

# Enhancing credit card security using RSA encryption and tokenization: a multi-module approach

Mainak Saha, M. Trinath Basu, Arpita Gupta, K. Ashrith, Chevella Vamshi Vardhan Reddy, Shashanth Reddy, Rohith Reddy

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India

## Article Info

### Article history:

Received May 6, 2024

Revised Aug 4, 2024

Accepted Nov 22, 2024

### Keywords:

Credit card protection

Data privacy

Financial transaction

RSA encryption

Tokenization

## ABSTRACT

The security of credit card information remains a critical challenge, with existing methods often falling short in safeguarding data integrity, confidentiality, and privacy. Traditional approaches frequently transmit sensitive information in unencrypted formats, exposing it to significant risks of unauthorized access and breaches. This study introduces a robust security framework that leverages Rivest-Shamir-Adleman (RSA) encryption and tokenization to protect credit card information during transactions. The proposed solution is structured into three key modules: merchant, tokenization, and token vault. The merchant module works in tandem with the tokenization module to generate transaction validation tokens and securely transmit credit card data. The token vault, maintained on a secure cloud storage platform, acts as a restricted-access database, ensuring that sensitive information is encrypted and inaccessible to unauthorized entities. Through this multi-layered approach, the study demonstrates a significant enhancement in the security of credit card transactions, effectively mitigating the risks of data breaches and unauthorized disclosures. The findings indicate that the proposed method not only addresses existing security vulnerabilities but also offers a scalable and efficient solution for protecting financial transactions.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Mainak Saha

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation

Hyderabad-500075, Telangana, India

Email: mainak.skms@gmail.com

## 1. INTRODUCTION

In today's digital landscape, safeguarding sensitive information such as credit card numbers is of paramount importance, given the widespread reliance on online financial transactions. Using strong encryption and decryption methods to guard against fraud and unauthorized access is a crucial part of information security [1]. The evolution of financial transactions from traditional in-person exchanges to online and digital platforms has dramatically increased the risks associated with these activities, particularly in the form of data breaches and identity theft [2]. This study explores the fundamental principles of credit card encryption and decryption and underscores their crucial role in securing online financial transactions.

Despite technological advancements, current strategies for protecting sensitive financial data often fall short, especially in the transmission and storage of credit card information. Unencrypted data is frequently sent to remote servers, increasing the risk of unauthorized access and breaches. Ensuring the integrity, confidentiality, and privacy of credit card data is crucial for maintaining consumer trust and preventing financial fraud [3], [4]. The limitations of existing encryption methods underscore the urgent need for more secure and reliable solutions to protect financial data from malicious actors.

Several studies have investigated various approaches to enhancing credit card security, with encryption and tokenization techniques being at the forefront of these efforts. Encryption, a process that converts credit card data from plain text into ciphertext, renders the data unreadable without the appropriate decryption key as shown in Figure 1. Symmetric and asymmetric encryption are the two main types of encryption methods. AES (advanced encryption standard) and RSA (Rivest-Shamir-Adleman) are two popular techniques [5]. At instance, RSA encryption is a well-known public-key cryptosystem that has shown to be successful at protecting private data [6]. It has also been shown that tokenization, which substitutes distinct identifiers for sensitive data, is beneficial in lowering the exposure of credit card information during transactions [7]. However, the challenge lies in integrating these technologies into a comprehensive security framework. Regulatory compliance standards such as payment card industry data security standard (PCI DSS) and general data protection regulation (GDPR) further underscore the importance of encrypting credit card data to prevent unauthorized access and interception. Numerous data breaches have occurred due to improper encryption of credit card data, resulting in severe consequences for both individuals and organizations [8].

This study presents a security solution combining RSA encryption with tokenization to protect credit card information. The system includes three modules: merchant, tokenization, and token vault. The merchant and tokenization modules generate transaction validation tokens and securely transmit credit card data, while the token vault, hosted on a cloud platform, ensures controlled and restricted access to stored data. This multi-module design encrypts and safely stores critical information, reducing the risk of data breaches and unauthorized disclosures. However, the decryption process faces challenges from brute-force attacks and cryptographic vulnerabilities [9], [10].

