Available Online: 10 November 2026 DOI: 10.54254/2977-3903/2026.38941

# Application of symmetric encryption in internet data security: a review of AES technology

***Lechen Zhang***

York School, Monterey, USA

rose0211hk@gmail.com

**Abstract.** Internet services are deeply embedded in financial transactions, medical records, government administration, and personal communications, making data protection a core security concern. Since its adoption by the National Institute of Standards and Technology (NIST) in 2001, the Advanced Encryption Standard (AES) has remained one of the most widely used symmetric cryptographic standards. This paper reviews AES deployment across four major Internet sectors: network communication security, online payments and e-commerce, social media and instant messaging, and cloud storage and data protection. The study employs a literature review combined with case studies, drawing on NIST and Internet Engineering Task Force (IETF) standards, peer-reviewed literature published between 2020 and 2026, and industry incident reports. The review finds that no practical attacks have been demonstrated against the full AES algorithm at its specified security levels, while AES generally provides its higher computational efficiency than public-key algorithms for bulk data encryption. Documented security incidents are more often associated with key-management failures, configuration errors, and implementation-level vulnerabilities than with weaknesses in AES itself. Regarding quantum computing, the threat posed by Grover's algorithm to AES-256 is generally considered less immediate than the threat posed by Shor's algorithm to current public-key systems. This review highlights the importance of security engineering and clarifies the continuing role of AES during the transition to post-quantum cryptography.

**Keywords:** Advanced Encryption Standard (AES), Internet data security, symmetric encryption, key management, post-quantum cryptography

## 1. Introduction

The economic cost of data breaches has become quite substantial. According to IBM's Cost of a Data Breach Report 2025, the average cost of a single data breach worldwide is $4.44 million, while the average cost for U.S. companies has risen to a record high of $10.22 million; the average time from detection to containment of a breach is 241 days [1]. Among the available technical controls, encryption has always served as the first line of defense against such risks, and in the field of symmetric cryptography, AES holds a near-monopoly position. Existing research on AES can be broadly divided into two categories. The first category focuses on the mathematical structure of the algorithm itself and its resistance to cryptanalysis; recent studies have provided a relatively comprehensive overview of its Substitution-Permutation Network (SPN) design and the

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

mathematical foundations of Galois fields [2]. The second category examines AES's performance in specific deployment scenarios, such as hardware accelerator architecture design or hybrid encryption frameworks for cloud storage [3, 4]. However, research capable of integrating these two levels while simultaneously examining AES's actual role across multiple Internet application domains remains relatively scarce; following the release of the first batch of NIST post-quantum standards in August 2024, studies that discuss this cross-scenario landscape within the context of post-quantum migration are even rarer [5].

This paper addresses the aforementioned gaps by proposing three research questions: where AES is currently deployed in Internet applications and what functions it performs; what the main limitations of AES-based security systems are; and how the role of AES may evolve as post-quantum cryptography enters production environments. Methodologically, the study combines a literature review and case analysis, drawing on NIST and IETF standards, peer-reviewed studies published primarily between 2020 and 2026, and documented security incidents. The findings aim to help practitioners prioritize security investments and identify the interaction between symmetric cryptographic primitives and post-quantum key establishment mechanisms as a direction for future research.

## 2. Overview of AES

### 2.1. Fundamentals of symmetric encryption

Symmetric encryption uses the same shared key for both encryption and decryption. This design offers significant efficiency advantages over asymmetric cryptography, but it also introduces the problem of key distribution: the communicating parties must first agree on a secret before secure communication can begin. Modern Internet protocols resolve this tension through a hybrid encryption architecture, in which asymmetric cryptography is responsible for establishing the session key, while symmetric cryptography handles the encryption of bulk data. Empirical data confirms the validity of this division of labor. In comparative tests across AWS, Azure, and Alibaba Cloud, RSA-4096 showed substantially higher computational overhead than AES, illustrating asymmetric cryptography is generally used for key establishment rather than bulk data encryption, while AES-256 provided a favorable balance between performance and security [6].

