

REVIEW OF THE ROLE OF ENCRYPTION PROTOCOLS IN PROTECTING NETWORK COMMUNICATION SYSTEMS.

Idris, Saheed Asimiu¹; Ibrahim, Hussain²; Koleosho, Saheed Adedimeji³; Amoo, Mutiu Adewale⁴ and Egbonwonu, Patricia Nkiru⁵

^{1,2}Department of Computer Science, Federal Polytechnic Ohodo, Enugu State

³Owu College of Education, Wasimi, Ogun State, Nigeria

⁴Federal College of Forestry, Jericho, Ibadan

⁵Department of Computer Engineering, Federal Polytechnic Ohodo, Enugu State

saheed.idris@fedpod.edu.ng

Abstract:

Digital communication technologies have rapidly developed providing capacity and giving rise of transmission of sensitive information over computer networks. Whether it is an organization, a government department, or financial institutions, everyone needs safe communication systems to secure sensitive information from unauthorized access, cyberattacks, and data breaches. But growing risk of cyber threats like eavesdropping, man-in-the-middle (MitM) attacks, ransomware, spoofing, phishing, session hijacking and interception of data put holes in the network communication system. Encryption protocols have evolved to ensure confidentiality, integrity, authentication of information and non-repudiation. A systematic Literature Review of Encryption Protocols for Secure Network Communication Systems and a Conceptual Framework. It reviews popular encryption algorithms such as Advanced Encryption Standard (AES); Rivest-Shamir-Adleman (RSA); Elliptic Curve Cryptography (ECC); Transport Layer Security (TLS); Internet Protocol Security (IPSec); Secure Shell (SSH), Virtual Private Networks (VPNs) and End-to-End Encryption E2EE. The results show that contemporary encryption protocols dramatically mitigate the risks of unauthorized access, data interception and cyber espionage while enabling secure online banking, cloud computing, e-commerce and Internet of Things (IoT) communications. However, challenges ranging from computational power overhead to weak key management to implementation bugs and the advent of quantum computing still pose risks for cryptographic security. The report advises various measures to protect networks, such as modern encryption standards, Public Key Infrastructure (PKI), Zero Trust security principles, multi-factor authentication, continuous cryptographic updates and quantum-resistant encryption algorithms.

Keywords: Encryption, Cryptography, Network Security, TLS AES RSA, Internet Security, Cyber security

1.0 Introduction

Computer networks are of utmost importance in modern society because they support communication, commerce, education, health care, government operations and industrial automation. Cloud computing, mobile technologies, electronic commerce, online banking, remote work and a wider range of Internet of Things (IoT) devices has caused more sensitive information to flow across public and private networks than ever before in history. As a result, securing information during transit is now an important concern for individuals, businesses and even governments.

Background: Network communication systems are constantly threatened by cyber attacks that focus on compromising confidentiality, integrity, and availability of information. Cybercriminals misuse unsecured

Cite this article as:

Idris et al (2025). Review of the Role of Encryption Protocols in Protecting Network Communication Systems.

Journal of Multidisciplinary Innovations and Perspectives (JMIP), 1(2) 119-128.

communication channels by launching eavesdropping, packet sniffing, man-in-the-middle (MitM) attack, spoofing attacks, replay attacks or use of ransomware, phishing activity as well as session hijack and hacking for accessing sensitive information. These successful attacks can result in financial loss, identity theft, critical service disruption, reputational damage as well as violations of privacy regulations.

With the increasing reliance on network communication systems, organisations and individuals alike have become vulnerable to advanced cyber threats that seek sensitive user information during transit. Too many organizations are still being breached due to a lack of encryption; improperly managed keys, or poor key practices; using outdated communication protocols and insecure network configurations. In addition, new technologies such as cloud computing, IoT and quantum computing have also presented some security threats that the traditional cryptographic method cannot cope with. Hence it is essential to assess the importance of current encryption approaches for improving system communication protection.

This study seeks to review the use of encryption protocols in network communication systems and assess their abilities to secure information in cybersecurity. The specific objectives are to: Examine the importance of encryption in network communication systems and review major encryption algorithms and communication protocols used in modern networks.

The study will be useful for researchers, students in the field of computer science and information technology, network administrators, cybersecurity professionals, policymakers, organizations that look to enhance the confidentiality, integrity and availability information transmitted over the computer networks. The theoretical framework of this study can serve as a basis for future empirical studies and practice in corporate environments.

2.0 Literature Review

2.1 Concept of Cryptography

Cryptography solves this problem through the algorithm and key that is, cryptography converts readable data (plaintext) into unreadable data (ciphertext). It is among the most fundamental means of securing digital communications from unauthorized access, interception, and tampering. Confidentiality, integrity, authentication and non-repudiation are the four main purposes of cryptography.

