMBs, providing robust protection tailored to specific needs and environments.

3.1. Symmetric Encryption vs. AI-Enhanced Homomorphic Encryption

Symmetric encryption is a cornerstone of traditional data protection (Shallal & Bokhari, 2016). While it is efficient and fast, its security hinges on the safe management and exchange of keys. Any breach in key management can compromise the entire encrypted data set, making symmetric encryption vulnerable to various attacks (Rana et al., 2023). On the other hand, AI-enhanced homomorphic encryption offers a more advanced alternative, addressing some of these limitations. Homomorphic encryption allows computations to be performed directly on encrypted data without requiring decryption, ensuring that sensitive information remains secure throughout the entire process (Su et al., 20240. This capability is particularly valuable in financial data processing, where confidentiality is paramount.

AI-driven enhancements to homomorphic encryption introduce a new level of flexibility and security. Artificial Intelligence can enhance the encryption process by utilizing machine learning techniques, making it more efficient and scalable (Umoga et al., 2024). For instance, AI can dynamically adjust the complexity of encryption based on the sensitivity of the data, ensuring that highly sensitive information is encrypted with stronger methods while less critical data can be processed more quickly. Moreover, AI can help detect and mitigate potential vulnerabilities in real time, lowering the possibility of data breaches (Familoni, 2024). This makes AI-driven homomorphic encryption particularly well-suited for SMBs that handle sensitive financial information and require high security without compromising operational efficiency.

3.2. Asymmetric Encryption vs. Quantum-Resistant Encryption

Asymmetric encryption, including RSA and Elliptic Curve Cryptography (ECC), relies on the use of public and private key pairs, offering a secure method for exchanging information over untrusted networks. While effective, these traditional methods are increasingly at risk from the advent of quantum computing, which has the potential to break current cryptographic standards (Emmanni, 2023). Quantum-resistant encryption, developed with the help of AI, aims to address this emerging threat by creating algorithms resistant to quantum attacks (Radanliev, 2024).

AI is essential to the advancement of quantum-resistant encryption methods. By analyzing the mathematical structures of potential encryption algorithms, AI can identify those most likely to withstand quantum computing capabilities (Radaliev, 2024). For instance, lattice-based cryptography, a promising quantum-resistant technique, has been significantly advanced through AI-driven research. AI algorithms can optimize these encryption methods, making them more efficient and easier to implement in real-world applications (Li et al., 2021).

Compared to traditional RSA or ECC, quantum-resistant encryption provides a forward-looking approach to data security, ensuring that encryption methods stay protected even as the field of quantum computing develops. This is particularly important for SMBs, which must future-proof their data protection strategies. By integrating AI into developing these encryption techniques, businesses can better prepare for the challenges posed by quantum computing and maintain the security of their financial transactions.

3.3. Adaptive Encryption vs. Traditional Encryption Protocols

Traditional encryption protocols typically involve static methods where the encryption process remains constant, regardless of the context in which it is applied (Baseri, 2024). While these methods provide a baseline level of security, they do not adapt to changing threat landscapes or the varying sensitivity of data. AI-driven adaptive encryption offers a dynamic alternative, automatically adjusting encryption protocols based on the current threat environment and the sensitivity of the data being protected (Ramos-Cruz et al., 2024).

Adaptive encryption leverages AI to monitor the network environment in real time, detecting potential threats and adjusting encryption strength accordingly (Manoharam et al., 2022). If a system detects unusual activity or an increase in cyber threats, AI can enhance the encryption level for ongoing transactions, ensuring that sensitive financial data remains secure. Conversely, during periods of lower risk, the encryption process can be optimized for speed and efficiency, reducing the computational load on the system.

This dynamic approach offers significant advantages over traditional encryption protocols, particularly for SMBs that must balance security with performance. By adjusting to the specific needs of the moment, AI-driven adaptive encryption ensures that data is always protected at the appropriate level without the need for constant manual intervention (Aldoseri et al., 2023). This enhances security and improves the overall efficiency of the encryption process, making it a more effective solution for modern financial data protection.

