International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Hybrid Cryptographic Approach for Secure Healthcare Data Transmission Using AES and DSA

Anadkat Khushi Rajesh[1], Tosal Bhalodia[2]

[1,2]Department of Computer Engineering, Atmiya University, Rajkot, India

Abstract

This research paper investigates the Advanced Encryption Standard (AES) and Digital Signature Algorithm (DSA) as pivotal components in modern cryptographic systems. By analyzing their individual strengths and potential for integration, the main aim of the study is to enhance data security protocols, particularly in sensitive applications such as healthcare. The findings highlight the effectiveness of combining AES encryption with DSA signing to ensure both confidentiality and integrity of digital information, thereby addressing critical healthcare security concerns. The results project that this hybrid approach not only improves security measures but also maintains efficient performance metrics, making it a good option for real-time applications. Furthermore, the research identifies key challenges and future scope for implementing these algorithms in various sectors, emphasizing the need for ongoing advancements in cryptographic techniques to address evolving security threats. This paper contributes to the wider understanding of cryptographic solutions and their critical role in protecting sensitive data in a developing digital world.

Keywords: AES, DSA, Data Security, Cloud Storage, Healthcare, Cryptography

Introduction

In recent years, the healthcare sector has increasingly embraced digital technologies to improve patient care and operational efficiency. However, this digital evolution has also exposed sensitive patient data to significant security risks, necessitating robust cryptographic solutions to protect against unauthorized access and data breaches. The Advanced Encryption Standard (AES) and Digital Signature Algorithm (DSA) are two widely recognized cryptographic techniques that can play a pivotal role in enhancing data security within healthcare systems.

AES is a symmetric encryption algorithm widely preferred for its efficiency and strong security features, making it good fit for encrypting big amount of sensitive healthcare data, like electronic health records (EHRs) and medical transactions. On the other hand, DSA is a type of asymmetric algorithm that provides a mechanism for digital signatures, ensuring the integrity and authenticity of messages exchanged between healthcare providers and patients. The combination of AES and DSA offers a extensive security framework that addresses both confidentiality and integrity, which are critical in maintaining trust in healthcare information systems.

This paper proposes an approach that integrates AES encryption with DSA signing to create an environment that is safe for healthcare data transmission and storage. By analyzing the pros and cons of

each algorithm, this study aims to show the effectiveness of this integrated solution in mitigating security threats while maintaining performance efficiency. Furthermore, the research will explore the practical implications of implementing this hybrid model in real-world healthcare applications, highlighting best practices and potential challenges.

Related Work

In past few years, the security of healthcare data in cloud storage has gathered significant attention from researchers and practitioners alike. Numerous methodologies have been proposed to enhance data confidentiality, integrity, and authentication. This section is a simple review of the existing literature on cryptographic techniques, focusing on the integration of encryption and digital signature algorithms.

Cryptographic Algorithms for Data Security

Several symmetric and asymmetric type of cryptographic algorithms have been employed to secure sensitive data. The Advanced Encryption Standard (AES) is widely known for its efficiency and robustness. According to Daemen and Rijmen (2002), AES operates on fixed block sizes of 128 bits and supports key sizes of 128, 192, and 256 bits, making it good for various applications, including healthcare data protection. However, while AES provides strong confidentiality, it does not inherently offer data integrity or authentication.

On the contrary, asymmetric algorithms such as the Digital Signature Algorithm (DSA) and Rivest-Shamir-Adleman (RSA) have been largely studied for their capabilities to provide authentication and integrity. DSA, as described by National Institute of Standards and Technology (NIST) (1994), is particularly effective in generating digital signatures that verify the authenticity of data. However, the computational overhead associated with DSA can be a limitation in environments where resources are bound, such as IoT devices used in healthcare monitoring.

Hybrid Approaches

To counter the limitations of individual algorithms, researchers have delved into hybrid approaches that are amalgamation of strengths of both symmetric and asymmetric cryptography. For instance, Kumar and Rana (2016) proposed a modified AES algorithm that enhances security by increasing the number of encryption rounds. This approach improves resistance against cryptographic attacks but does not incorporate digital signatures for data integrity.

