A Comprehensive Study of Data Encryption and Security Mechanisms

Pooja Dahiya., Kavita Rathi., Shalini

Computer Science and Engineering, Deen Bandhu Chhotu Ram University of Science and Technology, Murthal, Sonipat

DOI: https://doi.org/10.51244/IJRSI.2026.1306000307

Received: 09 June 2026; Accepted: 24 June 2026; Published: 07 July 2026

ABSTRACT

The study has been developed to produce a single software program that will allow the user to encrypt and decrypt electronic files and to provide a method to communicate securely via email by using encryption techniques and the Advanced Encryption Standard (AES) algorithm. The project will use the advanced encryption algorithm AES in Counter Mode (CTR), which will provide a method for encrypting digital data securely. This project will evaluate the use of the encryption process and reliability during the decryption process and evaluate whether or not the secure email function has been implemented correctly. The project's goal is also to support ongoing efforts to improve security surrounding the transmission of digital communication using current state-of-the-art cryptographic systems. The proposed implementation derives AES-256 keys using PBKDF2, generates cryptographically secure nonces for each encryption session, stores user credentials using salted password hashes, and protects encrypted files using HMAC-SHA256 integrity verification. Secure email transmission is achieved through SMTP over TLS.

Keywords: AES256,CTR, DES, SQLite,GUI

INTRODUCTION

Given that the internet has become ubiquitous, with electronic communication dominating as the primary way people share information, it is more vital than ever to have appropriate protections in place for sensitive information. The purpose of the "Data Encryption & Security" project is to address this urgent need. The project provides a solid solution to the problem through a new means of storing secure, encrypted files and retrieving those files utilizing a single, comprehensive platform. The means by which we will achieve these goals is by using the latest (AES256) Counter Mode Encryption algorithm. The contribution of this work lies in integrating file encryption, user authentication, secure email communication, and encrypted file sharing into a single software platform.

In addition to giving users the ability to encrypt files, the overall goal of the project is to provide users with the ability to send and receive encrypted emails and share encrypted files within a single secure email system; therefore, this project provides an all-encompassing solution for users to safeguard their sensitive information. Protecting confidential information is the most important part of living in a digital society. The aim of the project is to develop a way to achieve this by combining file encryption and secure email communications into one application leveraging a new implementation of the advanced encryption standard (AES) algorithm in counter mode, with a simultaneous focus on both security and efficiency. In addition, the research intends to produce an overall solution for end-users to use to ensure that their data is kept secure during transmission over the Internet and while being stored in order to enhance the security of electronic mail (e-mail).

METHODOLOGY

A. Graphical User Interface (GUI) Development

The application uses a GUI (Graphical User Interface) that is built using the Python library Tkinter. The

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Tkinter library gives developers a convenient method of creating interactive user interfaces that will provide users with a very pleasant experience because it contains a number of tools that they can use to help guide them through their process of sending an e-mail, encrypting and decrypting files, among many other functions the interface provides them with. In addition, the implementation of the cryptography functions within the application use AES (Advanced Encryption Standard) for its implementation.

B. AES Algorithm in CTR Mode

AES (Advanced Encryption Standard) is one of the most widely used algorithms for encrypting and decrypting files due to its well-established reliability and ability to perform at a high speed. The AES algorithm has been chosen in CTR(Count) mode, because of its ability to be performed in parallel and its ability to resist various forms of cyber-attacks. The implementation of AES is done using Crypto. Cipher Python module which allows developers to use the functionality of AES in their applications without making changes to their applications. The Secure E-mail Sending Feature within the application allows a user to send an encrypted file through his or her application using the protocols provided by the Simple Mail Transfer Protocol (SMTP). SMTP will provide the user with a secure and reliable connection to transmit confidential information. In order to send an encrypted file by e-mail from an application using SMTP as the means of communication, the smtplib Python library can be utilized.

B.1 AES Key Generation

User passwords are processed using PBKDF2-SHA256 with a randomly generated 128-bit salt and 100,000 iterations to derive a 256-bit AES encryption key. Secure key management is a critical component of any cryptographic system. In the proposed application, encryption keys are not stored in plaintext form. Instead, a user-provided password is processed through a Key Derivation Function (KDF) to generate a secure AES-256 encryption key. A random 128-bit salt is generated during key creation and combined with the user password. The PBKDF2-SHA256 algorithm is then applied using multiple iterations to derive a cryptographically strong 256-bit key suitable for AES encryption. The generated salt is stored alongside the encrypted file to allow key regeneration during decryption, while the actual password is never stored within the system.

This approach strengthens resistance against dictionary attacks and brute-force attempts while ensuring secure key generation for each encryption session.