3.4. Real-Time Application of AI in Financial Data Encryption

AI has revolutionized the encryption of financial data by significantly improving the speed and adaptability of encryption processes, both in traditional and AI-enhanced techniques (Radanilev, 2024). Traditional encryption methods, such as AES and RSA, rely on predefined algorithms that, while robust, may not always offer the flexibility needed to handle the complexities of modern financial transactions. These methods are typically static, meaning the encryption process remains the same regardless of the context, potentially leading to inefficiencies or vulnerabilities in rapidly changing environments (Havercamp & Samah, 2024).

On the other hand, AI-enhanced encryption introduces dynamism and responsiveness that traditional methods lack. By integrating machine learning algorithms, AI can analyze transaction patterns in real time, identifying potential threats and adjusting encryption protocols accordingly (Paul, 2024). In a high-volume financial transaction environment, AI can prioritize encrypting the most sensitive data first, ensuring critical information is secured immediately. Additionally, AI can help streamline the encryption process by optimizing key management and reducing the time required to encrypt and decrypt data (Radanilev, 2024).

One of the most significant benefits of AI in financial data encryption is its ability to learn and adapt. As AI algorithms process more data over time, they become better at predicting potential security threats and can adjust encryption methods proactively. This is particularly valuable in financial transactions, where the risk of fraud and cyberattacks is high. By continuously analyzing transaction data, AI can detect anomalies indicating fraudulent activity, allowing for immediate adjustments to encryption protocols to prevent data breaches.

Moreover, AI enhances the efficiency of encryption processes by reducing the computational load (Li et al., 2021). Traditional encryption methods can be resource-intensive, particularly when encrypting large volumes of data. AI can optimize these processes by selecting the most appropriate encryption method for each situation, balancing the need for security with the available computational resources. This speeds up transactions and reduces the overall cost of encryption, making it a more viable solution for SMBs with limited resources.

Hence, the real-time application of AI in financial data encryption offers significant advantages over traditional methods. By improving the speed, adaptability, and efficiency of encryption processes, AI ensures that financial transactions are both secure and efficient, meeting the demands of modern digital environments. This makes AI-enhanced encryption a critical tool for SMBs looking to protect their financial data in an increasingly complex and dynamic cyber landscape.

3.5. Performance Metrics for Traditional vs. AI-Integrated Encryption Systems

Evaluating encryption systems' performance, particularly in SMB environments, requires an understanding of key metrics such as processing time, scalability, and cost-effectiveness. While effective in securing data, traditional encryption systems often struggle to balance these factors, especially when dealing with large volumes of data or complex transaction environments. AI-integrated encryption systems, however, offer a more sophisticated approach, addressing many of the limitations associated with traditional methods.

Traditional encryption systems like AES and RSA are known for their reliability but can be time-consuming, particularly when encrypting large datasets or during the key exchange process (Prashant et al., 2022). This can be a bottleneck in environments where speed is critical, such as in high-frequency trading or real-time payment processing. AI-integrated encryption systems, by contrast, can significantly reduce the processing time by optimizing encryption processes in real time. AI algorithms can dynamically select the most efficient encryption method based on the specific context, ensuring data is encrypted quickly without compromising security (Radanilev, 2024). This reduction in processing time is particularly valuable for SMBs that need to maintain fast and efficient operations while ensuring data security.

As SMBs grow, their data security needs evolve, often requiring encryption systems to scale rapidly to accommodate increased data volumes and transaction complexity. Traditional encryption methods can struggle to scale effectively, particularly when they rely on manual key management or fixed encryption protocols. AI-integrated systems, however, offer superior scalability by automating key management and adapting encryption strength based on data sensitivity and threat levels (Manoharan & Sarker, 2022). As an SMB expands, its encryption system can scale seamlessly without requiring significant manual intervention or reconfiguration, ensuring continuous data protection across all operations.

Cost is a critical consideration for SMBs, which often operate with limited budgets. Traditional encryption systems can be costly to implement and maintain, particularly if they require dedicated hardware or specialized personnel (Quereshi et al, 2022). AI-integrated encryption systems, while potentially requiring a higher initial investment, can offer long-term cost savings by automating many of the processes that would otherwise require manual intervention. AI can also

optimize resource usage, reducing encryption's computational and energy costs. Additionally, by improving the efficiency and scalability of encryption, AI-integrated systems can reduce the overall cost of data protection, making them a more cost-effective solution for SMBs in the long run.

