International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Encryption of Card Details Using AES with a 128-bit Key a Secure Approach to Data Protection

Dipen Limbachia[1]
Student, Department of MSc. IT,
Nagindas Khandwala College,
Mumbai, Maharashtra, India
limbachiadipen5@gmail.com

Dr. Pallavi Devendra Tawde[2]
Assistant professor,
Department of IT and CS,
Nagindas Khandwala College,
Mumbai, Maharashtra, India
pallavi.tawde09@gmail.com

Abstract: Data security is a critical concern in today's digital age, particularly regarding the protection of sensitive information such as cardholder data. This research paper explores the implementation of Advanced Encryption Standard (AES) encryption with a 128-bit key as a means of safeguarding card details. The project demonstrates the encryption and decryption process, ensuring data confidentiality and integrity. Utilizing the pycryptodome library in Python, the AES encryption technique is applied to encrypt card details, offering a secure approach to data protection.

The methodology section outlines the AES encryption process, emphasizing key generation, encryption, and decryption. A detailed explanation of the Python implementation highlights the importance of key length and randomness in the encryption process. The results section presents the outcomes of encrypting and decrypting card details using AES encryption, analyzing the efficiency and security of the encryption process. Additionally, potential vulnerabilities and challenges encountered during implementation are discussed, along with their resolutions.

In the discussion section, the research findings are interpreted in the context of data security and encryption standards. A comparison between AES encryption and other encryption algorithms is provided, evaluating performance and security aspects. Consideration is given to future research directions in the field of data encryption and security.

Overall, this research paper underscores the significance of AES encryption with a 128-bit key for protecting cardholder information. By implementing AES encryption, organizations can enhance data security measures, ensuring the confidentiality and integrity of sensitive data in digital transactions.

This abstract provides a concise overview of the research paper, summarizing the objectives, methodology, results, and implications of implementing AES encryption for card data protection. It highlights the importance of data security and encryption techniques in safeguarding sensitive information in digital transactions.

Tokenizing cards enhances security, ensures regulatory compliance, boosts customer trust, and streamlines payment processes while reducing liability for organizations. Future developments may involve tokenizing cards even without customer consent.

Keywords: Tokenization, Payment systems, Encryption, Fraud prevention

1. Introduction:

In the digital era, the protection of sensitive data has become paramount, with a particular focus on safeguarding cardholder information. The proliferation of online transactions and the storage of financial data necessitate robust security measures to prevent unauthorized access and mitigate the risk of data breaches. Encryption stands as a fundamental tool in the arsenal of data security, offering a means to render plaintext information unintelligible to unauthorized parties.

Among encryption algorithms, the Advanced Encryption Standard (AES) has emerged as a widely adopted and trusted method for securing sensitive data. AES provides a robust and efficient encryption technique, offering various key lengths to accommodate different security requirements. With its adoption by governments and organizations worldwide, AES has become the de facto standard for encrypting data in transit and at rest.

The focus of this research paper is to explore the implementation of AES encryption with a 128-bit key for protecting card details. Cardholder data, including credit card numbers, expiration dates, and security codes, represent highly sensitive information vulnerable to exploitation if not adequately protected. By applying AES encryption, organizations can enhance the security posture of their systems and comply with regulatory standards such as the Payment Card Industry Data Security Standard (PCI DSS).

The objectives of this research paper are twofold: first, to demonstrate the effectiveness of AES encryption in securing cardholder data, and second, to provide insights into the encryption process and its implications for data security practices. Through a Python implementation utilizing the pycryptodome library, we aim to showcase the encryption and decryption process, emphasizing key generation, encryption modes, and best practices in key management.