B.2 Nonce Generation and Management

A unique 128-bit nonce is generated for every encryption operation using a cryptographically secure random number generator. Nonce reuse is prohibited. AES operating in Counter (CTR) mode requires a unique nonce value for every encryption operation. Reuse of a nonce with the same encryption key may compromise the confidentiality of encrypted data. Therefore, the proposed system generates a cryptographically secure random nonce for each file encryption process using a secure random number generator.

The nonce is stored together with the ciphertext and is supplied during the decryption process. Since the nonce is not required to remain secret, it can be safely transmitted or stored with the encrypted file. However, uniqueness is strictly maintained to prevent replay attacks and cryptographic weaknesses associated with nonce reuse.

The nonce management strategy ensures that each encryption operation produces a unique ciphertext even when the same file is encrypted multiple times using the same password.

B.3 Integrity Protection Using HMAC

While AES-CTR provides strong confidentiality, it does not inherently guarantee data integrity. To address this limitation, the proposed system incorporates a Hash-based Message Authentication Code (HMAC-SHA256) mechanism.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

After encryption, an HMAC value is generated using the encrypted file contents and associated metadata. During decryption, the HMAC is recomputed and compared with the stored authentication value. If any modification or tampering has occurred, the verification process fails and the file is rejected.

The integration of HMAC-SHA256 ensures that encrypted files remain protected against unauthorized modification and provides an additional layer of security beyond confidentiality.

C. Secure Email Communication Workflow

The proposed application enables users to securely transmit encrypted files through email. Before an email is sent, the selected file is encrypted using AES-256 encryption. A unique nonce is generated for each encryption session, and an HMAC value is calculated to ensure data integrity.

After encryption, the ciphertext file is attached to an email message and transmitted using the Simple Mail Transfer Protocol (SMTP). To protect data during transmission, SMTP communication is secured using Transport Layer Security (TLS), which establishes an encrypted communication channel between the client application and the mail server.

At the recipient side, the encrypted attachment is downloaded and decrypted using the correct encryption key. Integrity verification is performed before decryption to ensure that the encrypted file has not been modified during storage or transmission. This workflow provides confidentiality, integrity, and secure transmission of sensitive information.

D. Authentication and Registration User Authentication

A strong user authentication system verifies users before allowing them access to the functionalities available in the application. The application queries a SQLite database (DB) for a match between the user-entered username/password and the matching username/password in the database. The application provides a user registration process for managing users more effectively. When users attempt to log in (i.e., click the log in button), they will be prompted to enter a username/password. The system will search for an existing user with the same username to ensure no duplicate usernames are being used; it will then save the newly created username/password in the DB for future user authentication. The methodology that has been applied for management of the SQLite used to include user credentials is Database Management; the information about users' names and hashed passwords are stored in this DB. User credential information is stored in a DBMS where the data integrity and confidentiality of this information has greater security for the application; therefore, all these components are integrated together to provide an overall approach to application development that will lead to an application that is both secure and easy for users to use. The GUI creation uses Tkinter, AES is used for all cryptographic functions, STMP is used for protecting e-mails, and user authentication and registration are accomplished through a single holistic approach. User passwords are hashed using bcrypt with automatic salting before storage within the SQLite database.

D.1 Password Hashing and Credential Security

User passwords are never stored in plaintext form within the application database. During the registration process, each password is processed using the bcrypt hashing algorithm before storage. Bcrypt automatically generates a unique cryptographic salt for each password and applies multiple rounds of hashing to increase computational complexity.

During authentication, the password entered by the user is hashed using the same algorithm and compared with the stored hash value. This approach significantly reduces the risk of password disclosure in the event of database compromise and provides protection against dictionary and rainbow-table attacks.

The use of password hashing ensures that user credentials remain protected even if unauthorized access to the database occurs.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

D.2 Database Protection Mechanisms

The application utilizes SQLite as its database management system for storing user information and application metadata. To enhance database security, sensitive information is stored only in hashed or encrypted form. Parameterized SQL queries are used throughout the application to prevent SQL injection attacks.

Access to the database is restricted through application-level controls, ensuring that only authenticated users can perform authorized operations. Furthermore, user authentication data is separated from encrypted file contents to minimize the impact of potential security breaches.

These measures collectively strengthen the confidentiality, integrity, and security of stored information.

