iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80868

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

SecureCrypt Desktop: A Conventional Encryption and Decryption System for Data Security

Mr. S.W. Koli[1], Sumit Kaulage[2], Shivam Chavan[3], Rohan Patil[4], Swapnil Khandekar[5]
[1]*Computer Science and Engineering SVERI's College of Engineering, Pandharpur, India*
[2, 3, 4, 5]*Undergraduate Student, Computer Science and Engineering SVERI's College of Engineering, Pandharpur, India*

Abstract: ***In the era of digital transformation, ensuring data confidentiality and integrity has become a critical requirement across various domains such as finance, healthcare, and communication systems. This paper presents SecureCrypt Desktop, a system designed to implement and analyze conventional encryption and decryption algorithms for secure data transmission and storage. The system incorporates widely used cryptographic algorithms including AES, DES, Blowfish, RC4, and RSA.***
The proposed system provides a user-friendly interface for encrypting and decrypting data while evaluating algorithm performance based on execution time, memory usage, and
accuracy. Experimental results demonstrate that AES offers an optimal balance between
security and efficiency, whereas RC4 provides faster execution with relatively lower security strength. The system also ensures 100% data integrity during encryption and decryption processes.
The study highlights the continued relevance of conventional cryptographic techniques in modern cybersecurity applications and provides a scalable framework for secure data handling. The proposed solution can be effectively applied in real-world systems requiring secure communication and data protection.

I. INTRODUCTION

The rapid expansion of digital technologies and internet-based services has significantly increased the volume of data being transmitted and stored across various platforms. From financial transactions and healthcare records to personal communications, sensitive information is continuously exchanged over networks. This growing dependence on digital systems has made data security a critical concern, as cyber threats such as unauthorized access, data breaches, and interception attacks continue to evolve in complexity and frequency. Ensuring the confidentiality, integrity, and authenticity of data has therefore become essential in modern computing environments.

Encryption is one of the most effective techniques used to protect sensitive data from unauthorized access. It involves transforming readable data, known as plaintext, into an unreadable format called ciphertext using cryptographic algorithms and keys. Only authorized users with the correct key can decrypt the data back into its original form.

Conventional encryption algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish, RC4, and RSA have been widely adopted in various applications due to their proven effectiveness in securing information.

Among these algorithms, AES is considered the most secure and efficient symmetric encryption standard and is widely used in government and commercial applications. DES, although historically significant, has become less secure due to its shorter key length. Blowfish offers flexibility and strong security, while RC4 provides fast encryption but suffers from known vulnerabilities. RSA, an asymmetric encryption algorithm, is primarily used for secure key exchange and digital signatures. Each algorithm has its own strengths and limitations, making it important to evaluate them based on performance and security requirements.

Despite the availability of these encryption techniques, there is a lack of integrated platforms that allow users to implement, analyze, and compare multiple algorithms within a single system. Existing tools often focus on individual algorithms and do not provide comprehensive insights into performance metrics such as execution time, memory usage, and accuracy.

Additionally, many systems are complex and not user-friendly, making it difficult for students, researchers, and developers to understand and apply encryption techniques effectively.

To address these challenges, this paper presents SecureCrypt Desktop, a comprehensive system that integrates multiple conventional encryption and decryption algorithms into a unified platform. The system provides a user-friendly interface for secure data processing and enables real-time performance evaluation of different algorithms. By combining usability, efficiency, and strong cryptographic techniques, the proposed system aims to enhance data
security while providing valuable insights into the behavior and performance of various encryption methods in practical scenarios.

©IJRASET: All Rights are Reserved

II. LITERATURE REVIEW

Cryptography plays a fundamental role in securing digital communication and protecting sensitive information from unauthorized access. Conventional encryption algorithms such as AES, DES, Blowfish, RC4, and RSA have been widely studied and implemented in various security systems. These algorithms differ in terms of security strength, computational efficiency, and applicability. Previous research highlights that the choice of encryption technique depends on factors such as data sensitivity, system performance, and resource constraints.