The remainder of this paper is structured as follows: Section 2 provides background information on encryption techniques, AES encryption, and related research in the field of data security. Section 3 outlines the methodology employed in implementing AES encryption for card data protection, including key generation, encryption, and decryption processes. Section 4 presents the results of encrypting and decrypting card details using AES encryption, along with an analysis of the encryption process's efficiency and security. Section 5 offers a discussion of the research findings, interpreting the results in the context of data security standards and implications for future research. Finally, Section 6 concludes the paper by summarizing the key findings and highlighting the significance of AES encryption for protecting cardholder information in digital transactions.

In summary, this research paper aims to contribute to the body of knowledge on data security by demonstrating the efficacy of AES encryption with a 128-bit key for safeguarding card details. By understanding the encryption process and its implications, organizations can bolster their data security measures, ensuring the confidentiality and integrity of sensitive information in an increasingly interconnected world.

1.1 Tokenization Systems: Requirements and PCI DDS Guidelines

The basic architecture of a tokenization system is described in Fig. 1. In the diagram we show three separate environments: the merchant site, the tokenization system and the card issuer. The basic data objects of interest are the primary account number (PAN), which is basically the credit card number and the token which represents the PAN. A customer communicates with the merchant environment through the "point of sale", where the customer provides its PAN. The merchant sends the PAN to the tokenizer and gets back the corresponding token. The merchant may store the token in its environment. At the request of the merchant the tokenizer can detokenize a token and send the corresponding PAN to the card issuer for payments. We show the tokenization system to be separated from the merchant environment, this is true in most situations today, as the merchants receive the service of tokenization from a third party. But it is also possible that the merchant itself implements its tokenization solution, and in that case, t he tokenization system is a part of the merchant environment.

1.2 As, a tokenization system has the following components:

1. A method for token generation: A process to create a token corresponding to a primary account number (PAN) there is no specific recommendation regarding how this process should be implemented. Some of the mentioned options are encryption functions, cryptographic hash functions and random number generators.

2. A token mapping procedure: It refers to the method used to associate a token with a PAN. Such a method would allow the system to recover a PAN, given a token.

3. Card-Vault: It is a repository which usually will store pairs of PANs and tokens and maybe some other information required for the token mapping. Since it may contain PANs, it must be specially protected according the PCI DSS requirements.

4. Cryptographic Key Management: This module is a set of mechanisms to create, use, manage, store and protect keys used for the protection of PAN data and also data involved in token generation.

The PCI guidelines for tokenization are quite vague (this has been pointed out before in many places including), and it is difficult to make out what properties tokens and tokenization systems should posses for functionality and security. We state two basic requirements for tokens and tokenization systems. We assume that tokenization is provided as a service, thus multiple merchants utilize the same system for their objectives:

Enhanced Security: The primary objective of tokenization is to enhance the security of card transactions. By replacing sensitive card details, such as the primary account number (PAN), with unique tokens, the risk of exposing

valuable card data is significantly reduced. Tokens are useless to attackers if intercepted because they are meaningless outside of the specific payment system.

Protection against Data Breaches: Tokenization helps mitigate the impact of data breaches. Even if a breach occurs and tokenized data is compromised, the stolen tokens cannot be used to conduct fraudulent transactions without the corresponding authentication and validation mechanisms.

Facilitation of Mobile Payments: Tokenization enables the seamless integration of cards into mobile payment systems. Mobile wallets and payment apps utilize tokens to represent card details securely stored on the user's device. This allows consumers to make contactless payments using their smartphones, enhancing convenience and accessibility.

Compliance with Regulations: Tokenization helps organizations comply with industry regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS). By reducing the storage and transmission of sensitive card data, businesses can simplify their compliance efforts and minimize the scope of PCI DSS assessments.

Reduced Fraud and Liability: Tokenization contributes to the reduction of card-present and card-not-present fraud. By substituting sensitive card information with tokens, merchants and payment processors can authenticate transactions more securely, thereby lowering the likelihood of fraudulent activities. Additionally, tokenization can help shift liability away from merchants in the event of fraudulent transactions.