Confidentiality means only a person authorized can read the information and integrity assures no data gets modified through the channel. Authentication provides assurance to the participants of the communication, whereas non-repudiation prevents users from denying they performed a transaction. These security services are necessary for e-commerce, online banking, cloud computing, healthcare information systems, government communications and enterprise networking.

Standardized algorithms and protocols over both public and private networks to make secure communication in modern day cryptographical system

2.2 Types of Encryption Techniques

Three Major Groups of Encryption Techniques are:

Symmetric Encryption

For symmetric encryption, the same private key is used to encrypt and decrypt information. As symmetric algorithms only need a single key, they are computationally efficient and well suited for encrypting large quantities of data. One of the most widely used symmetric algorithm is Advanced Encryption Standard (AES) which accepts key sizes of 128, 192 and 256 bits. AES provides high strength security as well as processing efficient, so it is most used cryptographic algorithm in wireless communication, cloud computing, VPN (Virtual Private Networks), secure file storage and government information system. Some symmetric algorithms like Blowfish, Twofish and ChaCha20 are designed for special purposes where speed of encryption is required.

Asymmetric Encryption

Asymmetric encryption uses two keys that are mathematically related in some manner and also is known as a Public-key cryptography: Public key (used for encryption) and Private Key (used for decryption). In contrast with symmetric encryption, the key to encrypt is a public one (in this case no trade-off on security if the key goes public). Common asymmetric algorithms include: Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH).

2.3 Role of Encryption in Network Security

Encryption protocols rival with cybersecurity functions in some crucial areas.

Data Confidentiality

Encryption stops any unallowed persons from reading data being transferred.

Authentication

Before any secure communication can take place, entities communicating are first authenticated using digital certificates, cryptographic keys and Public Key Infrastructure.

Data Integrity

Highest level Hash functions, and Message Authentication Codes (MACs) catch unauthorized changes to transmitted information.

Non-Repudiation

They prevent a user from denying that he has signed an electronic transaction or document.

Secure Key Exchange

Secure protocols like RSA, Diffie-Hellman and Elliptic Curve Diffie-Hellman for the secure exchange of keys over an insecure channel.

Network Encryption: Emerging Trends

With rapid advancements in technology, cryptographic research has witnessed a continuous evolution.

Zero Trust Security

Zero Trust Architecture enhances encryption by ensuring that no user or device can be trusted by default. Insider threats and misuse are lessened with continuous authentication & encrypted transmission.

Artificial Intelligence: As AI continues to support almost all cryptographic systems, applications of AI have begun taking intelligent threat detection, anomaly identification, automated management of certificates and cryptographic risk assessment too.

Blockchain Technology

It is an amalgamation of cryptographic hashing, digital signatures and decentralized consensus for making secure, transparent, and tamper-proof transactions on distributed systems.

2.5 Empirical Review

It is now well established through recent studies that strong encryption protocols greatly enhance network security. According to Stallings (2022), AES is the specification of a symmetric key algorithm based on block-cipher design principles established and used to encrypt and decrypt data.

According to Whitman and Mattord (2022); TLS and IPSec provide safe communications at the enterprise level by providing confidentiality, integrity, and authenticity across enterprises.

Katz and Lindell (2021) stressed that encryption algorithms are only as secure as their cryptographic key management. Likewise, NIST (2023) advised the migration into quantum-resistant cryptographic standards for protection from future quantum computing threats. Studies also show that encryption combined with Zero Trust Architecture, Multi-Factor Authentication, and Public Key Infrastructure gives more protection in contrast to just deployment of cryptographic algorithms.

3.0 Methodology

The study is a literature review which tends to locate, assess and synthesize academic work related to cryptographic algorithms, secure communication protocols and network security technologies. It uses the results from previous literature for a thorough assessment of knowledge that currently exists, identification of contemporary security issues and an examination of modern encryption methods, without conducting primary data collection.

3.2 Sources of Data

The research was based entirely on secondary data from academic and professional sources, which encompassed: Peer-reviewed journal articles, International conference proceedings, Books on cryptography and cybersecurity, IETF (Internet Engineering Task Force) standards, International Organization for Standardization (ISO/IEC) standards, IEEE, ACM, Springer, Elsevier and Taylor & Frances publications and Reports from both cyber security firms and technology vendors. The articles reviewed included modern encryption algorithms and secure

3.3 Reviewed Encryption Framework

Specifically, this research reviewed a multi-layered encryption framework for authenticated security during network communication systems based on literature that has been reviewed. This framework combines identity verification, secure key management and encryption protocols, authentication mechanisms, continuous monitoring and the like to protect cyber threats.

The framework consists of User Authentication, Public Key Infrastructure (PKI), Secure Key Exchange, Encryption Layer, Secure Communication Protocols, Integrity Verification, Security Monitoring and Incident Response. An integrated approach ensures the communication channels remain protected while sending data during transfer, thus reducing risks associated with unauthorized access and interception of data.