The Advanced Encryption Standard (AES) has emerged as the most widely accepted symmetric encryption algorithm due to its high security and efficiency. It is extensively used in modern applications including secure communication protocols, cloud storage, and financial systems. In contrast, the Data Encryption Standard (DES), once a popular algorithm, is now considered insecure due to its small key size and vulnerability to brute-force attacks.

Comparative studies consistently demonstrate that AES outperforms DES in both security and performance.

Blowfish and RC4 are also important symmetric encryption algorithms explored in literature. Blowfish is known for its flexibility and strong encryption capabilities with variable key lengths, making it suitable for applications requiring enhanced security. RC4, being a stream cipher, offers high-speed encryption and simplicity of implementation. However, several studies have identified vulnerabilities in RC4, which limits its use in modern secure systems. As a result, RC4 is generally recommended only for low-security applications.

Asymmetric encryption algorithms such as RSA are widely used for secure key exchange and authentication. Research suggests that hybrid encryption techniques, which combine symmetric and asymmetric algorithms, provide improved security by leveraging the strengths of both approaches. Additionally, recent studies emphasize the importance of evaluating encryption algorithms based on performance metrics such as execution time, memory usage, and accuracy. However, many existing systems lack integrated platforms for comparative analysis, highlighting the need for solutions like SecureCrypt Desktop that provide both functionality and performance evaluation in a unified environment.

III. PROBLEM STATEMENT

Despite advancements in cryptography, several challenges remain in implementing secure and efficient encryption systems:

1) Lack of integrated platforms supporting multiple encryption algorithms
2) Difficulty in comparing algorithm performance in real-time
3) Trade-off between security strength and computational efficiency
4) Complexity in key management and encryption processes
5) Limited user-friendly tools for understanding encryption mechanisms

These challenges necessitate the development of a system that can efficiently implement and evaluate multiple encryption techniques while ensuring ease of use and high security.

IV. PROPOSED SYSTEM

The proposed system, SecureCrypt Desktop, is a comprehensive encryption and decryption platform designed to provide secure data handling using conventional cryptographic
algorithms.

Key Features

1) Support for multiple algorithms (AES, DES, Blowfish, RC4, RSA)
2) Real-time encryption and decryption
3) Performance analysis (time, memory, accuracy)
4) User-friendly interface
5) Secure key generation and management

The system allows users to input data, select an encryption algorithm, generate keys, and
perform encryption and decryption operations. It also provides performance insights to help users understand the efficiency and security of different algorithms.

V. METHODOLOGY

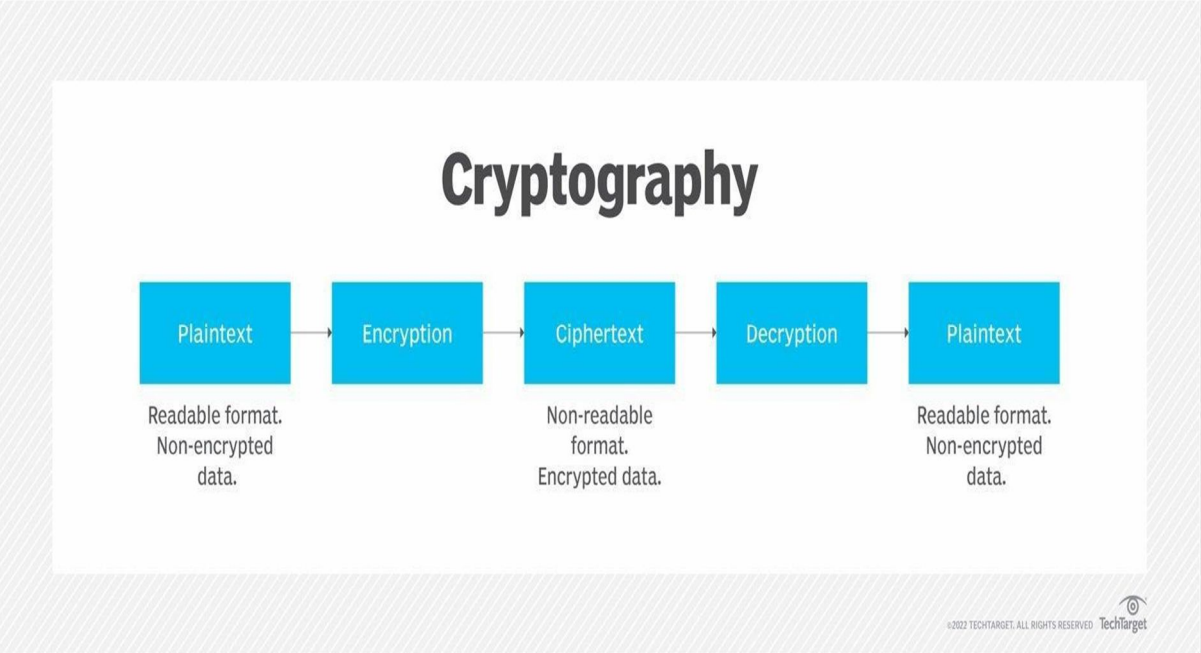
The proposed system, SecureCrypt Desktop, follows a structured methodology to ensure secure data encryption, efficient processing, and accurate decryption. The methodology is designed to provide a clear workflow from user input to final output while maintaining data confidentiality and integrity.