### 2.2. Evolution from DES to AES

The Data Encryption Standard (DES) was adopted in 1977, but its 56-bit key length gradually lost its protective value as computing power increased; by the late 1990s, dedicated hardware had demonstrated practical brute-force recovery of DES keys. Although Triple DES extended the effective key length, it came at a significant performance cost. In response, NIST launched a public international competition in 1997. This process was renowned for its transparency: candidate algorithms had to undergo public cryptanalysis at consecutive academic conferences over a period of several years before advancing to the final selection [7]. Rijndael, designed by Daemen and Rijmen, was selected by NIST in 2000 based on criteria including security, efficiency, and implementation flexibility [2]. The algorithm was standardized as FIPS 197 in 2001 [8].

### 2.3. Basic working principles of AES

AES operates on 128-bit blocks arranged as a 4×4 state matrix of bytes, filled column by column. Three key lengths are specified—128, 192, and 256 bits—corresponding to 10, 12, and 14 rounds, respectively [8].

Processing begins with an initial AddRoundKey operation that combines the plaintext state with the cypher key. Each subsequent round applies four transformations. SubBytes performs non-linear byte substitution

through a fixed S-box, providing confusion. ShiftRows cyclically shifts the rows of the state, while MixColumns transforms each column using operations over a Galois field.

Together, ShiftRows and MixColumns provide diffusion by spreading changes across the state over successive rounds. AddRoundKey then combines the state with a round key derived through the key schedule, which uses word rotation, S-box substitution, and round constants [2].

The final round omits MixColumns. Decryption uses the corresponding inverse transformations and applies the round keys in reverse order.

### 2.4. Key features of AES

The security of AES in practice depends heavily on the mode of operation. The Electronic Codebook (ECB) mode is not suitable for general-purpose use because independent block encryption can reveal plaintext patterns. Cipher Block Chaining (CBC) mode provides confidentiality but does not provide authentication or integrity protection on its own. Modern Internet protocols therefore commonly favor authenticated encryption modes such as GCM, which combines encryption and authentication and supports efficient parallel processing [9]. Hardware acceleration has further solidified AES's status as a standard—dedicated instruction sets built into modern processors, along with high-throughput hardware architectures designed for AES-GCM, have substantially reduced the computational overhead of AES, particularly on modern processors that provided dedicated cryptographic instructions [3].

## 3. Applications of AES in the internet

### 3.1. Secure network communication

The Transport Layer Security (TLS) protocol protects the vast majority of web traffic. TLS 1.3, as specified in RFC 8446, removed legacy and insufficiently secure cipher suites and retained a small set of authenticated encryption options, including AES-GCM and AES-CCM [10]. AES thus remains one of the principal symmetric encryption algorithms used to protect HTTPS traffic. The same pattern is observed in wireless networks and IPsec-based Virtual Private Networks (VPNs): AES carries the payload in authentication mode, while key exchange is handled by a separate mechanism.

### 3.2. Online payment and e-commerce

Payment infrastructure is perhaps the most heavily regulated area of AES application. The Payment Card Industry Security Standards Council requires strong cryptography to protect cardholder data in relevant circumstances, and AES is widely used to meet these encryption requirements [2]. In practice, payment systems combine AES encryption with Hardware Security Modules (HSMs), which isolate key material from application code; tokenization can further reduce the exposure of primary account numbers by replacing them with token values in downstream systems. This layered approach itself reflects the recognition that cryptographic algorithms alone are insufficient.

### 3.3. Social media and instant messaging

The Signal protocol has brought End-to-End Encryption (E2EE) to billions of users, and apps such as WhatsApp, Facebook Messenger, and Wire have all adopted it [9]. Within the Signal protocol, message encryption is performed using AES-256 in CBC mode with PKCS#5 padding, while authentication is provided by HMAC-SHA256 [11]. The Double Ratchet mechanism derives a new message key for each message,

thereby achieving forward secrecy and post-compromise security. The significance of this case lies in its scale: this deployment demonstrates that AES-based end-to-end encryption can be compatible with usability requirements on billions of consumer devices—a claim that very few cryptographic constructs can support.