The proposed solution significantly advances credit card security by integrating RSA encryption and tokenization into a unified framework, addressing the limitations of existing measures and offering a scalable, robust solution for securing financial transactions. By encrypting sensitive information during transmission and securely storing it in a controlled environment, the system enhances credit card data security. Emerging encryption technologies, such as homomorphic and quantum encryption, show promise for further securing transactions against evolving cyber threats. This study also presents case studies of organizations that have successfully implemented robust encryption practices, highlighting best practices for securely storing and transmitting credit card information, including tokenization and end-to-end encryption. Future trends and challenges in credit card encryption include the integration of artificial intelligence and blockchain technology, which could set new standards for financial data protection, contributing to efforts to prevent fraud and maintain consumer trust in digital transactions.



Figure 1. Process of encryption and decryption [5]

## 2. RELATED WORK

### 2.1. Historical development of encryption in payment systems

The development of encryption in payment systems began with basic cryptographic techniques, such as symmetric key encryption, to protect cardholder information during transmission. As cyber threats evolved, more robust methods like AES and public-key infrastructure (PKI) were developed specifically to secure financial transactions [11].

### 2.2. Encryption standards and protocols

Credit card transactions use industry-standard encryption mechanisms to ensure data integrity and confidentiality. The PCI DSS mandates strong encryption methods like triple data encryption standard (DES) or AES to protect sensitive cardholder data. Protocols such as secure sockets layer (SSL) and transport layer security (TLS) secure communication channels and enhance electronic payment security [12]. Despite these

measures, credit card systems still encounter security challenges, including cryptographic attacks and malware threats. These vulnerabilities highlight the need for additional security measures, such as endpoint protection and user authentication.

### 2.3. Future directions and emerging trends

Future advancements in credit card encryption are poised to address current security issues and enhance payment system resilience. Innovations like quantum-resistant cryptography, homomorphic encryption, and blockchain-based solutions promise significant improvements in financial transaction security [13]. Furthermore, advancements in artificial intelligence and machine learning are expected to play a crucial role in detecting threats and enabling proactive security systems to swiftly counter evolving cyber risks [14].

## 3. PROPOSED METHOD

The proposed system addresses the shortcomings identified in evaluated and published works by incorporating merchant and tokenization modules, along with a token vault, as illustrated in Figure 2.

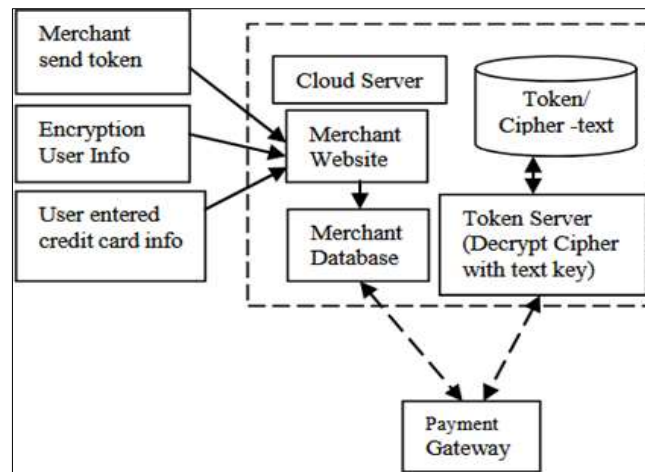


Figure 2. The proposed system's architectural design [6]

### 3.1. System architecture

The system is designed to enhance security by separating the credit card processing into distinct modules:

- i) Merchant module: this module is where customers enter their credit card information. It functions as the initial point of interaction for cardholders, capturing essential data such as card number, expiration date, and CVV code. This data is then securely transmitted to the tokenization module.
- ii) Tokenization module: the payment gateway controls this module, which is responsible for generating unique transaction validation tokens. When a credit card transaction is initiated, the tokenization module replaces sensitive card information with a non-sensitive token. This token is used in place of the actual card number during the transaction process, thereby reducing the risk of data breaches.
- iii) Token vault: the token vault is a secure, restricted access database stored on a cloud storage platform. It holds the mapping of tokens to their respective credit card information. Access to this vault is tightly controlled and regulated to ensure the protection of the sensitive data it contains.