2. Review of Literature:

In 2002, research delved into efficient AES hardware implementations, categorizing optimization methods into architectural and algorithmic approaches. Another study in 2003 analyzed RC4 and AES energy consumption in wireless LANs, favoring AES for smaller packets. In 2010, a proposal surfaced for a compact AES hardware-software co-design tailored for low-cost systems.

In 2013, research showcased FPGA implementations of AES, comparing Basic and Fully Pipelined architectures. Another study utilized VHDL for AES implementation on different FPGA families. Additionally, an efficient FPGA implementation of AES was proposed, featuring an AES en/decryptor design.

Cloud computing enables the sharing of IT resources, services, and data among users over a network. However, this openness can make data vulnerable to unauthorized access during transmission.

To address this, an encryption-based system is proposed to enhance security during data transfer. The system utilizes the Advanced Encryption Standard (AES) to secure data transmission and storage in cloud computing environments. Future work will involve conducting a Systematic Literature Review (SLR) to identify opportunities and suggestions for improving AES in cloud computing.

Current methods for credit card security often fail to ensure confidentiality, privacy, and integrity due to unencrypted data transmission, resulting in unauthorized access. To address this, a new system based on RSA encryption and tokenization is proposed. It includes merchant and tokenization modules interacting with a token vault database hosted on a cloud storage engine. Implementation on a Pentium IV with 2.0 GHz Duo Core Processor and 2 GB of RAM running Windows 7 utilized APACHE server, HTML (Sublime) with CSS JavaScript for frontend, and MySQL database with PHP for backend.

Evaluation with Master, Verve, and Visa cards demonstrated high usability, adaptability, and security superiority in credit card protection, key size, mobile alerting, and tokenization.

PCI DSS certificate is a certification that confirms compliance with the Payment Card Industry Data Security Standard (PCI DSS). It demonstrates that an organization has implemented appropriate security measures to protect credit card data and comply with industry standards.

3. Methodology

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely used to secure data. AES operates on fixed-length blocks of data, typically 128 bits, and supports key lengths of 128, 192, or 256 bits. Here's an overview of the methodology behind AES 128-bit encryption:

Key Expansion: The original key is expanded into a set of round keys.

Initial Round: The plaintext block is combined with the first round key.

Rounds: Multiple rounds of operations (SubBytes, ShiftRows, MixColumns, AddRoundKey)

Final Round: Similar to other rounds but without MixColumns.

Output: The resulting block is the ciphertext, representing the encrypted data.

