AES-GCM Algorithm Implementation for the Protection of Online Shoppers Data in E-Commerce

Amruta J. Thakur; R. N. Jugele
Department of Computer Science Shivaji Science College, Nagpur

Abstract:
Cryptography embodies a sophisticated methodology that utilizes encryption and decryption techniques to safeguard sensitive information during online transactions. It serves as a fundamental cornerstone of secure e-commerce, effectively shielding customers' data from the malevolent designs of cyber criminals. Galois/Counter Mode (GCM) is a mode of operation for symmetric-key cryptography block ciphers, widely acclaimed for its exceptional performance. AES-GCM distinguishes itself as a prevalent cryptography algorithm specifically engineered for Authenticated Encryption with Associated Data (AEAD), ensuring both data confidentiality and integrity. This paper elucidates a Java implementation of AES-GCM (Galois/Counter Mode), meticulously crafted to protect sensitive data in online shopping, particularly concerning the safeguarding of credit card information during transmission or storage. This implementation exemplifies the process of encrypting customer data prior to its transmission to a server, followed by subsequent decryption on the server side. Such an implementation guarantees robust security for online shopping transactions.

Key words:
AES, GCM, cryptography, encryption, decryption, symmetric key

I.Introduction

Security constitutes a paramount concern in the realms of data management, communication, message transmission, and electronic transactions conducted over public networks. Cryptography represents the intricate process of transforming messages to safeguard information, rendering it secure and resilient against potential threats. The Advanced Encryption Standard (AES) is a symmetric encryption protocol endorsed by the National Institute of Standards and Technology (NIST). AES accommodates a data length of 128 bits, equivalent to 16 bytes, and supports key lengths of 128 bits, 192 bits, and 256 bits. The AES algorithm undergoes ten rounds for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys. The 128-bit data length is partitioned into four operational blocks and is treated as an array of bytes, organized into a 4x4 matrix referred to as the "state." AES-GCM (Advanced Encryption Standard - Galois/Counter Mode) is a widely adopted encryption algorithm that ensures both confidentiality and data integrity. It serves as a mode of operation for the AES block cipher and enjoys particular popularity in applications necessitating secure and efficient encryption, such as Transport Layer Security (TLS) utilized in HTTPS, Virtual Private Networks (VPNs), and secure data storage.

II.The Galois/CounterMode (GCM):

GCM ensures the confidentiality of data through a sophisticated variation of the Counter mode of operation for encryption. It also guarantees the authenticity of the confidential data (up to approximately 64 gigabytes per invocation) utilizing a universal hash function defined over a binary Galois (finite) field. Furthermore, GCM can offer authentication assurance for additional data (of virtually unlimited length per invocation) that remains not encrypted. When the GCM input is confined to data that is not intended for encryption, the resulting specialization, known as GMAC, serves solely as an authentication mode for the input data. Throughout this document, references to GCM equally pertain to GMAC. GCM provides a more robust authentication assurance than a mere (non-cryptographic) checksum or error-detecting code.

Specifically, GCM can identify both accidental alterations of the data and deliberate, unauthorized modifications. The dual functions of GCM are termed authenticated encryption and authenticated decryption. Each of these functions is characterized by relative efficiency and embarrassingly parallel, thusenablinghigh-throughputimplementationsin both hardware and software.

DOI: https://doi.org/10.5281/zenodo.18290731

GCM possesses several additional beneficial attributes, including the following:

- The GCM functions are "online" in that the lengths of the non-confidential and confidential data are computed as the data is received and processed, rather than needing to be known beforehand.
- The inverse direction of the underlying block cipher is not necessary for the GCM functions to function; only the forward direction needed. The authenticity of the protected data can be verified independently from the recovery of the confidential data from its encrypted form.
- If the unique initialization string is predictable and the length of the confidential data is known, then the block cipher invocations within the GCM encryption mechanism can be pre-computed.

If some or all of the additional, non- confidential data is fixed, then the corresponding elements of the

- GCM authentication mechanism can be pre-computed.

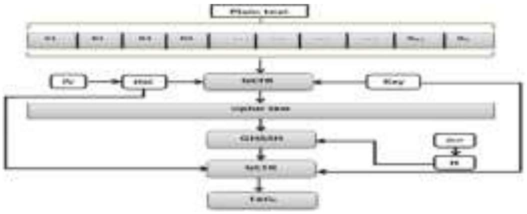


Figure 1: Galois/Counter Mode GCM

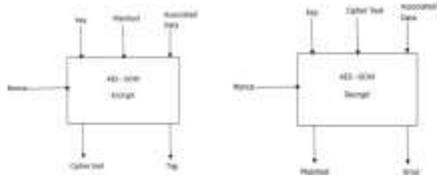
The overall architecture of Galois/Counter Mode (GCM), as illustrated in Figure 1, reveals that the output cipher text generated by GCTR is concatenated prior to being transmitted to the GHASH function. Although GCTR inherently supports parallel processing, the aggregation of all cipher text before its input to the GHASH function diminishes performance [11]. The Galois/Counter Mode (GCM) of operation has been formalized by NIST to facilitate single-pass authenticated encryption. The GHASH authentication component of GCM is categorized within the realm of Wegman-Carter polynomial universal hashes, functioning within the finite field GF(2^128).