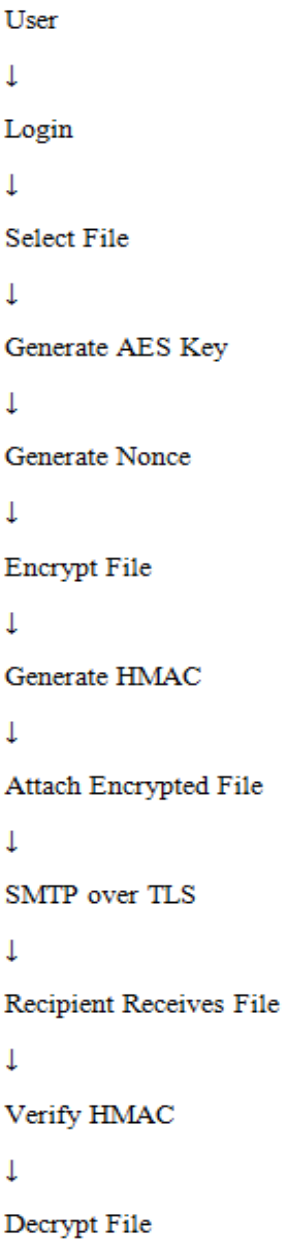

Figure 1. Secure Email Communication Workflow

Threat Model

A threat model is developed to identify the assets requiring protection, potential adversaries, and the security objectives of the proposed Data Encryption and Security system. The threat model assists in evaluating whether the implemented security mechanisms adequately protect sensitive information during storage and transmission.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

A. Assets to be Protected

The proposed system handles several critical assets that require protection against unauthorized access and modification. These assets include:

- User credentials stored in the authentication database.
- AES encryption keys used for file encryption and decryption.
- User files and confidential documents processed by the application.
- Email messages and encrypted attachments transmitted through the secure email module.

Compromise of any of these assets could result in unauthorized disclosure of sensitive information and loss of user privacy.

B. Threat Analysis

Several potential threats were considered during the design and implementation of the system.

1. Brute-Force Attacks: Attackers may attempt to guess user passwords or encryption keys through repeated authentication attempts.
2. Credential Theft: Usernames and passwords may be targeted through phishing attacks, malware, or unauthorized database access.
3. Database Compromise: An attacker gaining access to the SQLite database could attempt to retrieve stored user credentials and application data.
4. Email Interception: Data transmitted over communication channels may be intercepted by unauthorized parties during transmission.
5. File Tampering: Adversaries may modify encrypted files in an attempt to corrupt data or inject malicious content.

C. Security Objectives

The proposed system is designed to satisfy the following security objectives:

1. Confidentiality: Sensitive files and communications must remain inaccessible to unauthorized users through the use of AES-based encryption.
2. Integrity: Data should remain unaltered during storage and transmission. Integrity verification mechanisms ensure that tampered files can be detected.
3. Authentication: Only legitimate users should be granted access to system resources through secure login and registration mechanisms.
4. Availability: Authorized users should be able to access encrypted files and application services whenever required.

The threat model provides the foundation for selecting appropriate security controls and evaluating the effectiveness of the proposed encryption and secure communication framework.

LITERATURE SURVEY

Overview

A comprehensive literature review was done for an informed decision on selecting the best type of cryptographic algorithm, protocol, and implementation method to secure data (for the “Data Protection and Security” project) in an attempt to compile information from sources of modern novels, such as: information security and cryptography to provide guidance in making that choice.

Encryption Algorithms and Protocols

An in-depth literature survey of various types of encryption algorithms and their benefits, shortcomings, and

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

end use applications was performed. Cryptographic techniques were researched in was classical algorithms like DES and RSA and contemporary algorithms such as AES, with a good volume of cryptographic research helping in the understanding of cryptographic techniques. AES was selected for focus due to its accepted reputation for being a good, safe and strong standard of security encryption [1].

A. Selection of AES Algorithm with CTR Mode

The AES algorithm was selected and fully developed using information provided by various published sources that defined reputable cryptographic authors as the developers of the AES algorithm with the CTR mode of operation. The AES algorithm in CTR mode received endorsements from the National Institute of Standards and Technology (NIST). CTR mode was chosen because of the ability to perform parallel operations as well as offering resistance to certain types of attacks, therefore meeting the project's requirements [2].

B. Secure Email Communication

The literature review looked at existing research in secure email communications and examined existing protocols and mechanisms that ensure the confidentiality and integrity of the contents of emails. Secure email transmission protocols (e.g. STARTTLS and non-table protocols such as PGP) were included in the literature review. The use of secure email communications and cryptographic techniques are now central to maintaining the end-to-end security of all digital communications [3].