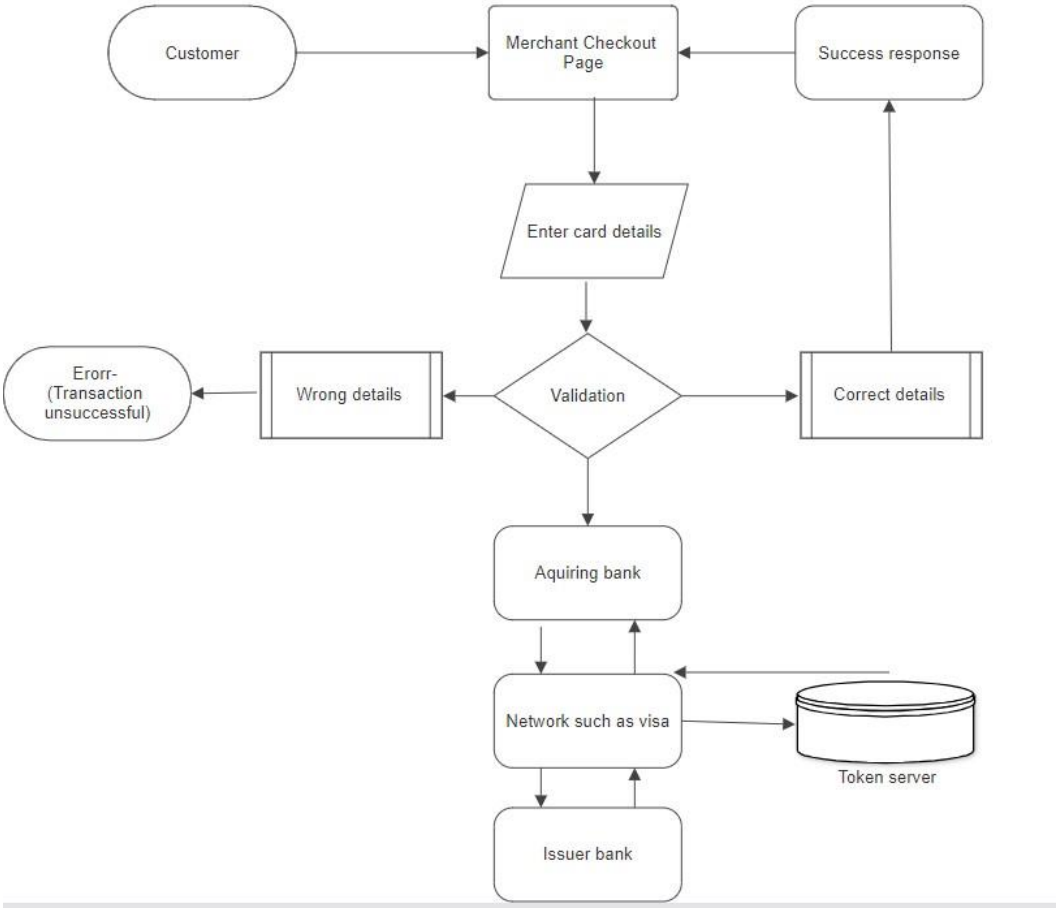

Fig 1: Working of Payment ecosystem for token generation

3.1 Example work flow

A consumer initiates the enrollment of their Visa account with a digital payment service provider, providing necessary account details such as the primary account number (PAN) and security code. The service provider then requests a payment token from Visa for the enrolled account, sometimes involving the issuing bank. Upon approval from the account issuer, Visa replaces the consumer's PAN with the token, which is then shared with the digital payment service provider for online and mobile payment use. Payment tokens may be restricted to specific devices, merchants, or transaction limits.

Tokenization introduces a new participant called a token requestor, responsible for initiating the tokenization process. To obtain tokens from the Visa Token Service, entities must register as token requestors and agree to Visa's participation requirements.

APIs enable issuers to securely provision tokens on devices in collaboration with Visa and wallet providers. This process involves interactions between the token requestor, Visa, and the issuer, covering provisioning, credential management, and notifications.

3.2 Evaluation criteria for choosing algorithm

3.2.1 Security

One of the most crucial aspects that was considered to choose algorithm it is security. The main reasons behind this was obvious because of the main aims of AES was to improve the security issue of DES algorithm. AES has the best ability to protect sensitive data from attackers and is not allowed them to break the encrypt data as compared to other proposed algorithm. This was Cryptography and Network Security 2017 achieved by doing a lot of testing on AES against theoretical and practical attacks.

3.2.2 Cost

Cost Another criterion that was emphasis by NIST to evaluate the algorithms it is cost. Again, the factors behind this measures was also clear due to another main purpose of AES algorithm was to improve the low performance of DES. AES was one of the algorithm which was nominated by NIST because it is able to have high computational efficiency and can be used in a wide range of applications especially in broadband links with a high speed

3.3 Basic Structure AES Algorithm

AES is an iterative instead of Feistel cipher. It is based on two common techniques to encrypt and decrypt data knowns as substitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out in block cipher algorithms [7]. AES has the ability to deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds. The number of rounds is relied on the

Encryption process

Encryption is a popular techniques that plays a major role to protect data from intruders. AES algorithm uses a particular structure to encrypt data to provide the best security. To do that it relies on a number of rounds and inside each round comprise of four sub-process. Each round consists of the following four steps to encrypt 128 bit block