III.AES-GCM:

AES-GCM, which denotes Advanced Encryption Standard coupled with Galois Counter Mode, is a symmetric cryptographic algorithm that synthesizes the Advanced

Encryption Standard (AES) with the Galois/Counter Mode (GCM) [2]. This algorithm is widely utilized for Authenticated Encryption with Associated Data (AEAD) applications, as it proficiently guarantees both data confidentiality and authenticity [4].

The remarkably high-performance AES-GCM IP core is available and possesses the capability to process messages without incurring additional message-specific latencies, thereby ensuring an uninterrupted processing flow. All IP cores are meticulously designed for seamless integration into FPGA and ASIC architectures, adhering to a vendor-neutral design philosophy, with their functionality remaining independent of any manufacturer-specific FPGA attributes [3].



IV.AES-GCM Parameters:

Key size 128 bits, 192 bits, or 256 bits (with AES-256 being the most secure alternative) delineates the parameters of the specifications. For optimal security, it is advisable to employ an initialization vector (IV) of 12 bytes (96 bits). To ensure formidable integrity, the authentication tag is conventionally 16 bytes (128 bits). Additional data may be incorporated at discretion; this data, which is authenticated but not encrypted, is referred to as Additional Authenticated Data (AAD) [8].

The operational mechanics of AES-GCM are as follows:

- Initialization: Employs a key alongside a unique initialization vector (IV). The IV is conventionally 12 bytes (96 bits) in length and must be distinctive for each encryption operation [1].
- Encryption: Transforms plaintext into cipher text utilizing the Advanced Encryption Standard (AES) in counter mode (CTR).
- Authentication: Produces an authentication tag through Galois field multiplication of the cipher text and additional authenticated data (AAD). This tag serves to ensure both data integrity and authenticity.
- Decryption: Reverts the cipher text back to

DOI: https://doi.org/10.5281/zenodo.18290731

- plaintext using the identical key and IV, while concurrently validating the authentication tag to confirm integrity [5].

Figure 2: Encryption and decryption with AES GCM

There are four fundamental components integral to authenticated encryption: the secret key, the initialization vector (IV) — often referred to as a nonce† — the plain text itself, and optional additional authentication data (AAD) [6]. The nonce and AAD are transmitted in plain text. The process yields two outputs: the cipher text, which maintains the same length as the plain text, and an authentication tag, commonly known as the "tag." This tag may also be designated as the message authentication code (MAC) or integrity check value (ICV).A nonce, an abbreviation for "Number Once," is a value that is intended for singular use within a cryptographic communication context. In the AES-GCM encryption scheme, the nonce serves as a pivotal element in safeguarding the integrity of the encryption process.

V.Role of Nonce in AES-GCM:

In AES-GCM, the nonce functions as an initialization vector for the counter mode of AES encryption. It imparts the essential randomness required to ensure that identical plaintexts yield distinct cipher texts, contingent upon the nonce, even when encrypted with the same key. Notably, a nonce must never be reused in conjunction with the same encryption key; such an action would severely undermine the integrity and confidentiality of the encrypted data.

Nonce and Cipher Text: When transmitting encrypted data, the nonce is generally not regarded as sensitive;
however, it is indispensable for the decryption process. The nonce must be known by the recipient and should never be reused. It is customary to convey the nonce alongside the cipher text. Nevertheless, there are significant considerations to bear in mind when doing so:

- Appending to Cipher Text: One may append the nonce to the cipher text prior to transmission. This approach is frequently adopted for the sake of simplicity.

- Prepending to Cipher Text: Conversely, the nonce can be prepended to the cipher text. This method is prevalent and facilitates the extraction of the nonce at the receiving end.

VI.Security Considerations:

1)Attacker Knowledge:

If an adversary is aware that the initial 12 bytes represent the nonce, does it hold significance? Generally, no, as the nonce is not intended to be confidential. Its primary function is to confer uniqueness upon the cipher text.

2)Integrity:

Although the nonce is not secretive in nature, it must be transmitted with utmost reliability. Any modification to the nonce will render decryption unattainable or, even more critically, may jeopardize the integrity of the data.