Hence, AI-integrated encryption systems outperform traditional methods across key performance metrics such as processing time, scalability, and cost-effectiveness. By leveraging AI to optimize encryption processes, SMBs can achieve higher data security while maintaining efficient and cost-effective operations. This makes AI-integrated encryption an increasingly attractive option for businesses looking to protect their data in a rapidly evolving digital landscape.

3.6. AI-Driven Threat Detection and Response in Encryption

In the evolving landscape of cybersecurity, maintaining the capacity to recognize threats and take immediate action in real-time is essential to the integrity of encryption systems. Traditional encryption methods, while effective at securing data, often lack the capability to respond dynamically to emerging threats (). This is where AI-driven threat detection and response systems offer a significant advantage, particularly for SMBs that face increasing risks from sophisticated cyberattacks.

Traditional encryption systems typically rely on predefined rules and static algorithms to protect data. While these methods can effectively secure data under normal conditions, they may struggle to detect and respond to novel or complex threats (Olubudo, 2024). For example, traditional systems may not recognize patterns of behavior that indicate a sophisticated phishing attack or an advanced persistent threat (APT). As a result, these systems are often reactive rather than proactive, responding to threats only after they have been detected, which can be too late to prevent damage.

AI-driven encryption systems, on the other hand, are designed to detect and respond to threats in real time, offering a proactive approach to data security. By leveraging machine learning algorithms, massive data sets can be analyzed by AI to find trends and abnormalities that might point to a possible threat (Ibrahim, 2024). AI can detect unusual access patterns or data transfers that deviate from normal behavior, flagging them for further investigation or automatically initiating countermeasures. This real-time detection capability is particularly valuable in financial transactions, where the speed and accuracy of threat detection are critical to preventing fraud and data breaches.

Furthermore, AI-driven systems can adapt to evolving threats by continuously learning from new data. As cyber threats become more sophisticated, AI algorithms can be updated to recognize new attack vectors and strategies, ensuring that the encryption system remains effective against the latest threats (Paul, 2024). This adaptability is a significant advantage over traditional systems, which may require manual updates or reconfiguration to address new security challenges.

In addition to improving threat detection, AI also enhances encryption systems' response capabilities. Once a threat is detected, AI can automatically adjust encryption protocols, increase the security level of ongoing transactions, or isolate affected systems to prevent the spread of an attack (Kumar et al., 2023). This rapid response capability is essential for minimizing the impact of a security breach and ensuring the continued protection of sensitive data.

Hence, AI-driven threat detection and response systems significantly enhance traditional encryption methods. By providing real-time detection, adaptive learning, and automated response capabilities, AI ensures that encryption systems remain resilient against evolving cyber threats. For SMBs, this translates to increased trust in their capacity to safeguard sensitive financial information and uphold the integrity of their business practices in a risky and complicated digital environment.

4. Discussion of findings

Symmetric encryption, like the Advanced Encryption Standard (AES), is widely used by SMBs for securing financial data due to its robustness, speed, and efficiency. It uses a single key for both encryption and decryption, making it suitable for high-volume data processing. However, its security relies heavily on key management; if the key is compromised, the data becomes vulnerable. Asymmetric encryption, such as RSA, addresses some limitations by using a public-private key pair, which is effective for secure communications and digital signatures. However, it is computationally intensive and at risk from future quantum computing threats.

In response to these challenges, AI-powered encryption technologies have emerged as promising solutions. AI-enhanced homomorphic encryption allows computations on encrypted data without decryption, optimizing security and efficiency for SMBs handling sensitive financial information. Quantum-resistant encryption is also critical, with AI

helping to develop algorithms that withstand quantum attacks. AI-driven adaptive encryption marks a significant advancement, as it dynamically adjusts encryption protocols based on real-time threat levels, providing SMBs with robust, automated security that aligns with current risks. These AI-driven innovations offer SMBs future-proof encryption solutions, safeguarding financial data against evolving cyber threats.