3.4 Conceptual Secure Communication Architecture

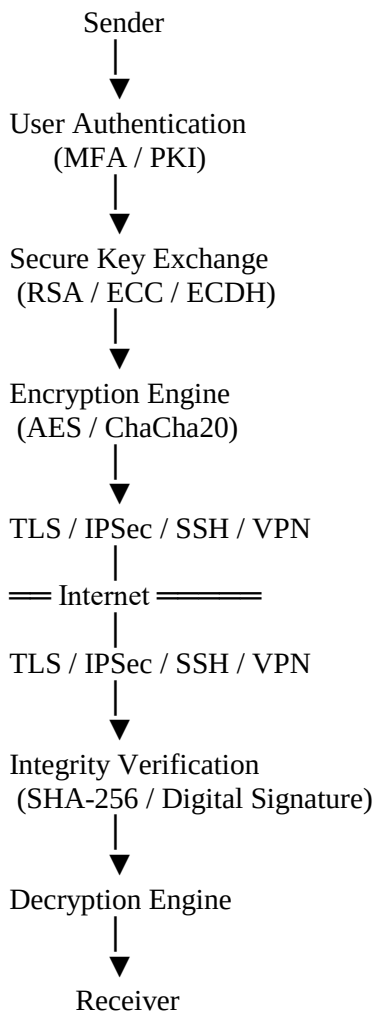


Figure 1: Conceptual secure communication Architecture (reference)

The architecture proposed describes how authentication, encryption, secure transmission, integrity verification and

plain text (decryption) work together to provide a defense plane to allow network communications free from the interception(tampering), impersonation.

3.5 Security Implementation Process

The steps involved in the application of the secure communication architecture framework included the use multi-factor authentication (MFA) and certificates to authenticate users and devices; an RSA, ECC or ECDH (EC Diffie Hellman) generate and exchange keys suitably in secured way; encrypt in transit data with strong symmetric ciphers (AES-256 or ChaCha20); the use of TLS, IPSec, SSH or VPN to protect the communication channels; ensure message integrity by using hashes function and digital signatures and the use of SIEM Systems to monitor for anomalies in communication sessions.

Identify a reasonable and automated incident response to quickly respond to detected threats.

The duo of this implementation process facilitates secure communication but reduces the risk of data exposure.

3.6 Evaluation Criteria

The performance metrics that may be used to assess the efficiency of encryption protocols are:

Performance Metric	Purpose
Encryption Speed	Measures processing efficiency
Decryption Speed	Evaluates communication performance
Confidentiality Level	Assesses protection against unauthorized access
Authentication	
Success Rate	Measures identity verification accuracy
Data Integrity Rate	Evaluates resistance to tampering
Key Management	
Efficiency	Assesses secure key distribution and storage
Resistance to Cyberattacks	Measures protection against MitM, replay, and interception attacks
Protocol Overhead	Evaluates the impact of encryption on network performance

3.7 Ethical Considerations

The study was based only on available published academic literature, international standards and technical reports. No human data, no confidential organizational data, and no personal information have been utilized. All cited materials should be acknowledged in accordance with **APA 7th edition** to ensure academic integrity and avoid plagiarism.

3.8 Justification of Method

The methodology juxtaposes a systematic review of the literature together with a conceptual framework to assess the impact of encypte protocol on securing network communications system. The framework can be implemented by incorporating present day cryptography algorithms, public key infrastructure, secure communication protocols, multifactor & far authentication and continuous monitoring to address confidentiality integrity & resilience issues

Results and Discussion

4.1 Results

Based on the reviewed literature, most secure network communication systems rely on encryption protocols. The analysis demonstrates that organizations deploying robust cryptographic algorithms in combination with standardized communication protocols are at a dramatically reduced risk of unauthorized access, data interception, identity theft, and cyber espionage than those employing outdated or weak encryption methods.

The review shows that Advanced Encryption Standard (AES-256) is still the predominant symmetric algorithm due to excellent computational efficiency, and resilience against brute-force attacks. Elliptic Curve Cryptography (ECC) keeps be replaced RSA in mible and IoT environments more and more for its shorter key sizes offer equivalent security, requiring less computational power and energy. In a similar vein, Transport Layer Security (TLS 1.3), the most widely used protocol securing Internet communications by guaranteeing confidentiality, integrity, and authentication of transmitted data has made its way into many application protocols. Internet Protocol Security, the technology that is used for a Virtual private networks (VPNs), has not been completely phased out in favor of newer protocol, while Secure Shell is still widely used to securely administer servers and networking devices over a network.

