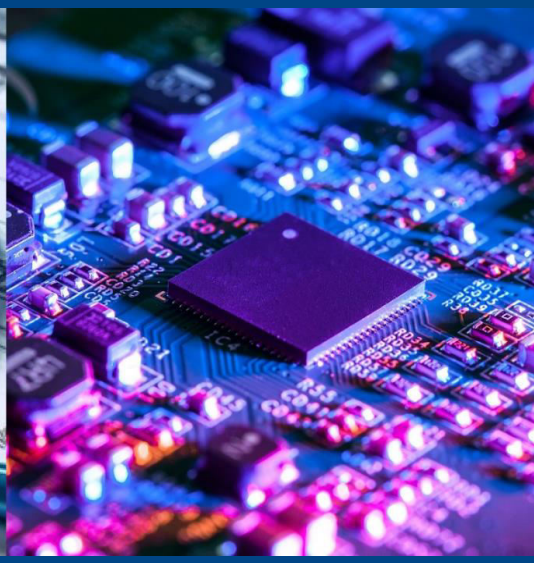
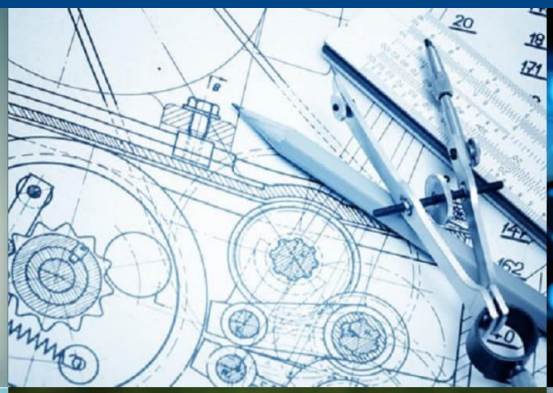
ISSN: 2582-7219

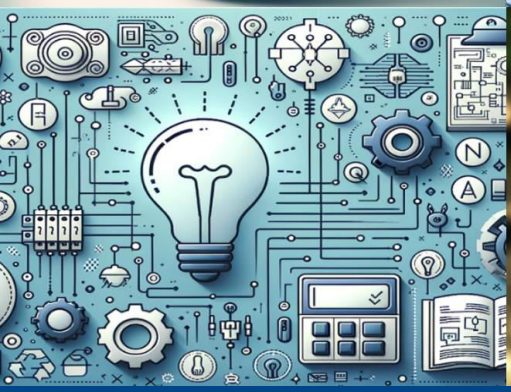




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 6, June 2025**

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806030

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Digital Payment in E-Commerce using AES Algorithm

Jennifer, Prakriti Bhandary

PG Student, St Josheph Engineering College, Vamanjoor, Mangalore, India

Assistance Professor, St Josheph Engineering College, Vamanjoor, Manglore, India

ABSTRACT: The Era of Information and Communication Technology (ICT) and digital innovation lead to dynamic changes in the business environment, where business transactions continue to shift from cash-based transactions to electronic-based transactions. The e-payment system was not introduced to replace cash but as a better alternative to cash and trade barter. Electronic payments can be understood as a payment mechanism using electronic media that does not involve cash. Electronic payment system (e-payment) is an important aspect of e-commerce.

I. INTRODUCTION

E-commerce grows rapidly and provides an opportunity for companies to increase sales over the internet. The advent of e-commerce has created new financial needs that are not effective in many cases met traditional payment systems. An electronic payment system comes to replace a cash payment system. Sales of goods and services increased significantly with the adoption of the use of e-payment systems so that electronic payments became an increasingly important part of the payment system.

E-Payment is a system that provides tools for payment of services or goods carried on the internet. E-payment system provides the ease of transaction processing in e-commerce between consumers and sellers. Using the E- payment System has many benefits for payers, payees, E-commerce, banks, organizations and governments.