The integration of traditional and AI-powered encryption technologies offers a comprehensive solution to the financial security challenges SMBs face. Traditional methods like AES and RSA provide a strong foundation of security, particularly when combined with robust key management practices and regular updates to address emerging threats. However, the limitations of these methods, especially in the face of new challenges like quantum computing, necessitate the adoption of AI-powered solutions.

AI-driven encryption technologies complement traditional methods by enhancing their flexibility, adaptability, and resilience. For instance, AI can be used to optimize the implementation of AES in environments where processing speed is critical or to bolster RSA's security against quantum threats through the development of quantum-resistant algorithms. Moreover, AI's ability to dynamically adjust encryption protocols in real time ensures that SMBs can maintain high security even as the cyber threat landscape evolves.

Hence, the state of encryption technologies in SMB financial security is characterized by a blend of traditional and AI-powered approaches. While traditional encryption methods provide a reliable baseline for data protection, AI-driven innovations offer the necessary enhancements to meet the demands of a rapidly changing digital environment. By integrating these technologies, SMBs can achieve a more comprehensive and resilient security posture, ensuring the protection of sensitive financial data in an increasingly complex and dangerous cyber landscape.

4.1. Implication

The findings of this study highlight significant implications for small and medium-sized businesses (SMBs) considering the adoption of AI-driven encryption solutions. One of the key takeaways is the balance between initial costs and long-term benefits. Although AI-driven encryption may require a higher upfront investment, particularly in terms of acquiring advanced technology and expertise, it can lead to substantial long-term savings. This is achieved by automating processes that would traditionally require manual intervention, such as key management and security updates. Consequently, while traditional encryption methods might seem more cost-effective initially, they often result in ongoing expenses that can outweigh the initial savings as the business scales.

Scalability emerges as another critical advantage of AI-driven encryption. Traditional methods often struggle to keep pace with increasing data volumes, necessitating considerable resources to maintain effective security. In contrast, AI-driven solutions are inherently more scalable, as they can dynamically adjust encryption protocols based on real-time data demands and the evolving threat landscape. This adaptability ensures that SMBs can maintain high levels of security without the need for significant manual oversight, making AI-enhanced solutions more practical as businesses grow and data requirements expand.

Moreover, AI-driven encryption offers superior protection against modern and emerging threats, such as those posed by quantum computing. Traditional methods like AES and RSA, while still useful, are increasingly vulnerable to sophisticated cyberattacks. AI-enhanced encryption techniques, including homomorphic encryption and quantum-resistant algorithms, provide a higher level of security, especially in complex and evolving threat environments. The ability of AI to monitor and respond to threats in real-time ensures that encryption remains robust, even as new vulnerabilities arise.

4.2. Future Research Directions

Current research on AI-driven encryption has made significant strides, yet gaps remain, particularly in the seamless integration of AI into existing encryption infrastructures. One key challenge is the compatibility of AI-enhanced encryption techniques, like homomorphic encryption and quantum-resistant algorithms, with legacy systems that SMBs often rely on. These systems may not be designed to support the computational demands and dynamic nature of AI-driven solutions, leading to potential inefficiencies and security vulnerabilities during integration.

Moreover, there is limited research on the real-world application and scalability of AI-powered encryption in diverse SMB environments. Studies often focus on theoretical models or large-scale enterprises, leaving a gap in understanding how these technologies can be tailored to the specific needs and constraints of smaller businesses.

Future research should explore methods to bridge these gaps, such as developing lightweight AI algorithms that can be more easily integrated with existing encryption protocols. Additionally, research should focus on creating standardized frameworks for implementing AI-driven encryption across various SMB platforms, ensuring scalability and ease of adoption. Finally, empirical studies that assess the effectiveness and cost implications of these integrations in real-world SMB scenarios are essential for guiding practical implementation and driving broader adoption of AI-enhanced encryption technologies.