The process begins with data input, where the user provides plaintext data or uploads a file for encryption. The system accepts ultiple input formats and ensures that the data is preprocessed to remove inconsistencies or unsupported characters. This preprocessing step improves encryption accuracy and system performance.

In the next phase, the user selects an appropriate encryption algorithm such as AES, DES, Blowfish, RC4, or RSA based on security and performance requirements. The system then generates or accepts a cryptographic key, which is essential for both encryption and decryption. Proper key handling ensures that only authorized users can access the encrypted data.

Once the algorithm and key are selected, the system performs the encryption process, where plaintext is converted into ciphertext using the chosen algorithm. The encrypted data is then displayed or stored securely. The system also records performance metrics such as encryption time and memory usage during this stage.

Finally, the decryption process is carried out, where the ciphertext is converted back into plaintext using the same key. The system verifies the accuracy of the decrypted data by comparing it with the original input. Additionally, performance evaluation is conducted to analyze algorithm efficiency, enabling users to compare different encryption techniques.



VI. SYSTEM ARCHITECTURE

The system architecture of SecureCrypt Desktop is designed using a modular and layered approach to ensure scalability, flexibility, and efficient execution of encryption and decryption processes. The architecture separates different functionalities into independent modules, allowing better maintainability and future enhancements. This structured design ensures smooth data flow from input to output while maintaining high security and performance.

At the top layer, the User Interface (UI) Module provides an interactive platform for users to input plaintext data or upload files, select encryption algorithms, and view results. The

interface is designed to be intuitive and user-friendly, enabling both technical and non-technical users to operate the system efficiently. It acts as the entry point for all user interactions within the system.

The Application Logic Layer acts as the core controller of the system, managing the workflow and coordinating communication between different modules. It validates user inputs, processes algorithm selection, and ensures proper execution of encryption and decryption operations. This layer also handles error management and maintains the overall system flow.

The Encryption Module is responsible for converting plaintext into ciphertext using selected algorithms such as AES, DES, Blowfish, RC4, or RSA. Along with this, the Key Management Module generates, stores, and validates cryptographic keys securely. Proper key handling is critical to ensure that only authorized users can decrypt the data, thereby maintaining confidentiality and preventing unauthorized access.

The Decryption Module performs the reverse operation by converting ciphertext back into its original plaintext form using the appropriate key. This ensures data integrity and correctness.

Additionally, the Performance Analysis Module evaluates key metrics such as encryption time, decryption time, and memory usage, allowing users to compare the efficiency of different algorithms.

Finally, the Data Storage and Output Module is responsible for storing encrypted data and displaying results to the user. The architecture ensures secure data handling, smooth interaction between modules, and reliable system performance. The modular design also allows future integration of advanced features such as hybrid encryption, cloud deployment, and real-time secure communication systems.