An efficient and reliable e-payment system enables faster payouts, better tracking, transparent transactions, reduced time use, cost savings and increased trust between sellers and buyers. We require an electronic payment (e-payment) system that are not only provides secure payments system but also must have properties such as online customers and seller authentication, proof of transactions authorized by customers to both sellers and banks, customer privacy and transactional data security.

Many individuals are excited about obtaining their own online website for their company, as it is possible to market items online around the world. Customers are also interested in online shopping since they do not wish to waste valuable time shopping-commerce implies an electronic purchasing and marketing process online by using typical Web browsers.

II. LITERATURE

Electronic payment systems have continued to grow over recent years because of the increase of online banking and shopping. As the world advances much more with technological advancements, we are able to see the growth of e-payment methods and transaction processing devices. A payment gateway is a service provider that offers equipment to procedure a transaction between buyers and merchants, along with banks over the World Wide Web. It supports secure a purchase along with a person's transaction information inside a transaction. This paper is focused on understanding main payment methods and latest trends caused by new digital platforms development in terms of online shopping consumers´ behavior. A payment gateway defends transaction information by encrypting sensitive information, to guarantee the information is transferred securely between a consumer and the transaction processor.

To help make it secure between each element, particularly between the client and the Internet payment or merchant gateway, a few strategies are recommended. Specifically, online buyers have to feel comfortable that their personal information and banking details are protected and cannot be seen by hackers. Thus, a connection that is secure it needed

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806030

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

to assure payment transactions. Internet is not only media for networking but also a place where customers could shop or buy goods and services. Digitization and modern trends are forcing businesses to offer goods and services to the digital market and sell their goods or services to consumers. Internet shop, in other words also e- store, e-shop, web shop, internet shop or online store, gives businesses a much wider reach to potential customers.

Online shopping has evolved and gained more market share and rapidly approached the customer. E-commerce is a concept used for buying, selling, or exchanging products, services and information via the Internet. Online payment methods include the following forms of payment for goods or services: Payment cards, Payment buttons, electronic wallet, Deferred payment, Benefit payments, Mobile application, M-payment or payment via Premium SMS. Offline methods are: Cash on delivery, Payment for personal collection, Transfer to account, Purchase in instalments. Another possibility of dividing payment methods is according to the assortment offered by the trader (digital content and services or tangible goods). Payment methods can also be divided according to which entity technically provides and mediates the payment methods offered by the e-shop.

Figure 1. How a payment gateway works

III. METHODOLOGY

The methodology used in this paper is the analysis, synthesis, comparison in time. This study develops part of the quantitative analysis of online shopping habits among customers.

A. Triple Data Encryption Standard:

The 3DES algorithm utilizes the data encryption standard (DES) cipher three times to encrypt its information. DES is a symmetric key algorithm based on the Feistel cipher. As a symmetric crucial cipher, it applies a similar element for both encryption and decryption processes. The Feistel cipher can make both processes almost precisely the same, which results in an algorithm that is more effective to put into action. DES has both a 64-bit
block and key measurement but, in training, grants just 56 bits of security. 3DES was created as a safe option due to DES's small crucial length. In 3DES, the DES algorithm is operated three times with three secrets and is regarded as safe in the event that three individual keys are used. They encourage cryptographic libraries, such as certified AES 3DES.