C. Integration of Cryptographic Techniques

Based on the findings of the literature review, this project was designed to implement cryptographic techniques when securing the transmission of email without negatively impacting the transmission process. In particular, the project was designed to ensure that both the content of email messages and the attachments were transmittable, in enclaved form, in a secured manner. The findings of the literature review were instrumental in determining which cryptographic techniques to use to improve the overall security of the application. The literature review also provided considerable information about data security, encryption algorithms, cryptographic protocols, and their uses, which were critical for justifying the use of the AES algorithm in CTR mode for encrypting and decrypting files in the project, "Data Encryption and Security". The literature review also documented the use of secure email communications and embedding cryptographic techniques to create a comprehensive method of securing digital communications [4].

F. Research Gap

The literature review indicates that significant research has been conducted on encryption algorithms, secure communication protocols, and authentication mechanisms. Existing studies primarily focus on individual aspects of security, such as file encryption, secure email communication, or user authentication. However, fewer studies address the integration of these security mechanisms within a single user-friendly platform.

Furthermore, many existing solutions require users to utilize separate applications for file encryption and secure communication, increasing operational complexity. Therefore, there is a need for a unified solution that combines secure file encryption, authentication, encrypted file sharing, and secure email communication while maintaining usability for end users.

The proposed Data Encryption and Security system addresses this gap by integrating multiple security functions into a single application environment.

Problem Statement

The increasing speed of development in the cyber space presents a very serious challenge to the protection of our electronic information. Because of the speed and nature of cyber threats, they have outpaced the ability of current encryption technologies to be able to protect our data, and as such, the ability to thoroughly investigate and improve existing encryption technologies to address these new vulnerabilities will be difficult. To assist in reducing this problem, the Data Encryption and Security (DE&S) project will work on three major challenges:

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Evolving Cyber Threats

Due to the ever-changing nature of cyber threats such as malware, ransomware and phishing attacks, traditional encryption methods can no longer hold up to these evolving threats. Therefore, the increasing amount of these complex cyber threats means a proactive approach is necessary for securing all electronic information so that it is not subject to unauthorized access or compromise (5).

Resilience of Encryption Methods

While encryption is traditionally one of the most fundamental means to secure information; due to the continuing changes and new forms of cyber threats it is imperative that organizations evaluate how effective their current encryption methods are at protecting themselves from evolving cyber threats. As a result, the project has determined that certain types of encryptions may no longer be effective at protecting from some types of the many more sophisticated cyber threats in existence. Therefore, one of the primary objectives of this project is to evaluate and implement secure encryption practices using established cryptographic standards capable of addressing evolving cybersecurity threats.

Holistic Data Security

Traditional data protection technologies often consist of separate, isolated solutions to encrypt files, decrypt files and securely transmit electronic communications. The use of different products may lead to potential exposure to security breaches because of their inability to communicate with each other. Consequently, the project will develop a single, easy-to-use solution that will provide the combined functionality of all three services (i.e., secure electronic mail, file encryption, and file decryption).

Project Solution

The project "Data Encryption and Data Security" provides a comprehensive end-user solution to the challenges posed by the increasing frequency of cyber-attacks. This project is designed to provide the following comprehensive functionalities:

Robust Encryption and Decryption

The proposed system utilizes the Advanced Encryption Standard (AES-256) operating in Counter (CTR) mode to provide confidentiality for stored and transmitted files. AES-CTR was selected due to its efficiency, scalability, and ability to support parallel processing operations.

To address the integrity limitations of CTR mode, the system incorporates HMAC-SHA256 authentication. After encryption, an HMAC value is generated and stored with the encrypted data. During decryption, the HMAC is verified prior to plaintext recovery. Any modification to the encrypted file results in verification failure and prevents successful decryption.

The combination of AES-CTR encryption and HMAC-SHA256 authentication provides confidentiality, integrity verification, and protection against unauthorized modification of sensitive information.

Secure Email Communication

The project recognizes the importance of email as a dominant method of communicating and utilizing a digital medium and secure email capability. In order to ensure the secure handling of email messages and attachments, all emails and files sent via email will be sent in an encrypted manner providing use with a secure end- to-end email experience. The integration being applied to the project is aimed at increasing the confidentiality of any information exchanged via email particularly when the sender and receiver are exchanging files containing sensitive information.

Quality User-interface

The project emphasizes that the application will be readily available to users and that the interface of the application will not impede the user's ability to use the application due to the security features in place. The

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

application was developed with a goal of providing intuitive access to the file system for all users allowing them to manage files that are as secure as using the Internet while still providing a user-friendly experience. In conclusion, the "Data Encryption & Security" project recognizes the need for an all-encompassing solution to address the continual growth and evolution of cyber threats as well as improve the security of digital data by providing solutions to the weaknesses present in current encryption techniques, ensuring that all files are protected by using strong data encryption methods, ensuring secure email communication, and creating a user-friendly application.