VII. THE SYSTEM IMPLEMENTATION INVOLVES MULTIPLE TECHNOLOGIES

Frontend: HTML, CSS, JavaScript / React.js Backend: Python (Flask / FastAPI)

Libraries: PyCryptodome, NumPy, Pandas

Database: SQLite / MongoDB (for storing encrypted data and logs) Authentication: Basic Login System / JWT (optional for security) Deployment: Local Server / AWS EC2 / Render

The encryption engine executes multiple cryptographic algorithms such as AES, DES, Blowfish, RC4, and RSA efficiently, enabling secure data processing. The key management module ensures safe generation and handling of cryptographic keys, maintaining data confidentiality. The system supports real-time encryption and decryption with performance tracking. The dashboard provides visual insights into algorithm efficiency using metrics such as execution time, memory usage, and accuracy through charts and graphs.

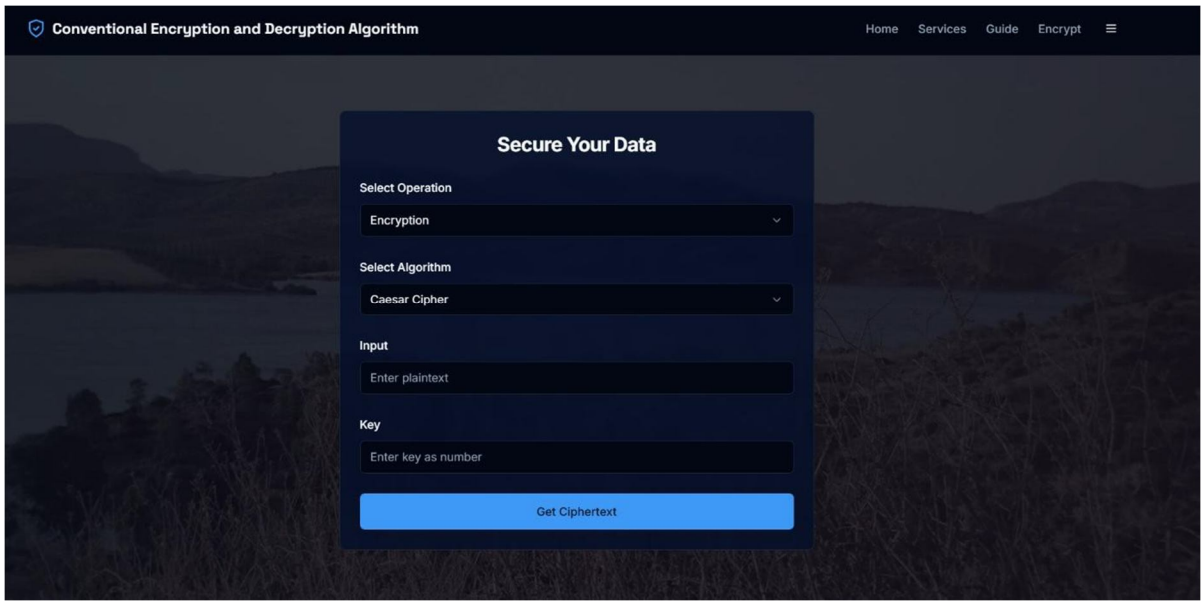
VIII. RESULTS AND DISCUSSION

The performance of SecureCrypt Desktop was evaluated using encryption algorithms such as AES, DES, Blowfish, and RC4 based on metrics like encryption time, decryption time, memory usage, and accuracy. All algorithms achieved 100% accuracy, confirming correct encryption and decryption operations.

Among the algorithms, RC4 showed the fastest execution time, while AES provided the best balance between security and performance, making it suitable for practical applications. DES was found to be less secure due to its shorter key length, and Blowfish, although secure, required slightly higher execution time.

Overall, the results demonstrate that conventional encryption algorithms are effective for secure data processing, and the system helps users choose appropriate algorithms based on performance and security requirements.

Additionally, the system provides real-time performance analysis through a dashboard, allowing users to visualize and compare algorithm efficiency using metrics such as execution time and memory usage, thereby enhancing usability and decision-making.