The interaction between these modules is crucial for secure credit card transactions. The merchant module collects and transmits card information securely, while the tokenization module generates and manages tokens. These tokens are stored in the token vault for validation, minimizing unwanted access and reducing the risk of disclosing private credit card information.

### 3.2. Hardware and software requirements

The hardware requirements for this system include a standard computer with a multi-core processor and sufficient RAM to handle data processing efficiently. The software stack comprises [15]: i) backend:

APACHE server; ii) frontend: HTML, CSS, and JavaScript; and iii) database: MySQL, used for managing credit card encryption and decryption processes essential for secure payment processing.

### 3.3. Security protocols

Security protocols are critical for protecting credit card information during transmission and storage [16]. The following protocols and encryption methods are implemented:

- i) SSL/TLS: this industry-standard security protocol creates secure connections by encrypting data in transit to guarantee secrecy between a user's web browser and a website or between servers within a network.
- ii) Point-to-point encryption: using a card reader or other point of sale, this method encrypts credit card data all the way to the payment processor. It requires specialized hardware and software for data encryption during the transaction process.
- iii) End-to-end encryption: this comprehensive approach encrypts credit card data from the moment the cardholder enters it until the payment gateway or processor processes it, typically involving secure payment gateway services and software that handles encryption.

### 3.4. Payment gateway services and encryption algorithms

Third-party payment gateway services facilitate payment processing, often incorporating built-in encryption to safeguard cardholder information. Examples of such services include Stripe, PayPal, and Authorize.Net. Several encryption techniques, such as the AES, triple DES, and RSA algorithms, are used to safeguard credit card data [17], [18]. These algorithms are implemented through software libraries and frameworks.

### 3.5. Algorithm used

RSA encryption: the security of data storage and transmission is enhanced by the RSA asymmetric encryption technique. By encrypting and decrypting data using a pair of keys (public and private), RSA guarantees secure communication between parties, as illustrated in Figure 3, which shows the flowchart of the RSA algorithm and tokenization process [19]. RSA encryption process includes:

- i) Key generation: generate two keys - a private key ( $d$ ) and a public key ( $e$ ). The encryption process uses the public key, whereas the decryption process uses the private key.
- ii) Encryption: given a plaintext message  $M$ , the encryption process is represented as  $C=E(M)$ , where  $C$  is the ciphertext.
- iii) Decryption: the decryption process is  $M=D(C)$ , where  $M$  is the recovered plaintext message.

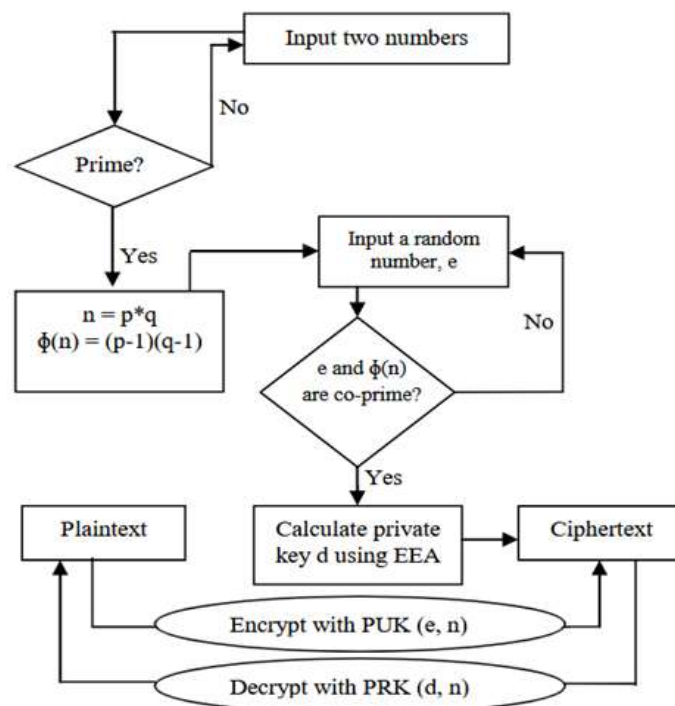


Figure 3. Flowchart of RSA algorithm tokenization [6]