5. Conclusion

In conclusion, the analysis highlights the critical role that both traditional and AI-powered encryption technologies play in safeguarding financial data for small and medium-sized businesses (SMBs). While traditional methods like AES and RSA have long been effective in providing robust security, they are increasingly challenged by sophisticated cyber threats and the impending rise of quantum computing. AI-driven encryption solutions offer a promising advancement, bringing greater adaptability, scalability, and real-time threat detection to the table. These innovations are particularly valuable for SMBs, which often face resource constraints in managing complex security infrastructures.

However, the integration of AI into existing systems presents challenges, particularly in terms of compatibility and cost. Addressing these issues requires ongoing research and development, focusing on creating more accessible and scalable AI encryption methods tailored to the needs of SMBs. Ultimately, the study underscores the importance of a hybrid approach, combining the strengths of both traditional and AI-powered encryption to build a more resilient and future-proof security framework. By embracing these advanced technologies, SMBs can better protect their financial data, ensuring business continuity and maintaining trust in an increasingly volatile digital landscape.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest/ Competing Interests in the publication of the manuscript or with any institution or product that is mentioned in the manuscript and/or is important to the outcome of the study presented.

References

[1] Aldoseri A, Al-Khalifa KN, Hamouda AM. Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges. Appl Sci. 2023;13:7082. https://doi.org/10.3390/app13127082

[2] Al-Shabi M. A Survey on Symmetric and Asymmetric Cryptography Algorithms in Information Security. Int J Sci Res Publ (IJSRP). 2019;9:8779. https://doi.org/10.29322/IJSRP.9.03.2019.p8779

[3] Bani Yassein M, Qawasmeh E, Khamayseh Y, Mardini W. Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms. 2017. https://doi.org/10.1109/ICEngTechnol.2017.8308215

[4] Baseri Y, Chouhan V, Hafid A. Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. Comput Secur. 2024;142. Available: https://doi.org/10.1016/j.cose.2024.103883

[5] Danquah P, Kwabena-Adade H. Public Key Infrastructure: An Enhanced Validation Framework. J Inf Secur. 2020;11:241-260. https://doi.org/10.4236/jis.2020.114016

[6] Emmanni PS. The Impact of Quantum Computing on Cybersecurity. J Math Comput Appl. 2023;2:1-4. https://doi.org/10.47363/JMCA/2023(2)140

[7] Familoni BT. Cybersecurity Challenges in the Age of AI: Theoretical Approaches and Practical Solutions. 2024;5:703-724. Available at: file:///C:/Users/acer/Downloads/930-Article%20Text-2404-1-10-20240321%20(1).pdf

[8] Farooq M, Mubashir H. AI-Driven Network Security: Innovations in Dynamic Threat Adaptation and Time Series Analysis for Proactive Cyber Defense. Int J Wirel Microw Technol. 2024;14:17-26. https://doi.org/10.5815/ijwmt.2024.02.02

[9] Haverkamp I, Sarmah DK. Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis. Int J Inf Secur. 2024;23:2607–2635. https://doi.org/10.1007/s10207-024-00853-9

[10] Issad M, Anane N, Bellemou M, Boudraa B. Secure Hybrid Crypto-system AES/RSA on FPGA for Data Communication. Malays J Comput Appl Math. 2020;3:14-23. https://doi.org/10.37231/myjcam.2020.3.1.38

[11] Khan A, Basharat S, Riaz M. Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange. 2018. https://doi.org/10.13140/RG.2.2.30495.61602

[12] Kumar S, Gupta U, Singh A, Singh A. Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era. J Comput Mech Manag. 2023;2:31-42. https://doi.org/10.57159/gadl.jcmm.2.3.23064

[13] Li B, Feng Y, Xiong Z, et al. Research on AI security enhanced encryption algorithm of autonomous IoT systems. Inf Sci. 2021;575:379-398. Available at: https://doi.org/10.1016/j.ins.2021.06.016

[14] Manoharan A, Sarker M. Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. Int Res J Mod Eng Technol Sci. 2022;4:2151-2164.

[15] Olubudo P. Data Encryption Techniques: Evolution and Future Directions. 2024.

