iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

A COMPARATIVE ANALYSIS OF NETWORK SECURITY ALGORITHMS: STRENGTHS, WEAKNESSES, AND PERFORMANCE EVALUATION

DVH Venu Kumar, Ch. Venkateswarlu, K. Chiranjeevi
MTech (CSE), Dept. Of CSE, venukumardvh@gmail.com
MTech (CSE), Dept. Of CSE, venkibbb@gmail.com
MTech (CSE), Dept. Of CSE, chiranjeevi.kasukurthy@gmail.com

ABSTRACT
With the rapid growth of digital communication, ensuring network security has become a critical challenge. Various cryptographic and security algorithms have been proposed to safeguard data transmission against cyber threats. This paper provides a comparative analysis of different network security algorithms, including symmetric and asymmetric encryption techniques, hash functions, and authentication mechanisms. The study evaluates these algorithms based on computational efficiency, security strength, and vulnerability to attacks. Simulation results and comparative performance analysis demonstrate that while AES provides robust security for data encryption, RSA ensures secure key exchange, and SHA-256 enhances data integrity. The research highlights the strengths and weaknesses of each approach and recommends optimal security strategies based on application requirements.

Keywords:
Network security, cryptography, encryption, authentication, AES, RSA, SHA-256.

1. INTRODUCTION

The expansion of the Internet and cloud-based systems has increased security concerns in data transmission, making network security algorithms essential for protecting confidential information. Security mechanisms such as encryption, authentication, and intrusion detection systems (IDS) aim to safeguard sensitive data from unauthorized access, eavesdropping, and cyberattacks [1].

Encryption algorithms, including symmetric (AES, DES, 3DES) and asymmetric (RSA, ECC), play a crucial role in securing data. Additionally, cryptographic hash functions such as MD5 and SHA ensure data integrity, while authentication techniques like digital signatures enhance user verification. Despite advancements, security algorithms remain vulnerable to brute-force, side-channel, and quantum attacks [2].

This paper presents an in-depth analysis of various network security algorithms, evaluating their strengths, weaknesses, and performance metrics. The objective is to guide researchers and practitioners in selecting the most suitable security mechanism based on network requirements and computational efficiency.

2. NETWORK SECURITY ALGORITHMS

2.1 Symmetric Encryption Algorithms

2.1.1 Advanced Encryption Standard (AES)

AES is a widely used symmetric encryption algorithm that operates on 128, 192, or 256-bit keys. It utilizes multiple rounds of substitution and permutation for secure encryption [3]. AES is resistant to brute-force attacks due to its long key length but is susceptible to side-channel attacks.

2.1.2 Data Encryption Standard (DES) and Triple DES (3DES)

DES uses a 56-bit key and 16 encryption rounds, making it vulnerable to brute-force attacks. 3DES enhances security by applying DES three times with different keys, increasing complexity but reducing efficiency [4].

2.2 Asymmetric Encryption Algorithms

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

2.2.1 RSA (Rivest–Shamir–Adleman)
RSA relies on large prime number factorization for encryption and key exchange. It provides strong security but requires high computational power, making it less efficient for real-time applications [5].

2.2.2 Elliptic Curve Cryptography (ECC)
ECC offers security equivalent to RSA but with shorter key lengths, reducing computational overhead. It is widely used in mobile and IoT security applications [6].

2.3 Cryptographic Hash Functions

2.3.1 SHA (Secure Hash Algorithm) Family
SHA-256, a member of the SHA-2 family, generates a fixed-length 256-bit hash, ensuring data integrity. It is widely adopted in blockchain security and digital signatures [7].

2.3.2 MD5 (Message Digest Algorithm 5)
MD5 produces a 128-bit hash but is vulnerable to collision attacks, making it unsuitable for secure applications [8].

2.4 Authentication Mechanisms

2.4.1 Digital Signatures
Digital signatures use asymmetric cryptography to verify the authenticity of messages, commonly employed in electronic transactions and secure communications [9].

2.4.2 Biometric Authentication
Biometric security, such as fingerprint and facial recognition, provides enhanced authentication but raises privacy concerns [10].

3. Comparative Analysis of Security Algorithms
To assess the efficiency of security algorithms, a comparative analysis based on encryption speed, key length, and attack resistance is provided in Table 1.

Algorithm	Key Length	Security Level	Computational Overhead	Vulnerabilities
AES	128, 192, 256-bit	High	Moderate	Side-channel attacks
DES	56-bit	Low	Low	Brute-force attacks
3DES	168-bit	Medium	High	Slow performance
RSA	1024, 2048-bit	High	Very High	Quantum computing threats

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

ECC	160-521-bit	High	Low	Implementation flaws
SHA-256	256-bit	High	Low	Collision resistance
MD5	128-bit	Low	Low	Collision attacks

4. Performance Evaluation and Simulation Results

Experiments were conducted using MATLAB and OpenSSL to analyze the encryption time and decryption latency of AES, RSA, and SHA-256 under different data sizes. Results indicate that:
AES-256 provides fast encryption with minimal computational overhead.
RSA-2048 exhibits slower performance due to key length but ensures strong security.
SHA-256 performs efficiently for integrity verification but lacks encryption capabilities.

5. Conclusion and Future Work

This paper presents a comparative study of network security algorithms, highlighting their advantages and limitations. AES remains a robust choice for encryption, while RSA is preferable for secure key exchange. Future research should explore quantum-resistant cryptographic techniques such as lattice-based encryption to counter emerging threats.

REFERENCES

[1] Stallings, W. (2006). Cryptography and Network Security: Principles and Practice. Pearson Education.
[2] Schneier, B. (2005). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.
[3] Daemen, J., & Rijmen, V. (2011). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.
[4] Diffie, W., & Hellman, M. E. (2007). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.
[5] Rivest, R. L., Shamir, A., & Adleman, L. (2005). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.
[6] Koblitz, N. (2009). Elliptic Curve Cryptography. Mathematics of Computation, 48(177), 203-209.
[7] National Institute of Standards and Technology (2012). Secure Hash Standard (SHS) - FIPS PUB 180-4.
[8] Wang, X., & Yu, H. (2005). How to Break MD5 and Other Hash Functions. EUROCRYPT, 19-35.
[9] Menezes, A., van Oorschot, P., & Vanstone, S. (2010). Handbook of Applied Cryptography. CRC Press.
[10] Jain, A., Ross, A., & Pankanti, S. (2006). Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security, 1(2), 125-143.