Luhn formula: the Luhn algorithm is used to verify credit card numbers. Given a credit card number  $A_1, A_2, \dots, A_n$ , the algorithm calculates sums of digits at odd and even positions, verifying the card number if  $Z \bmod 10 = 0$ . For private key calculation, the private key for decryption is determined using the extended euclidean algorithm (EEA), Euler's totient function, Euler's totient theorem, and the RSA method. Euler's totient function for a prime number  $p$  is  $\phi(p) = p - 1$ . For two prime numbers  $p$  and  $q$ ,  $\phi(p \cdot q) = (p - 1)(q - 1)$ . In tokenization integration, tokenization servers use RSA and EEA to decrypt ciphertext transmitted by the payment gateway. The EEA calculates the private key  $A$  using a matrix iterative algorithm with  $\phi(n)$  and a public key  $e$ . HMAC (hash-based message authentication code) to guarantee data integrity and authenticity, HMAC uses a cryptographic hash function with a secret key [20]. Lastly, PKI in order to ensure the security of encryption key transfers and the legality and integrity of credit card transactions, PKI offers a safe framework for handling digital certificates and public-key encryption [21].

#### 4. METHOD

Credit card encryption ensures the security of sensitive financial data during transactions, including card numbers and billing details. Figure 4 illustrates the encryption and decryption process of a cipher, where plaintext ("Hello World") is converted to ciphertext and then back to plaintext using a shared key [22].

Encryption includes:

- i) Symmetric encryption: using a single key for encryption and decryption makes symmetric encryption quick and efficient for big data volumes. For instance, AES. This method encrypts credit card data using a private key, preventing unauthorized access. Since anybody with the key may decode the data, securely sharing and controlling it is difficult [23].
- ii) Asymmetric encryption: private keys decode data while public keys encrypt it in asymmetric encryption, or public-key encryption. The private key cannot be deduced from the public key since these keys are mathematically linked but separate. This algorithm is popular: RSA [24]. Credit card transactions are encrypted by the recipient's public key, and only the recipient's secure private key may decode it. This strategy boosts security by reducing the need to exchange the decryption key with external parties.
- iii) Transmission: the intended destination, usually a payment processor or a merchant's server, receives the encrypted credit card information safely across the network. The recipient uses the appropriate decryption key, either symmetric or asymmetric, to decrypt the data for further processing.
- iv) Data processing: once the credit card information is decrypted, it can be used for payment authorization and processing. Secure decryption ensures that sensitive data remains protected until it reaches a trusted party.

Security Measures includes:

- i) Key management: to prevent unauthorized access to sensitive data, encryption keys must be securely managed and stored. This includes using hardware security modules (HSMs), implementing key rotation policies, and restricting key access based on roles and responsibilities.
- ii) Transport layer protection: data transmitted over the internet is encrypted using secure channels like TLS, providing protection against interceptions and man-in-the-middle attacks. TLS ensures that intercepted data cannot be decrypted without the proper key.
- iii) Compliance standards: the payment card industry data protection standard mandates robust encryption and protection for credit card data [25]. Compliance ensures that sensitive data is protected throughout the transaction process.