[16] Orucho D, Awuor F, Makiya R, Oduor C. Review of Algorithms for Securing Data Transmission in Mobile Banking. Mod Econ. 2023;14:1192-1217. https://doi.org/10.4236/me.2023.149062

[17] Paul A. The Role of Artificial Intelligence in Enhancing Data Security. 2024.

[18] Prashant, Haque MD, Kaur A, Yadav P. Comparative Analysis of AES and RSA with Other Encryption Techniques for Secure Communication. Int J Sci Res Comput Sci Eng Inf Technol. 2024;10:565-574. https://doi.org/10.32628/CSEIT2410263 Qureshi MB, Qureshi MS, Tahir S, Anwar A, Hussain S, Uddin M, Chen C-L. Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud. Symmetry. 2022;14:695.

[19] Radanliev P. Artificial intelligence and quantum cryptography. J Anal Sci Technol. 2024;15. https://doi.org/10.1186/s40543-024-00416-6

[20] Ramos-Cruz B, Andreu-Perez J, Martínez L. The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. Neurocomputing. 2023;581. https://doi.org/10.1016/j.neucom.2024.127427

[21] Rana S, Parast KF, Kelly B, et al. A comprehensive survey of cryptography key management systems. J Inf Secur Appl. 2023;78. https://doi.org/10.1016/j.jisa.2023.103607

[22] Rowland H. The role of prime numbers in RSA cryptosystems. 2016. Available at: https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/rowland.pdf

[23] Ruman K, Phaneendra HD. Implementation of methods for transaction in secure online banking. Int J Technol Res Appl. 2015;3:41-43. Available at: https://www.ijtra.com/view/implementation-of-methods-for-transaction-in-secure-online-banking.pdf

[24] Iwasokun G, Akinyokun O, Alawode S, Omomule T. An RSA algorithm for securing financial data on the cloud. Int J Math Comput Sci. 2019;34. https://doi.org/10.9734/JAMCS/2019/v34i330215

[25] Satapathy A, Livingston J. A comprehensive survey on SSL/TLS and their vulnerabilities. Int J Comput Appl. 2016;153:31-38. https://doi.org/10.5120/ijca2016912063

[26] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. Healthcare data breaches: Insights and implications. Healthcare (Basel). 2020;8(2):133. https://doi.org/10.3390/healthcare8020133

[27] Shallal Q, Bokhari M. A review on symmetric key encryption techniques in cryptography. Int J Comput Appl. 2016;43.

[28] Singh S, Kumar D. Enhancing cyber security using quantum computing and artificial intelligence: A review. Int J Adv Res Sci Commun Technol. 2024;4:2581-9429. https://doi.org/10.48175/IJARSCT-18902

[29] Sousi AL, Yehya D, Joudi M. AES encryption: Study & evaluation. 2020.

[30] Su G, Wang J, Xu X, Wang Y, Wang C. The utilization of homomorphic encryption technology grounded on artificial intelligence for privacy preservation. Int J Comput Sci Inf Technol. 2024;2:52-58. https://doi.org/10.62051/ijcsit.v2n1.07

[31] Tanwar S, Kumar A. Extended design and implementation of certificate authorities. Int J Secur Appl. 2017;11:13-26. https://doi.org/10.14257/ijsia.2017.11.8.02

[32] Tawfiq F, Rahma AM, Abdulwahab H. A secure environment using a new lightweight AES encryption algorithm for e-commerce websites. Secur Commun Netw. 2021:1-15. https://doi.org/10.1155/2021/9961172

[33] Trzupek B. PKI is key to securing a post-Covid remote workforce. Comput Fraud Secur. 2020;2020(10):11–3. https://doi.org/10.1016/S1361-3723(20)30108-1

[34] Umoga U, Sodiya E, Ugwuanyi E, et al. Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. Magna Sci Adv Res Rev. 2024;10:368-378. https://doi.org/10.30574/msarr.2024.10.1.0028

[35] Zodpe H, Shaikh A. A survey on various cryptanalytic attacks on the AES algorithm. Int J Next-gen Comput. 2021;12. Available at: https://ijngc.perpetualinnovation.net/index.php/ijngc/article/view/202