3)Nonce Reuse:

The most paramount consideration is to unequivocally avoid the reuse of a nonce with the same key. The recurrence of a nonce can precipitate vulnerabilities such as the "forbidden attack," which can ultimately undermine the encryption.

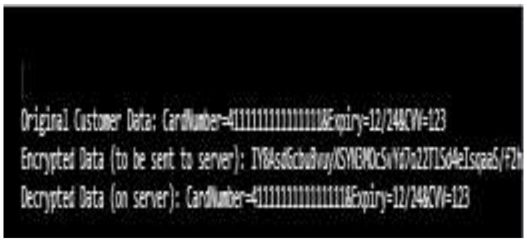
The 12-byte nonce of AES-GCM must be unique and, therefore, must never be repeated [7].
It is noteworthy that it does not necessarily need to be random; consequently, some practitioners prefer to utilize it as a counter, initiating it at 1 and incrementing
it for each subsequent encryption. In this scenario, it is imperative to employ a cryptographic library that permits the user to specify the nonce. This approach enables the encryption of up to 2^112 - 1 messages before reaching the nonce's maximum value.
The nonce prevents attackers from reusing previously intercepted ciphertexts to decrypt new messages or modify existing ones.
A nonce must be unique for every encryption performed with a given key.

VII.mplementationofAES-GCM (Galois/Counter Mode):

This document delineates a Java implementation of AES-GCM (Galois/Counter Mode) meticulously designed to safeguard sensitive information in online transactions, particularly in the protection of credit card details during both transmission and storage. This implementation elucidates the process of

DOI: https://doi.org/10.5281/zenodo.18290731

encrypting customer data prior to its transmission to a server and subsequently decrypting it on the server side [10].



```
Original Customer Data: CardNumber=4111111111111111&Expiry=12/24&CVV=123
Encrypted Data (to be sent to server): IY8AsdGchwBvwyXSYNEMOcSvYd7w22T1Sd4eIsqaa5/F2h
Decrypted Data (on server): CardNumber=4111111111111111&Expiry=12/24&CVV=123
```

Figure 3: Output of Java implementation for Encryption and Decryption in AES GCM

Client-Side

- Encrypts the plaintext CardNumber=4111111111111111&Expiry=12/24&CVV=123.
- Produces an encrypted message (cipher text) and IV.
- Sends the encrypted data to the server.

Server-Side

- Receives the cipher text and IV and decrypts the cipher text using the same secret key and IV.
- Verifies the authentication tag for integrity then retrieves the original plaintext:

CardNumber=4111111111111111&Expiry=12/24&CVV=123.

VIII.Conclusion:

AES-GCM is a widely utilized encryption algorithm that affords both confidentiality and data integrity. Functioning as a mode of operation for the AES block cipher, it is particularly esteemed in applications necessitating secure and efficient encryption, such as TLS (employed in HTTPS), VPNs and secure data storage. The Java implementation presented in this paper illustrates the process of encrypting customer data prior to transmission to a server and subsequently decrypting it on the server side. This implementation guarantees robust security for online shopping transactions.

References:

1.B. -Y. Sung, K. -B. Kim and K. -W. Shin, "An AES-GCM authenticated encryption crypto-core for IoT security," 2018 International Conference on Electronics, Information, and Communication (ICEIC), Honolulu, HI, USA, 2018, pp. 1-3, doi: 10.23919/ELINFOCOM.2018.8330586. Publisher: IEEE

2.Faster and Timing-Attack Resistant AES-GCMhttps://link.springer.com/chapter/10.1007/97 8-3-642-04138-9_1

3.Advanced Encryption Standard with Galois Counter Mode using Field Programmable Gate Array. 1st International Conference on Green and Sustainable Computing (ICoGeS) 2017 IOP Publishing IOP Conf. Series: Journal of Physics: Conf. Series 1019 (2018) 012008 doi :10.1088/1742-6596/1019/1/012008

4.Data Privacy Preservation using Aes-Gcm Encryption in Heroku Cloud, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019

5.F. J. D'souza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 647-652, doi: 10.1109/CCAA.2017.8229881, Publisher: IEEE

6.https://security.stackexchange.com/questions/249557/nonce-in-aes-gcm-aad

7.https://www.latticesemi.com/en/Products/DesignSoftwareAndIP/IntellectualProperty/IPCore/HelionTechCores/AESGCMCore.aspx

8.https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf

9.https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-28/rcr/21-28-change-reference/encrypt-aes-gcm-algorithmn.pdf

10.https://www.npci.org.in/PDF/nach/circular/2024-25/NACH-005-FY-24-25-Implementation-of-AES-Encryption-in-ONMAGS-Application.pdf[11]https://www.researchgate.net/publication/280732944_Analysis_and_optimization_of_GaloisCounter_Mode_GCM_using_MPI#pf2