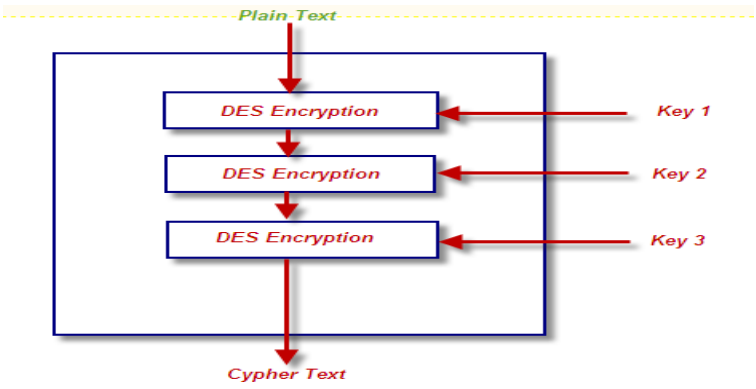


Figure 2 Triple Data Encryption Standard

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

B. RSA Cryptosystem:

RSA was planned and created by Ron Rivest, Adi Shamir, and Leonard Adleman around 1978. It is probably the supreme identified cryptosystem for replacing digital or key autograph or perhaps for enciphering chunks of information. RSA usually involves three steps: key generation, decryption, and encryption. RSA has numerous bugs in its strategy and thus is not encouraged for financial use. The most crucial security services that come with RSA are privacy and secrecy, authentication, integrity, and non-repudiation, because they prove RSA's being an excellent security public-key cryptosystem. The approach presented in this research paper requires a high level of safety, which can be effectively achieved and achieved and fulfilled.

The following is the algorithm of the RSA cryptosystem. P and Q both Prime, P , Q ∅ = (p-1) (q-1) 1 1 < e< n Cipher text: C = Me mod n Cipher text Decryption: Plaintext: M = Cd mod n

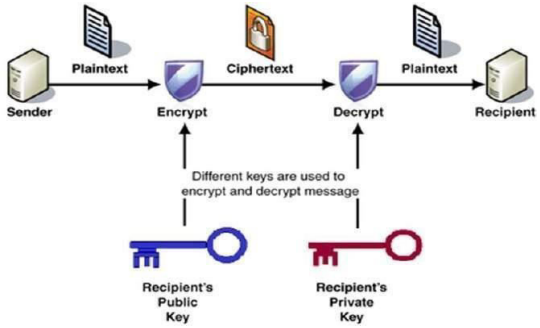


Figure 3. RSA is a public-key cryptosystem

IV. IMPLEMENTATION

Algorithms Used:

ADVANCED ENCRYPTION STANDARD(AES):

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is much stronger than DES and triple DES despite being harder to implement.

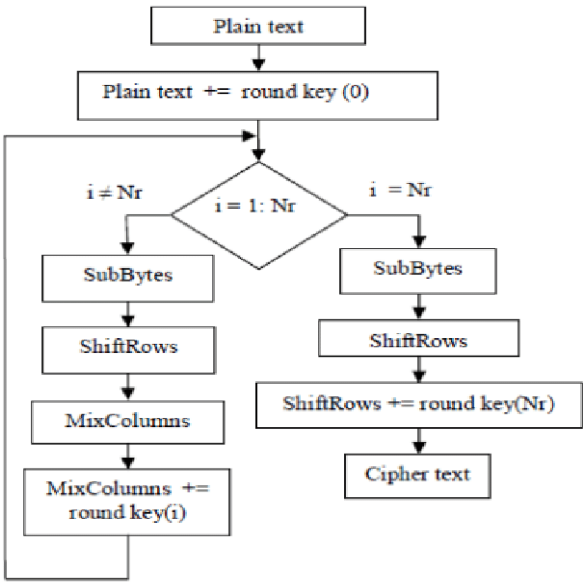


Figure 4. AES encryption algorithm

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits. Most AES calculations are done in a particular finite field.

High-level description of the algorithm:

1. Key Expansion: Round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128- bit round key block for each round plus one more.
2. Initial round key addition:
   - ✓ AddRoundKey – each byte of the state is combined with a byte of the round key using bitwise xor.
3. 9, 11 or 13 rounds:
   - ✓ SubBytes – a nonlinear substitution step where each byte is replaced with another according to a lookup table.
   - ✓ ShiftRows – a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   - ✓ MixColumns – a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
   - ✓ AddRoundKey
4. Final round (making 10, 12 or 14 rounds in total):
   - ✓ SubBytes
   - ✓ ShiftRows
   - ✓ AddRoundKey