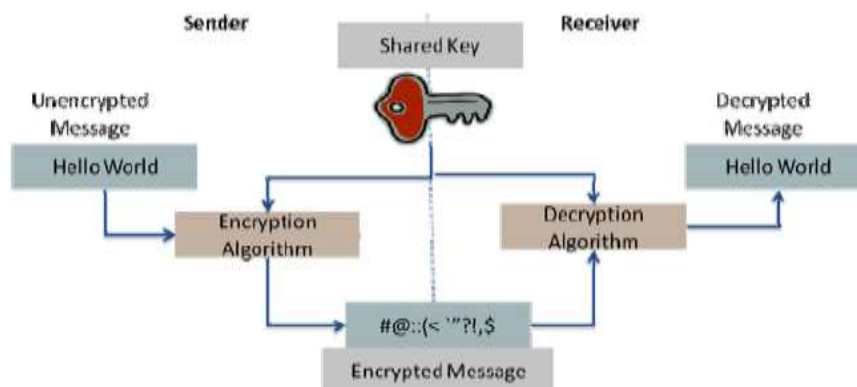


Figure 4. The methods used by ciphers to encode and decode data [22]

- iv) Tokenization: tokenization enhances security by replacing sensitive credit card information with a unique token. This token is meaningless without authorization and reduces the risk of data breaches by ensuring actual credit card numbers are not transmitted or stored.
- v) Authorization and processing: after decryption and validation, the transaction is authorized and payment processing begins. Strong encryption and decryption techniques and other security measures reduce the danger of data breaches and unauthorized access.

## 5. RESULTS AND DISCUSSION

Encrypting credit card data is crucial for protecting sensitive financial information. This process involves converting plaintext, readable credit card information, into ciphertext using sophisticated encryption algorithms and keys, making it unreadable to unauthorized users [26]. Decryption reverses this process, returning the ciphertext to its original form.

### 5.1. Encryption methods and key management

Strong encryption techniques are essential for securing credit card data. One of the most reliable algorithms is AES, which has key lengths of 128, 192, or 256 bits that are quite impervious to brute-force assaults. Companies like Visa and MasterCard use AES to secure transactions, significantly reducing unauthorized access risks [27]. Additionally crucial is secure key management, which covers key creation, distribution, storage, and revocation. Google's Cloud Key Management service, for example, provides automated key rotation and secure key management across cloud services.

### 5.2. Regulatory compliance

PCI DSS and other strict rules must be followed by businesses handling credit card data. PCI DSS outlines comprehensive rules for protecting credit card data [28]. Companies like Amazon and Stripe follow PCI DSS-compliant encryption protocols to avoid penalties and ensure data security, fostering customer trust.

### 5.3. Results of effective encryption and decryption

Good encryption and decryption techniques have the following beneficial effects:

- i) Enhanced security: strong encryption protocols help protect credit card data from unauthorized access and potential breaches. Organizations may protect sensitive information from cyber-attacks by making sure that data is encrypted while it is in transit and at rest [29].
- ii) Privacy protection: effective encryption safeguards customer privacy by ensuring that sensitive information remains confidential. This builds trust with customers, who can be assured that their financial details are being handled securely.
- iii) Building trust with customers: encryption is one of the transparent security techniques that helps establish and preserve consumer confidence. Consumers are more inclined to interact with companies that show a dedication to protecting their financial and personal data.
- iv) Regulatory compliance: compliance with PCI DSS and other relevant regulations helps organizations avoid penalties and legal repercussions. It also ensures that best practices in data security are followed, reducing the likelihood of security incidents.
- v) Mitigated risks: organizations reduce the risks of financial losses, reputational harm, and operational interruptions connected with data breaches by encrypting credit card data.
- vi) Integrity of financial transactions: encryption helps maintain the integrity of financial transactions by protecting the data from tampering and unauthorized alterations. This ensures that transactions are processed accurately and securely.

### 5.4. Challenges

Encryption and decryption come with costs and complexities. Implementing and managing encryption solutions can be resource-intensive, requiring specialized knowledge and infrastructure [30]. For instance, small businesses might struggle with the initial costs and technical demands of advanced encryption. However, the trade-off in improved security and compliance generally justifies the investment. Large businesses and financial institutions often find that the long-term benefits of reduced data breach risks outweigh the initial and ongoing maintenance costs. Additionally, as encryption methods evolve, organizations need to continuously update their security strategies to counter new threats, adding to the complexity. Nonetheless, the long-term protection of sensitive data and regulatory compliance make these efforts worthwhile.