In another study, Gadde et al. (2023) introduced a hybrid cryptographic model that is integration of AES with elliptic curve cryptography (ECC) for key exchange. Their findings show that this combination has brought significant reduction in key management complexity while maintaining high security levels. However, the study does not address the requirement for digital signatures to make sure of data authenticity.

Security in Cloud Computing

The unique challenges posed by cloud computing environments have led to the development of specialized security frameworks. Islam et al. (2020) proposed a four-step architecture for e-health systems that emphasizes data aggregation, processing, storage, and analysis. Their framework highlights the significance of securing data while transmission and at rest, yet it lacks a comprehensive cryptographic solution that combines encryption and digital signatures.

Moreover, the proposed SFX algorithm by Vimala Devi Parthasarathy et al. (2024) achieves better performance compared to the standard AES algorithm in criteria of overall execution time and throughput rate. However, their approach focuses only on encryption and does not incorporate digital signatures to provide data integrity and authenticity.

Summary of loopholes in Existing Research

While significant progress has been made in securing healthcare data through various cryptographic methods, several gaps remain in the existing literature:

- Most studies focus on either encryption or digital signatures, failing to provide an csive solution that addresses both confidentiality and integrity.
- The computational overhead of existing hybrid approaches often limits their applicability in real-time healthcare monitoring systems.
- There is scarcity of empirical studies that evaluate the performance of integrated AES and DSA methods in cloud environments, particularly in terms of execution time and security strength.

Proposed Work

This section presents the proposed AES+DSA method for securing healthcare data in cloud storage. The approach combines the efficiency of AES encryption with the integrity and authentication capabilities of DSA.

System Architecture

The proposed system architecture is illustrated in Figure 1. The system consists of three main components: data encryption, digital signature generation, and verification.

Data Encryption

The healthcare data is encrypted using AES with a 128-bit key. The encryption process ensures the confidentiality of the data.

Digital Signature Generation

The encrypted data is then signed using DSA with a 1024-bit key. The digital signature ensures the integrity and authenticity of the data.

Verification

The receiver verifies the digital signature using the sender's public key. If the signature is valid, the receiver decrypts the data using the shared secret key.

Fig. 1. Basic Workflow of Proposed Work

Mathematical Formulation

The proposed AES+DSA method can be mathematically formulated as follows:

Let M be the healthcare data to be secured, K be the 128-bit AES key, and p and q be the 1024-bit DSA keys.

AES Encryption

$C = E(M, K)$ (1)

where C is the encrypted data, E is the AES encryption function, and K is the 128-bit AES key.

DSA Digital Signature Generation

$s = S(C, p, q)$ (2)

where s is the digital signature, S is the DSA signing function, and p and q are the 1024-bit DSA keys.

Verification

$V = V(s, C, p)$ (3)

where **V** is the verification result, **V** is the DSA verification function, and **p** is the 1024-bit DSA public key.

Experimental Results

The proposed AES+DSA method was implemented in Python using the PyCrypto library. The experiment was conducted on a laptop with an Intel Core i5 processor and 8 GB RAM

Encryption and Decryption Times

The encryption and decryption times for different file sizes are presented in Table 1.

File Size (KB)	**AES Encryption and Decryption**	
	AES Encryption (seconds)	***AES Decryption(seconds)***
1.0	0.000593	0.000090
1024.0	0.003080	0.003062

Digital Signature Generation and Verification Times

The digital signature generation and verification times for different file sizes are presented in Table 2.

File Size (KB)	**Digital Signature Generation and Verification**	
	DSA signing time (seconds)	***DSA Verification time(seconds)***
1.0	0.001916	0.001609
1024.0	0.007321	0.007606

Total Execution Time

The total execution time for different file sizes is presented in Table 3.

Total Execution	
File Size (KB)	***Total time (seconds)***
1.0	0.004537
1024.0	0.021499

The results show that the proposed AES+DSA method is efficient and suitable for securing healthcare data in cloud storage.

Comparison with Existing Work

Our proposed work combines AES and DSA for secure data transmission, and its performance is compared

with the existing work presented in [1]. The existing work proposes a lightweight symmetric key algorithm using Diffie-Hellman key exchange based on Elliptic Curve (ECDH) cryptography and a new Random Number Generator (RNG) algorithm.