Table 4.1 Major Encryption Protocols and Their Security Functions

Encryption Protocol/Algorithm	Primary Application	Security Benefit
AES-256	Data encryption	High confidentiality and processing speed
RSA	Secure key exchange	Authentication and digital signatures
Elliptic Curve Cryptography (ECC)	Mobile and IoT security	Strong security with shorter keys
TLS 1.3	HTTPS and web communication	Confidentiality, integrity, authentication
IPSec	VPN communication	Secure IP packet transmission
SSH	Remote system administration	Secure remote access
End-to-End Encryption (E2EE)	Messaging and collaboration	Protects messages from interception
SHA-256	Integrity verification	Detects unauthorized modification

The reviewed studies further demonstrate that synergy of encryption protocols with Public Key Infrastructure (PKI), Multi-Factor Authentication (MFA) and Zero Trust Architecture (ZTA) offers far superior protection than deploying encryption in isolation.

4.2 Discussion

The results validate that encryption is essential to safeguard modern-day network communication systems. With the world being more reliant on cloud computing, electronic commerce, online banking, remote work and IoT devices than ever before, encrypted communication has never been such a necessity to maintain confidentiality.

In terms of data encryption methods, the most important thing that you should keep in mind is that there is no perfect algorithm. Symmetric algorithms like AES perform very well on bulk data encryption while asymmetric algorithms like RSA and ECC allow for key exchanges and digital signatures. As a result, new communication protocols use both methods in the right proportion for maximal security and efficiency.

Conclusion

Encryption protocols are still one of the best ways to secure network communication systems from cyber threats. This work shows that modern cryptographic algorithms and secure communication protocols greatly enhance the confidentiality, integrity, authentication and non-repudiation of information transmitted. AES RSA ECC TLS IPsec SSH VPNs End-to-end tanidıkları szher step. With Public Key Infrastructure, Multi-Factor Authentication, Zero Trust Architecture and continuous security monitoring they work even more effective. Nevertheless, the explorations are far from being over due to several emerging threats such as key management weak points, erroneous implementations and running overhead when employing these solutions, not to mention quantum computing- which although still years away will have a significant influence on current protocols. Thus, organizations should implement adaptive standards-based encryption measures and prepare for migration to post-quantum cryptography.

6. Recommendations

In the light of findings from this research, the study recommended that organizations should implement AES-256 as the replacement symmetric encryption mechanism default for protecting sensitive information. The use of TLS 1.3, IPsec and SSH was also recommended in order to secure Internet and remote administration as well as enterprise communications with them. Organizations should implement a Public Key Infrastructure (PKI) to replace passwords and enforce two-factor, public key authentication; digital certificates; and cryptographic key management. It was further recommended that Multi-Factor Authentication should be used. It should not be able to rely only on encryption that tries to reduce unauthorized access and credential-based attacks. Lastly, the study recommends that organizations should enforce Zero Trust Architecture (Continuous Verifications of User/Device/App) – Organizations should enforce a zero trust architecture by making sure that all users, devices and applications are continuously authenticated.

References

- Barker, E., & Roginsky, A. (2020). *Recommendation for cryptographic key generation* (NIST Special Publication 800-133 Rev. 2). National Institute of Standards and Technology.
- Bernstein, D. J. (2008). ChaCha, a variant of Salsa20. *Workshop Record of SASC 2008*, 3, 1–22.
- Cisco Systems. (2023). *Enterprise encryption best practices and secure network communications*. Cisco Systems.
- Dierks, T., & Rescorla, E. (2008). *The Transport Layer Security (TLS) Protocol Version 1.2 (RFC 5246)*. Internet Engineering Task Force.
- Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.
- Eastlake, D., & Jones, P. (2011). *US Secure Hash Algorithm 1 (SHA1), SHA-224, SHA-256, SHA-384, and SHA-512*. Internet Engineering Task Force.
- International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.
- Katz, J., & Lindell, Y. (2021). *Introduction to modern cryptography* (3rd ed.). CRC Press.
- Kent, S., & Seo, K. (2005). *Security architecture for the Internet Protocol (RFC 4301)*. Internet Engineering Task Force.
- Krawczyk, H., Paterson, K., & Wee, H. (2019). On the security of the TLS 1.3 handshake protocol. *Proceedings of the IEEE Symposium on Security and Privacy*, 646–663.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC Press.
- National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2023). *Post-quantum cryptography: Selected algorithms*. U.S. Department of Commerce.
- NIST. (2001). *Advanced Encryption Standard (AES) (FIPS PUB 197)*. National Institute of Standards and Technology.
- Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446)*. Internet Engineering Task Force.
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
- Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (20th anniversary ed.). Wiley.

Review of the Role of Encryption Protocols in Protecting Network Communication Systems.

Stallings, W. (2022). *Cryptography and network security: Principles and practice* (9th ed.). Pearson.

Stallings, W. (2022). *Network security essentials: Applications and standards* (7th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.