Decryption process

The decryption is the process to obtain the original data that was encrypted. This process is based on the key that was received from the sender Cryptography and Network Security 2017 of the data. The decryption processes of an AES is similar to the encryption process in the reverse order and both sender and receiver have the same key to encrypt and decrypt data. The last round of a decryption stage consists of three stages such as InvShiftRows, InvSubBytes, and AddRoundKey as illustrated in Fig. 8. Fig. 15 Decryption Processes IX. IMPLEMENTATION AREAS AES algorithm is one of the most powerful algorithms that are widely used in different fields all over the

world. This algorithm enables faster than DES and 3DES algorithms to encrypt and decrypt data. Furthermore, it is used in many cryptography protocols such as Socket Security Layer (SSL) and Transport Security Layer protocol to provide much more communications security between client and server over the internet. Before AES algorithm released both of protocols to encrypt and decrypt data relied on DES algorithm but after appearing some vulnerable of this algorithm the Internet Engineering Task Force (IETF) decided to replace DES to AES algorithm. AES can also be found in most modern applications and devices that need encryption functionality such as WhatsApp, Facebook Messenger and Intel and AMD processor and Cisco devices like router, switch, etc. In addition, AES Crypt package is available on many libraries of software programs such as C++ library, C# /.NET.

4. Future Scope

The future outlook for tokenization includes the recent RBI guideline of ALT ID. This initiative allows for the generation of an Alternate ID, known as ALT ID, by the network providers like Visa, Mastercard, Rupay, Diners Club, and others. This ALT ID serves as a unique identifier for each transaction when customers decline consent for storing their card details. It ensures security and privacy while maintaining the integrity of transactions.

5. Conclusion

This paper introduces a system designed to combat fraud in online credit card transactions using AES encryption and tokenization. The system offers advantages such as ensuring transaction non-repudiation and secrecy of card data. Implementation results demonstrate its effectiveness, speed, and applicability, along with high usability, adaptability, and user experience. Comparative analysis with similar systems highlights its superiority in credit card security, key size, mobile alert, and tokenization.

As internet and network usage grows, the exchange of digital data increases, some of which is sensitive and requires protection from unauthorized access. Encryption algorithms, such as the Advanced Encryption Standard (AES), play a crucial role in safeguarding data. AES, with support for key sizes of 128, 192, and 256 bits and a 128-bit block cipher, is widely adopted due to its efficiency. This paper explores key features of AES and reviews previous research to evaluate its performance under various parameters. Research findings demonstrate AES's superior security compared to other algorithms like DES and 3DES.

References

1. Saini, V., Bangar, P., & Chauhan, H. S. (2014). Study and Literature Survey of Advanced Encryption Algorithm for Wireless Application. International, Journal of Emerging Science and Engineering (IJESE) ISSN, 2319-6378.

2. Hidayat, T., & Mahardiko, R. (2020). A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing. International Journal of Artificial Intelligence Research, 4(1), 49-57.

3. Iwasokun, G. B., Omomule, T. G., & Akinyede, R. O. (2018). Encryption and tokenization-based system for credit card information security. Int J Cyber Sec Digital Forensics, 7(3), 283-93.

4. Scoping, S. I. G., & Taskforce, T. (2011). Information supplement: Pci dss tokenization guidelines. Standard: PCI Data Security Standard (PCI DSS), 24.

5. Abdullah, A. M., & Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).

6. Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

7. Gaj, K., & Chodowiec, P. (2001, April). Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using Field Programmable Gate Arrays. In Cryptographers' Track at the RSA Conference (pp. 84-99). Springer Berlin Heidelberg. [4] Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India

8. Yenuguvanilanka, J., & Elkeelany, O. (2008, April). Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. In Southeastcon, 2008. IEEE (pp. 222- 225)

9. Lu, C. C., & Tseng, S. Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on (pp. 277-285)