## 6. CONCLUSION

Credit card encryption and decryption are vital in cybersecurity, ensuring the protection of sensitive data during transfer and storage. Encryption converts readable plaintext into an unintelligible code through complex algorithms and secure key management, acting as a barrier against unauthorized access. A popular symmetric key encryption method that maintains data privacy even in the event that initial security measures are compromised is the AES.

Encryption not only secures data but also builds trust between businesses and customers, crucial in today's digital economy where electronic payments are common. Compliance with industry standards, such as PCI DSS, is essential to avoid data breaches, legal issues, and reputational damage, making robust encryption both a security and strategic necessity.

Implementing encryption poses challenges, including managing key generation and transmission, and addressing integration costs. However, these challenges are outweighed by the risks of data breaches and regulatory penalties. By adopting advanced encryption practices and adhering to standards, organizations can protect financial data, ensure privacy, and maintain consumer trust in an increasingly interconnected world.





## REFERENCES

- [1] S. Kumar, B. K. Singh, Akshita, S. Pundir, S. Batra, and R. Joshi, "A survey on symmetric and asymmetric key based image encryption," in *2nd International Conference on Data, Engineering and Applications (IDEA)*, Feb. 2020, pp. 1–5, doi: 10.1109/IDEA49133.2020.9170703.
- [2] F. Bisogni and H. Asghari, "More than a suspect: an investigation into the connection between data breaches, identity theft, and data breach notification laws," *Journal of Information Policy*, vol. 10, pp. 45–82, May 2020, doi: 10.5325/jinfopoli.10.2020.0045.
- [3] M. Suganya and T. Sasipraba, "Stochastic gradient descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment," *Journal of Cloud Computing*, vol. 12, no. 1, p. 74, May 2023, doi: 10.1186/s13677-023-00442-6.
- [4] S. Gahane, R. Pohankar, K. Ugemuge, and D. Nakhate, "Data security in a cloud environment using cryptographic mechanisms," in *International Conference on ICT for Sustainable Development*, 2023, pp. 103–110, doi: 10.1007/978-981-99-4932-8\_11.
- [5] M. M. Hoobi, "Multilevel cryptography model using RC5, twofish, and modified serpent algorithms," *Iraqi Journal of Science*, pp. 3434–3450, Jun. 2024, doi: 10.24996/ij.s.2024.65.6.37.
- [6] G. B. Iwasokun, "Encryption and tokenization-based system for credit card information security," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 3, pp. 283–293, 2018, doi: 10.17781/P002462.
- [7] O. Al-Maliki and H. Al-Assam, "A tokenization technique for improving the security of EMV contactless cards," *Information Security Journal: A Global Perspective*, vol. 31, no. 5, pp. 511–526, Sep. 2022, doi: 10.1080/19393555.2021.2001120.
- [8] Q. Zhang, "An Overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption," in *2021 2nd International Conference on Computing and Data Science (CDS)*, Jan. 2021, pp. 616–622, doi: 10.1109/CDS52072.2021.00111.
- [9] R. Mei, H.-B. Yan, Y. He, Q. Wang, S. Zhu, and W. Wen, "Considerations on evaluation of practical cloud data protection," in *China Cyber Security Annual Conference*, 2022, pp. 51–69, doi: 10.1007/978-981-19-8285-9\_4.
- [10] M. L. N. V. S. Manikanta, C. S. Poojith, M. B. Prakash, V. B. Sathwik, R. Mothukuri, and S. Bulla, "Securing the cloud through the implementation of encryption algorithms- a comprehensive study," in *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAIC)*, Jun. 2024, pp. 1490–1498, doi: 10.1109/ICAIC60222.2024.10575777.
- [11] P. William, A. Choubey, G. S. Chhabra, R. Bhattacharya, K. Vengatesan, and S. Choubey, "Assessment of hybrid cryptographic algorithm for secure sharing of textual and pictorial content," in *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, Mar. 2022, pp. 918–922, doi: 10.1109/ICEARS53579.2022.9751932.
- [12] J. Han et al., "TIFF: tokenized incentive for federated learning," in *2022 IEEE 15th International Conference on Cloud Computing (CLOUD)*, Jul. 2022, pp. 407–416, doi: 10.1109/CLOUD55607.2022.00064.
- [13] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.
- [14] E. M. S. Balagolla, W. P. C. Fernando, R. M. N. S. Rathnayake, M. J. M. R. P. Wijesekera, A. N. Senarathne, and K. Y. Abeywardhana, "Credit card fraud prevention using blockchain," in *2021 6th International Conference for Convergence in Technology (I2CT)*, Apr. 2021, pp. 1–8, doi: 10.1109/I2CT51068.2021.9418192.
- [15] S. Diaz-Santiago, L. M. Rodríguez-Henríquez, and D. Chakraborty, "A cryptographic study of tokenization systems," *International Journal of Information Security*, vol. 15, no. 4, pp. 413–432, Aug. 2016, doi: 10.1007/s10207-015-0313-x.
- [16] D. D. Kumar, J. D. Mukharzee, C. V. D. Reddy and S. M. Rajagopal, "Safe and Secure Communication Using SSL/TLS," 2024 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2024, pp. 1–6, doi: 10.1109/ESCI59607.2024.10497224.
- [17] V. Veronica, R. S. Oetama, and A. Ramadhan, "Incorporating rivest-shamir-adleman algorithm and advanced encryption standard in payment gateway system," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 22, no. 3, pp. 629–644, Jun. 2024, doi: 10.12928/telkomnika.v22i3.25578.
- [18] P. Parikh, N. Patel, D. Patel, P. Modi, and H. Kaur, "CIPHERING the modern world: a comprehensive analysis of DES, AES, RSA and DHKE," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, Feb. 2024, pp. 838–842, doi: 10.23919/INDIACom61295.2024.10498330.
- [19] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.7551/mitpress/12274.003.0047.
- [20] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in *Advances in Cryptology-CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara*, 1996, pp. 1–15, doi: 10.1007/3-540-68697-5\_1.
- [21] A. Panigrahi, A. K. Nayak, R. Paul, B. Sahu, and S. Kant, "CTB-PKI: clustering and trust enabled blockchain based PKI system for efficient communication in P2P network," *IEEE Access*, vol. 10, pp. 124277–124290, 2022, doi: 10.1109/ACCESS.2022.3222807.