### 3.4. Cloud storage and data protection

Major cloud service providers widely support AES-256 encryption to static data by default and generally adopt an envelope encryption architecture: the data itself is protected by a data encryption key, which is in turn protected by a master key stored in a managed key service. The Key Management Systems (KMS) of AWS and Alibaba Cloud have implemented full lifecycle key management, while Transparent Data Encryption (TDE) extends automatic protection to database files and logs [6]. The academic community has also explored hybrid frameworks that integrate AES with adaptive key management and time-limited access controls to address the residual risks of this model [4]; broader review studies have separately mapped out the overall landscape of cloud storage protection mechanisms and the current state of cross-domain identity and access management [12, 13].

### 3.5. Cross-domain comparison

Viewed across these four domains, a consistent structural pattern emerges alongside meaningful differences in how AES is deployed.

In terms of mode selection, three of the four domains have converged on authenticated encryption. Network communication and many payment applications commonly use AES-GCM, while cloud storage primarily employs AES-256 in authenticated modes for data at rest. Instant messaging represents the exception: the Signal Protocol pairs AES-256 in CBC mode with a separate HMAC-SHA256 authentication step, an arrangement that achieves the same security goal through composition rather than through a single integrated mode [11].

The four domains diverge more sharply in key management, and this divergence is the more consequential one. In network communication, session keys are negotiated during the handshake and remain valid only for the duration of a single connection, so exposure is inherently time-bounded. Payment systems take the opposite approach, protecting long-lived keys within hardware security modules so that key material never crosses the boundary into application memory. Messaging protocols derive a fresh key for every individual message through the ratchet mechanism, minimizing the value of any single compromised key. Cloud storage relies on managed key services that hold master keys and perform full lifecycle management on the customer's behalf, concentrating trust in the provider's key infrastructure [6].

These differences in key management in turn determine where each domain's principal vulnerability lies. For network communication, the exposure is protocol-level—downgrade attempts and failures in the certificate trust chain. For payments, it is compliance and configuration: the encryption itself is mandated and audited, but plaintext data may still be exposed in downstream systems outside the protected boundary. For messaging, the residual risk shifts to the endpoint, since end-to-end encryption offers no protection once a device is compromised or the key verification step is bypassed by the user. For cloud storage, the dominant risk is over-broad access policy and master key permission scope [13]. What unites these four otherwise dissimilar cases is that the major practical risks identified in the literature generally arise from implementation, configuration, key management, access control, or endpoint security rather than from a practical break of AES itself. The issue is discussed further in Section 4.

# 4. Advantages and limitations of AES

Three characteristics collectively explain the enduring vitality of AES. The first is performance. Empirical data indicates that AES-256 provides a favorable balance between speed and security in the tested environments, making it suitable for real-time business scenarios where other solutions fall short [6]. The second is its resilience against cryptanalysis: for more than two decades, an international research community with strong incentives for success has conducted ongoing public analysis, yet no publicly known attack on full-round AES has been demonstrated to have practical consequences under realistic attack conditions. The third is the degree of standardization. Because AES is defined by a single authoritative document and is consistently implemented across various cryptographic libraries, operating systems, and chips, interoperability is effectively guaranteed—a feature that significantly reduces the design costs of security systems [8].

Many practical limitations of AES-based security arise from the surrounding systems in which the algorithm operates rather than the algorithm itself. Key management issues. AES does not—and is not intended to—address the distribution, rotation, and storage of keys. Once the key material is compromised, the encrypted data is completely compromised, and the encryption measures become ineffective [6]. This is the primary failure mode in the real world.

Implementation and configuration errors. The 2019 Capital One breach illustrates how cloud configuration and access-control weakness can undermine otherwise strong cryptographic protection. The incident affected the personal information of over 100 million customers in the United States and Canada [6, 14]. A systematic analysis of this incident identified organizational management and configuration errors—rather than cryptographic weaknesses—as the direct cause [14]. Industry data further corroborates this pattern: reports indicate that more than 60% of cloud data breaches stem from improper cloud service configuration [6].