IX. ADVANTAGES OF THE SYSTEM

The SecureCrypt Desktop system offers several advantages that make it effective for secure data handling and analysis. It provides strong data confidentiality by implementing well-established encryption algorithms such as AES, DES, Blowfish, RC4, and RSA. The system supports multiple algorithms within a single platform, allowing users to select the most suitable method based on their requirements.

Another key advantage is its user-friendly interface, which enables both technical and non-technical users to perform encryption and decryption operations بسهولة and efficiently. The system also ensures accurate results, achieving 100% correctness in encryption and decryption processes.

Additionally, the system includes a performance analysis feature, which allows users to compare algorithms based on execution time, memory usage, and efficiency. This helps in better decision-making while selecting encryption techniques. The modular design of the system ensures scalability and flexibility, making it easy to integrate future enhancements such as hybrid encryption and cloud-based deployment.

Overall, the system provides a balance between security, performance, and usability, making it suitable for both academic and practical cybersecurity applications.

X. LIMITATIONS

Despite its effectiveness, the SecureCrypt Desktop system has certain limitations. The implementation of multiple encryption algorithms can lead to higher computational overhead, especially when processing large datasets or files, which may affect system performance on low-end devices.

Some algorithms used in the system, such as RC4 and DES, have known security vulnerabilities and are not recommended for highly sensitive applications. Additionally, the system relies on proper key management, and any compromise or mismanagement of keys can lead to security risks.

The current system is primarily designed for standalone or small-scale use, and it may have limited scalability for real-time or large-scale distributed environments. Furthermore, the absence of advanced features such as automated key rotation or hardware-based security modules may restrict its use in enterprise-level security systems.

Overall, while the system is effective for learning, analysis, and moderate security applications, these limitations highlight areas for future improvement and enhancement.

.

XI. FUTURE SCOPE

The SecureCrypt Desktop system can be further enhanced in several ways to improve its functionality, security, and scalability. One major improvement is the implementation of hybrid encryption techniques, combining symmetric algorithms like AES with asymmetric algorithms such as RSA to achieve both high security and efficient key exchange.

The system can also be extended to support cloud-based deployment, enabling secure data encryption and decryption in distributed environments. Integration with real-time communication systems can allow secure transmission of data over networks, making the system more practical for real-world applications.

Another important enhancement is the incorporation of advanced key management mechanisms, such as automated key rotation, secure key storage, and integration with hardware security modules (HSMs). This would significantly improve the overall security of the system.

Additionally, the system can be expanded to support IoT devices and mobile platforms, ensuring secure data handling across emerging technologies. Future work may also include the implementation of post-quantum cryptography algorithms to make the system resilient against future quantum computing threats.

Overall, these enhancements can transform the system into a more robust, scalable, and industry-ready solution for modern cybersecurity applications.

XII. CONCLUSION

The SecureCrypt Desktop system successfully demonstrates the implementation and analysis of conventional encryption and decryption algorithms for secure data transmission and storage. By integrating algorithms such as AES, DES, Blowfish, RC4, and RSA into a single platform, the system ensures data confidentiality, integrity, and efficient processing.

The experimental results confirm that all algorithms achieve accurate encryption and decryption, while performance analysis highlights the trade-offs between speed and security.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Among the evaluated algorithms, AES emerges as the most suitable choice for practical applications due to its strong security and balanced performance.

The system also provides a user-friendly interface and real-time performance insights, making it useful for both academic learning and practical cybersecurity applications.