- [22] S. Hamad, "A novel implementation of an extended 8x8 playfair cipher using interweaving on DNA-encoded data," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 4, no. 1, pp. 93–100, Feb. 2014, doi: 10.11591/ijece.v4i1.4969.
- [23] M. N. Alenezi, H. K. Alabdulrazzaq, and N. Mohammad, "Symmetric encryption algorithms: review and evaluation study," *Int. J. Commun. Networks Inf. Secur.*, vol. 12, 2020, doi: 10.54039/IJCNIS.V12I2.4698.
- [24] S. Khatakar and R. Kamble, "A survey and performance analysis of various RSA based encryption techniques," *International Journal of Computer Applications*, vol. 114, no. 7, pp. 30-33, 2015, doi: 10.5120/19993-1736.
- [25] P. Atri, "Enhancing big data security through comprehensive data protection measures: a focus on securing data at rest and in-transit," *International Journal of Computing and Engineering*, vol. 5, no. 4, pp. 44-55, 2024, doi: 10.47941/ijce.1920.
- [26] S. Wang, "A study of the use of euler totient function in RSA cryptosystem and the future of RSA cryptosystem," *Journal of Physics: Conference Series*, vol. 2386, no. 1, p. 012030, Dec. 2022, doi: 10.1088/1742-6596/2386/1/012030.
- [27] D. Limbachia, "Encryption of card details using AES with a 128-bit key a secure approach to data protection," *Interantional Journal Of Scientific Research In Engineering And Management*, vol. 08, no. 03, pp. 1-5, 2024, doi: 10.55041/ijsrem29484.
- [28] A. Ukidve, D. S. SMantha, and M. Tadvalka, "Analysis of payment card industry data security standard [PCI DSS] compliance by confluence of COBIT 5 Framework," *International Journal of Engineering Research and Applications*, vol. 07, no. 1, pp. 42-48, 2017, doi: 10.9790/9622-0701014248.
- [29] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik*, vol. 127, no. 4, pp. 2341–2345, Feb. 2016, doi: 10.1016/j.ijleo.2015.11.188.
- [30] X. Zhang and K. K. Parhi, "Implementation approaches for the advanced encryption standard algorithm," *IEEE Circuits and Systems Magazine*, vol. 2, pp. 24-46, 2002, doi: 10.1109/MCAS.2002.1173133.