Side-channel attacks. Even mathematically sound cryptographic algorithms can be compromised if their physical execution process is observed. Power analysis and timing leaks can undermine robust cryptographic algorithms when implementation flaws are present [2]. This threat is particularly prominent in embedded and Internet of Things (IoT) scenarios and has spurred extensive research into countermeasures, including S-box design and masking techniques, as well as practical attack demonstrations targeting processor cores that integrate AES instructions [15, 16].

The Impact of Quantum Computing. The Grover algorithm provides a quadratic speedup for exhaustive key search, effectively halving the security strength of symmetric-key cryptography. However, specific resource estimates mitigate the urgency of this warning: existing research estimates that attacking AES-256 would require a circuit of approximately 6,681 qubits, with a time complexity of about $2^{151}$ operations [17]; subsequent optimizations of the oracle construction have not altered this fundamental conclusion [18]. The Grover algorithm is also highly inefficient when parallelized, further diminishing its real-world threat. AES-256 therefore retains approximately 128 bits of post-quantum security strength—a situation that differs fundamentally from that faced by RSA and Elliptic Curve Cryptography (ECC).

# 5. Future development of AES

## 5.1. Integration with other cryptographic technologies

On August 13, 2024, the publication of FIPS 203, 204, and 205 marked the conclusion of an eight-year standardization process, thereby initiating the transition period [5]. It is necessary to precisely define what this transition entails: post-quantum standards replace the key encapsulation mechanism and the digital signature mechanism—that is, the asymmetric layer; the symmetric layer remains unchanged. Hybrid key-establishment

schemes can combine a classical elliptic-curve mechanism with ML-KEM, while the resulting session key can still be used by AES-256 for bulk data encryption. Performance data supports this division of labor: measured encryption time for ML-KEM is approximately 2.7 times that of AES-256, and key management complexity is correspondingly higher, confirming that lattice-based algorithms should still be positioned for key establishment rather than bulk data protection [6].

### 5.2. Challenges in the post-quantum era

Two challenges warrant attention. The first is throughput: post-quantum algorithms currently impose a significant overhead in high-throughput cloud environments, and existing hardware architectures require optimization to support them efficiently [6]. The second concerns resource-constrained devices, where AES-GCM itself may prove too resource-intensive. In response, NIST selected the Ascon algorithm family in February 2023 and published SP 800-232 in August 2025, which specifies lightweight authenticated encryption, hashing, and scalar hash functions for IoT devices, embedded systems, and low-power sensors [19]. Ascon does not replace AES but rather complements it at the resource-constrained end of the deployment spectrum.

### 5.3. Future prospects for data security

A broader perspective points toward a layered architecture, in which encryption is just one of many components. Empirical evaluations across multiple cloud platforms show that the attack interception rate when relying solely on encryption and basic access controls is 68.3%; however, when combined with Attribute-Based Access Control (ABAC), Intrusion Detection Systems (IDS), zero trust, and threat intelligence federation, the full-stack solution achieved an interception rate of 99.2%, at the cost of approximately 30% additional computational overhead [6]. Encryption is always necessary, but it is never sufficient on its own.

## 6. Conclusion

This paper examines AES applications in Internet data security, focusing on its technical foundations, deployment across four major application areas, advantages and limitations, and future role in the post-quantum era. Three conclusions emerge. First, AES remains a widely adopted standard for symmetric encryption, supporting TLS-protected web traffic, end-to-end encrypted communications, payment infrastructure, and cloud data storage. Second, security risks often arise not from weaknesses in the AES algorithm itself but from key management failures, configuration errors, and implementation-level side-channel attacks. The Capital One incident illustrates how configuration errors can expose sensitive data despite the use of encryption. Therefore, effective key lifecycle management and secure configuration are essential to protecting encrypted data. Third, although quantum computing poses long-term challenges to cryptography, AES-256 is expected to remain useful in post-quantum security architectures, while key establishment and digital signature mechanisms require substantial transition efforts.

This study has limitations. It relies on published literature and documented cases rather than independent performance measurements, focuses mainly on consumer-facing Internet services, and provides only an overview of side-channel attacks. Future research could evaluate the performance overhead of hybrid post-quantum key exchange in production TLS environments, compare AES and Ascon on resource-constrained devices, and investigate recurring organizational failures in key management. These directions may help improve practical security and guide cryptographic deployment decisions.