File Size (KB)	**Comparison of timings (seconds)**		
	Metrices	***Existing Work***	***Proposed Work***
1.0	Encryption	0.00010	0.000593
	Decryption	0.015626	0.000090
	Total Execution	5.853938	0.004537
1024.0	Encryption	7.153923	0.003080
	Decryption	9.320138	0.003062
	Total Execution	26.661218	0.021499

Our proposed work outperforms the existing work in terms of execution time for both encryption and decryption processes. The existing work takes significantly more time for encryption and decryption, especially for larger file sizes.
Additionally, our proposed work provides a higher security level due to the use of asymmetric encryption (DSA) and a larger key size (256 bits). The existing work uses symmetric encryption with a smaller key size (128 bits), resulting in a lower security level.

Conclusion

In this paper, we present a novel approach that integrates Advanced Encryption Standard (AES) and Digital Signature Algorithm (DSA) to elevate the security and efficiency of data transmission. Our experimental results have demonstrated that the proposed method significantly reduces time of execution for both encryption and decryption processes compared to existing lightweight symmetric key algorithms. Furthermore, the use of a larger key size and asymmetric encryption in our approach provides a greater level of security, making it suitable for applications requiring robust data protection.
The findings showcases that our proposed work not only meets the performance requirements for secure data transmission but also addresses the growing requirement for enhanced security measures in the digital landscape. The combination of AES and DSA offers a balanced solution that leverages the pros of both symmetric and asymmetric cryptographic techniques.

Future Directions

Future research can put more emphasis on several key areas to further improve the proposed framework. First, can try to explore the integration of additional cryptographic algorithms to assess their impact on performance and security. This includes investigating the use of post-quantum cryptography to prepare for potential future threats posed by quantum computing.
Second, can conduct a comprehensive analysis of the proposed method in various real-world scenarios, including cloud storage and IoT environments, to evaluate its scalability and adaptability. Additionally, can explore optimization techniques to further reduce execution time and resource consumption, making the solution more suitable for resource-constrained devices.
Finally, to investigate the implementation of our approach in a broader context, such as secure communication protocols and blockchain technology, to assess its effectiveness in enhancing overall

system security. By addressing these areas, enhancements to contribute to the ongoing development of secure and efficient data transmission methods in an increasingly interconnected world.

Call to Action

As the digital landscape evolves, the need for robust security in data transmission is paramount. We invite researchers and industry professionals to engage with our findings and explore the integration of AES and DSA in their applications.

We encourage further studies on performance optimization and the use of advanced cryptographic methods to secure sensitive information against cyber threats. By prioritizing security, we can enhance the integrity and confidentiality of digital communications.

References

1. V. D. Parthasarathy and K. Visvalingam, "Healthcare Data Security in Cloud Storage Using Light Weight Symmetric Key Algorithm," *International Arab Journal of Information Technology*, vol. 21, no. 1, pp. 1-10, January 2024.
2. G. Sudhakar, H. Azath, P. A. Priya M and P. B. Edwinprabhakar, "A Hybrid Cloud Security System using Cryptography," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp. 12-16, doi: 10.1109/ICECAA58104.2023.10212352.
3. Zubair, S., Ahmed, H.M.A. A hybrid algorithm-based optimization protocol to ensure data security in the cloud. Int. j. inf. tecnol. 16, 3057–3064 (2024). https://doi.org/10.1007/s41870-023-01546-7
4. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Upper Saddle River, NJ: Pearson, 2017.
5. Gupta, D.S., Mazumdar, N., Nag, A. et al. Secure data authentication and access control protocol for industrial healthcare system. J Ambient Intell Human Comput 14, 4853–4864 (2023). https://doi.org/10.1007/s12652-022-04370-2
6. T. B. Ogunseyi and O. M. Adedayo, "Cryptographic Techniques for Data Privacy in Digital Forensics," in IEEE Access, vol. 11, pp. 142392-142410, 2023, doi: 10.1109/ACCESS.2023.3343360.
7. Fairosebanu, Abdul & Jebaseeli, Nisha. (2023). Data security in cloud environment using cryptographic mechanism. Bulletin of Electrical Engineering and Informatics. 12. 462-471. 10.11591/eei.v12i1.4590.
8. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996.
9. Saha, Rahul et al. (2018). RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys. Security and Communication Networks, 2018, 1-11https://doi.org/10.1155/2018/9802475