1. The SubBytes step:

After substitution, the bytes of the input are replaced by another byte using a SubByte lookup table. The state array before round 0 is merely plaintext/input. Thus, this operation makes AES nonlinear and hence more secure than linear transformations such as a simple substitution cipher. The S Box used is derived from the invertible multiplicative inverse over having good properties of non-linearity. For instance, to avoid attacks based on simple algebraic properties of the S-box, it can be constructed by combining the inverse function with an invertible affine transformation in order to produce necessary diffusion property. In addition, there must not be any pairs (ai,j,S(ai,j)) which are fixed points in order for all output values to be different from their input counterparts; that is, ai,j≠S(ai,j), and also S(ai,j)⊕ai,j≠FF16: this is done to prevent against finding each other's inverses easily through linear algebraic methods. The decryption process utilizes an InvSubBytes step i.e., the inverse operation of SubBytes which necessitates inversing first the affine transformation and finding multiplicative inverse next.

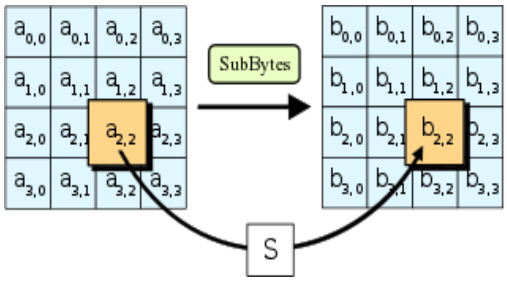


Figure 5. SubBytes

2. The ShiftRows step:

This is a step that works on the state's rows by cyclically moving the bytes of each row by certain offsets. In AES, the first row remains unchanged. This means that for every byte in the second row, it is shifted one position to the left as shown above. The same applies to third and fourth rows where they are moved with offset of 2 and 3 respectively. This way, any column or output state after ShiftRows step will comprise some bits from every column of input state.

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806030

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Conversely, if this stage were missed out upon in AES encryption mode each column would be encrypted separately turning AES into four independent block ciphers.

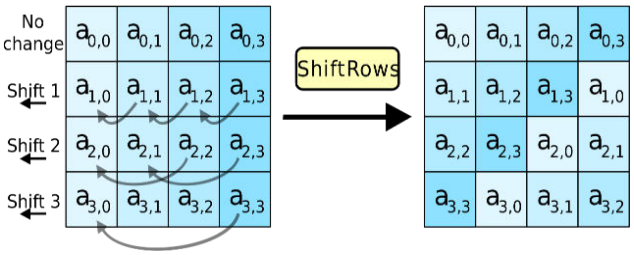


Figure 6. ShiftRows

3. MixColumns:

This step is a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result. In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher. Mix Columns Operation each column is mixed independent of the other.

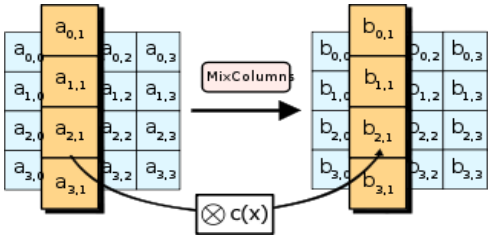


Figure 7. Mix Columns

4. The AddRoundKey:

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining of the state with the corresponding byte of the subkey using bitwise XOR.

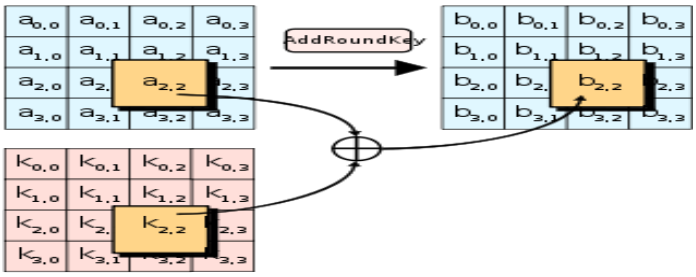


Figure 8. AddRoundkey

V. RESULTS

AES is a widely used symmetric encryption algorithm that secures data through various rounds of transformation, depending on the key size. The three main key sizes are 128, 192, and 256 bits. AES operates on blocks of 128 bits using a key size of 128, 192, or 256 bits. It involves multiple rounds of processing, including SubBytes, ShiftRows, MixColumns, and AddRoundKey operations. The number of rounds varies with the key size: 10 rounds for a 128-bit