## References


[1] IBM Security & Ponemon Institute. (2025). *Cost of a data breach report 2025*. IBM Corporation.

[2] Ganesh, R., Khan, B. U. I., Khan, A. R., & Kamsin, A. (2025). A panoramic survey of the advanced encryption standard: From architecture to security analysis, key management, real-world applications, and post-quantum challenges. *International Journal of Information Security, 24*(5), Article 216. https://doi.org/10.1007/s10207-025-01116-x

[3] Lin, M.-B., & Chuang, J.-H. (2024). The design of a high-throughput hardware architecture for the AES-GCM algorithm. *IEEE Transactions on Consumer Electronics, 70*(1), 425–432. https://doi.org/10.1109/TCE.2023.3332872

[4] Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control. *Alexandria Engineering Journal, 84*, 275–284. https://doi.org/10.1016/j.aej.2023.10.054

[5] National Institute of Standards and Technology. (2024). *FIPS 203: Module-lattice-based key-encapsulation mechanism standard.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

[6] Hao, H. (2026). Data security strategies and technologies for robust cloud computing. *Discover Applied Sciences, 8*, Article 91. https://doi.org/10.1007/s42452-025-08091-x

[7] Smid, M. E. (2021). Development of the Advanced Encryption Standard. *Journal of Research of the National Institute of Standards and Technology, 126*, Article 126024. https://doi.org/10.6028/jres.126.024

[8] National Institute of Standards and Technology. (2001). FIPS PUB 197: Advanced Encryption Standard (AES). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.197-upd1

[9] Dworkin, M. (2007). NIST SP 800-38D: Recommendation for block cipher modes of operation—Galois/Counter Mode (GCM) and GMAC. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-38D

[10] Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3* (RFC 8446). Internet Engineering Task Force. https://doi.org/10.17487/RFC8446

[11] Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. (2020). A formal security analysis of the Signal messaging protocol. *Journal of Cryptology, 33*(4), 1914–1983. https://doi.org/10.1007/s00145-020-09360-1

[12] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access, 8*, 131723–131740. https://doi.org/10.1109/ACCESS.2020.3009876

[13] Badirova, A., Dabbaghi, S., Moghaddam, F. F., Wieder, P., & Yahyapour, R. (2023). A survey on identity and access management for cross-domain dynamic users: Issues, solutions, and challenges. *IEEE Access, 11*, 61660–61679. https://doi.org/10.1109/ACCESS.2023.3279492

[14] Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the Capital One data breach: Critical lessons learned. *ACM Transactions on Privacy and Security, 26*(1), 1–29. https://doi.org/10.1145/3546068

[15] Singha, T. B., Palathinkal, R. P., & Ahamed, S. R. (2023). Securing AES designs against power analysis attacks: A survey. *IEEE Internet of Things Journal, 10*(16), 14332–14356. https://doi.org/10.1109/JIOT.2023.3265683

[16] Ignatius, T. M., Singha, T. B., & Palathinkal, R. P. (2024). Power side-channel attacks on crypto-core based on RISC-V ISA for high-security applications. *IEEE Access, 12*, 150230–150248. https://doi.org/10.1109/ACCESS.2024.3477961

[17] Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In *Post-Quantum Cryptography (PQCrypto 2016) (LNCS Vol. 9606)* (pp. 29–43). Springer. https://doi.org/10.1007/978-3-319-29360-8_3

[18] Jaques, S., Naehrig, M., Roetteler, M., & Virdia, F. (2020). Implementing Grover oracles for quantum key search on AES and LowMC. In *Advances in Cryptology—EUROCRYPT 2020 (LNCS Vol. 12106)* (pp. 280–310). Springer. https://doi.org/10.1007/978-3-030-45724-2_10

[19] Turan, M. S., McKay, K. A., Chang, D., Kang, J., & Kelsey, J. (2025). *NIST SP 800-232: Ascon-based lightweight cryptography standards for constrained devices*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-232