## BIOGRAPHIES OF AUTHORS







**Mainak Saha**     is an Assistant Professor in the Department of Computer Science and Engineering at K L Deemed to be University, Hyderabad, and is currently pursuing a Ph.D. in Computer Science and Engineering at the National Institute of Technology Agartala. He earned his Master of Technology degree from Tripura University, Agartala, India. His research primarily focuses on AI, ML, computer networks, and cloud computing. His commitment to academic excellence and his expertise in these domains contribute significantly to the department's academic and research endeavors. He can be contacted at email: mainak.skms@gmail.com.







**Dr. M. Trinath Basu**     received his Ph. D. in Engineering (Department of Computer science and Engineering) at K L University, Vijayawada, India. He is working as an Associate Professor in the Department of Computer Science and Engineering, K L Deemed to be University, Hyderabad. His research works have been published in numerous peer reviewed journals. He also has been as an active reviewer for many peer reviewed journals. He can be contacted at email: tmiriyala@gmail.com.







**Dr. Arpita Gupta**     received her Ph.D. from NIT, Tiruchirappalli in Transfer Learning. She is working as an Associate Professor and HOD in the Department of Computer Science and Engineering, K L Deemed to be University, Hyderabad Aziz Nagar Campus. Her research works have been published in numerous peer reviewed journals. She also has been an active reviewer for many peer reviewed journals. She can be contacted at email: arpitagupta2993@gmail.com.







**K. Ashrith**     is a final-year engineering student at K L Deemed to be University, Hyderabad, where he is completing his Bachelor of Technology (B. Tech) degree. Currently, he is gaining valuable industry experience as an intern at OnePlus, a leading global technology company. He is dedicated to honing his technical skills and applying his academic knowledge in a professional setting, making him a promising future engineer in the field. He can be contacted at email: ashritkarnati31@gmail.com.









**Chevella Vamshi Vardhan Reddy**     is a skilled Software Developer, working in a hybrid on-site capacity. He holds a Bachelor of Technology (B. Tech) degree in Computer Science and Engineering from K L University, Hyderabad. With a strong foundation in software development, he has demonstrated expertise in designing, implementing, and optimizing software solutions. His educational background and professional experience equip him with the technical skills and knowledge to contribute effectively to various software development projects. He can be contacted at email: Vamshivardhan031@gmail.com.



**Shashanth Reddy**     holds a Bachelor of Technology (B. Tech) degree in Computer Science and Engineering from K L University, Hyderabad. With a solid foundation in software development, he has demonstrated expertise in designing, implementing, and optimizing software solutions. Now preparing to pursue a master's degree, he aims to deepen his expertise and broaden his career opportunities in the field of software development. He can be contacted at email: Shashanthreddy18@gmail.com.



**Rohith Reddy**     holds a B. Tech in Computer Science and Engineering from K L University, Hyderabad. With a strong background in software development, he has expertise in designing, implementing, and optimizing software solutions. His educational and professional experiences have equipped him with the skills needed to excel in the field. He is now pursuing a master's degree to further his expertise and contribute to innovative software development projects. He can be contacted at email: Prohith1231@gmail.com.