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key. AES was designed to replace the Data Encryption Standard (DES) and is considered highly secure due to its resistance to various forms of cryptographic attacks, including brute-force attacks and differential cryptanalysis.

AES is efficient in both hardware and software implementations, making it suitable for a wide range of applications. AES is resistant to known cryptanalytic attacks such as linear and differential cryptanalysis. The large key sizes (especially 256 bits) provide robust security margins.AES-256 offers a higher level of security compared to AES- 128 and AES-192 due to the increased key size. AES's strength comes from its complex key schedule and the number of rounds.

With a sufficiently long key (e.g., 256 bits), the algorithm provides an extremely high level of security. While AES has been theoretically analyzed and found secure, practical attacks on AES implementations are more likely to target weaknesses in the implementation rather than the algorithm itself. AES-128 is generally the fastest among the three key sizes, followed by AES-192 and AES-256, due to fewer rounds of processing. AES requires less computational power and memory compared to older encryption algorithms like DES. Its performance is often optimized in hardware and software.

AES is used in a wide range of applications including file encryption, secure communications (e.g., SSL/TLS), and disk encryption. AES is compliant with various standards and regulations, such as FIPS PUB 197 (Federal Information Processing Standard) and is widely adopted in industry standards. The flexibility of AES makes it suitable for various use cases, from securing personal data to encrypting large-scale data communications. As computational power increases, the 256-bit key version of AES is seen as future-proof, providing long-term security assurance. Implementing AES requires careful attention to avoid common pitfalls such as improper key management or weak random number generation. AES is standardized, reducing the risk of vulnerabilities due to non-standard implementations. It also enhances customer retention and loyalty by allowing businesses to address negative feedback proactively and reinforce positive experiences.

VI. CONCLUSION

Innovative payment methods have completely changed the way that transactions are completed in the world of online purchasing, providing efficiency and convenience for both customers and merchants. With the popularity of payments growing, it is essential to guarantee the security of these transactions in order to preserve confidence and protect financial data. In this regard, the Advanced Encryption Standard (AES) algorithm is involved. Data transmitted during transactions is adequately protected from any cyber threats and unlawful access by AES's encryption feature. Digital payment systems can be made more secure by e-commerce platforms by using AES to protect financial data. As a result, adding AES to payment systems not only increases transaction security but also fosters client confidence, which in turn promotes the success and continued growth of online purchasing. AES encryption guarantees the effective protection of sensitive data during transmission in the context of digital payments, including credit card numbers, personal identity numbers, and transaction details. AES reduces the risk of data breaches and cyberattacks by encrypting this data to prevent unauthorized parties from accessing or altering it.

REFERENCES

1. Fatonah, S., A. Yulandari, and Ferry Wahyu Wibowo. "A review of e-payment system in e commerce." Journal of Physics: Conference Series. Vol. 1140. No. 1. IOP Publishing, 2018.
2. Geerling, Max. "E-commerce: A merchant's perspective on innovative solutions in payments." Journal of Payments Strategy & Systems 12.1 (2018): 58-67.
3. Miva. The History of Ecommerce: How Did It All Begin?—Miva Blog. Available online: https://www.miva. com/blog/the-history-of ecommerce-how-did-it-all-begin/ (accessed on 16 June 2020).
4. Kedah, Zulkarnain. "Use of e-commerce in the world of business." Startupreneur Business Digital (SABDA Journal) 2.1 (2023): 51-60

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com