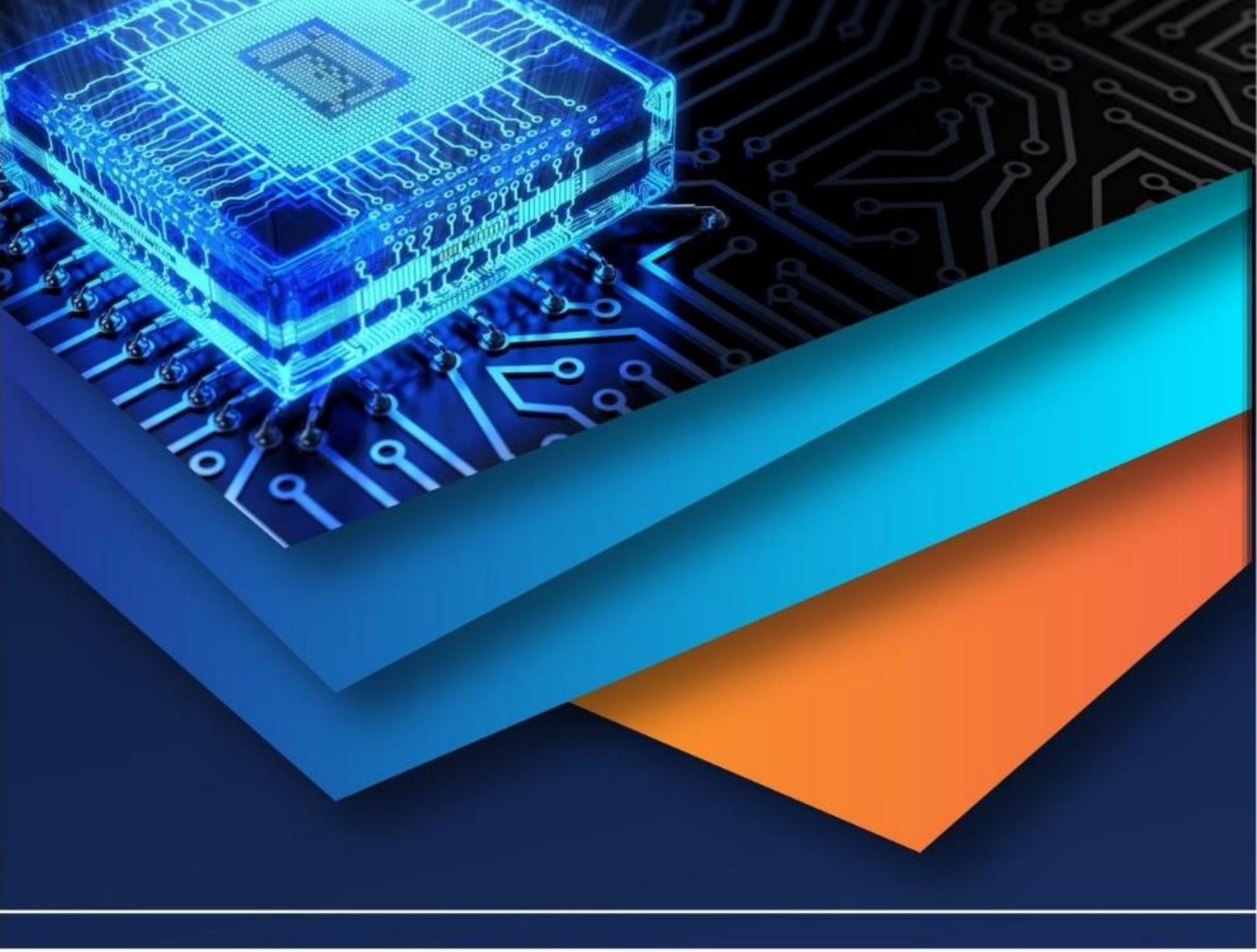
Although there are certain limitations, the proposed system establishes a strong foundation for secure data handling and can be further enhanced with advanced features such as hybrid encryption and cloud integration.

Overall, the project highlights the continued relevance of conventional cryptographic techniques in modern security systems and contributes toward building efficient and reliable solutions for data protection.

REFERENCES

[1] Research papers on conventional encryption and decryption algorithms
[2] Studies on symmetric and asymmetric cryptographic techniques (AES, DES, RSA, Blowfish, RC4)
[3] Documentation of cryptographic libraries (PyCryptodome, OpenSSL)
[4] Research on data security and cryptography in cybersecurity systems
[5] Articles on encryption performance analysis and optimization techniques
[6] Studies on key management and secure data transmission
[7] Journals on information security and cryptographic advancements
[8] Web security standards and best practices for data protection

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)