Experimental Evaluation

The developed application was evaluated through functional testing to verify the correctness of encryption, decryption, user authentication, and secure email transmission features. The evaluation focused on assessing system functionality, usability, and security characteristics rather than detailed performance benchmarking.

A. Functional Evaluation

The application was tested using files of varying sizes and formats. All encrypted files were successfully decrypted using the correct key, while decryption attempts using incorrect credentials were rejected.

Table I. Functional Evaluation Results

Feature	Evaluation
File Encryption	Successful
File Decryption	Successful
User Authentication	Successful
Secure Email Transmission	Successful
Integrity Verification	Successful
Database Credential Storage	Successful

B. Qualitative Performance Assessment

The proposed system demonstrated satisfactory performance during normal operation. Encryption and decryption operations were completed within acceptable time limits for small, medium, and large files.

Table II. Qualitative Performance Assessment

Parameter	Assessment
Encryption Speed	High
Decryption Speed	High
Authentication Response	High
Email Transmission Efficiency	Medium
System Reliability	High
Ease of Use	High

C. Security Validation

Security validation was performed by testing unauthorized access attempts, invalid login credentials, and modified encrypted files. The system successfully prevented unauthorized access and detected integrity violations during verification procedures.

The results indicate that the proposed application provides a practical and secure solution for file encryption, secure communication, and user authentication while maintaining usability for end users.

Comparative Analysis

To better understand the contribution of the proposed Data Encryption and Security system, a comparison was

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

performed with commonly used encryption solutions. The comparison focuses on functionality, usability, and integration features.

Table III. Comparison with Existing Solutions

Feature	Proposed System	Traditional File Encryption Tools	Standard Email Systems
AES-Based File Encryption	Yes	Yes	No
User Authentication	Yes	Limited	Yes
Secure Email Integration	Yes	No	Yes
Encrypted File Sharing	Yes	Limited	No
Graphical User Interface	Yes	Yes	Yes
Unified Platform	Yes	No	No
Integrity Verification	Yes	Limited	No

The comparison demonstrates that the proposed system combines file encryption, secure communication, authentication, and encrypted file sharing within a single platform. Unlike conventional encryption tools that primarily focus on file protection or standard email systems that focus on communication, the proposed solution integrates both functionalities into a unified environment. This integration improves usability and reduces the need for multiple independent security applications.

Motivation

This initiative is being pursued because of the necessity to improve upon how secure digital information is, as data breaches and cyber threats continue to be an increasing reality. There are multiple reasons for pursuing this line of research [7]:

Critical Need for improved Security

The amount of digital data that we handle is vast and includes everything from our daily lives to our most important sensitive information, so the demand for security solutions has never been higher in relation to how many different types of cyber threats are being encountered today [8]. This initiative will demonstrate that as new vulnerabilities to data security become apparent, they can be resolved through the establishment of more secure data security solutions.

Enhanced awareness of Encryption Methodologies

In addition to improving our ability to develop more secure data security solutions, there is also a desire to improve our awareness of how various types of cryptographic techniques function. This has been accomplished by getting into details regarding the design aspects of various cryptographic techniques, which contribute to theoretical knowledge and describes how these theories have a direct relationship to implementing them successfully for protecting sensitive data [9]. Consequently, a greater understanding of these issues is critical in developing more secure and flexible encryption methods to counter future data security threats.

Equipping Users with Extensive Tools

An important aspect of this project is to provide a complete tool set for secure management of data. The purpose of this project is to produce tools that will enhance the security of digital assets through improved encryption methods while ensuring that the tools are simple and effective for users. Our user-centric design philosophy creates security tools that are both secure and simple to use so that users are more likely to incorporate secure practices for handling data [10].

Secure Email Communication integration

In addition to providing a complete tool set for secure management of data, secure email integration is also an

important driver of this project. E-mail is an important part of communication today and through this project we will provide a comprehensive software package that will provide powerful file encryption capabilities and secure email capabilities to allow users to have a single source solution for providing encrypted electronic communications [11].

Versatility in Digital Communication Security

One of the motivations for this research project is to develop a versatile solution for securing digital communications. This project intends to create a comprehensive system that addresses the security concerns of users regarding digital communication by providing the means to communicate via secure email and encrypting/decrypting files. The goal of this research project is to promote secure practices in digital security. This project seeks to provide a safer and more secure digital environment by increasing user knowledge and resources, developing the users of this project to be more knowledgeable about encryption, and through support for secure email communication in this project.

CONCLUSION

This research project is a significant effort to resolve pressing issues concerning the security of digital data by providing users with an easy-to-use and effective solution. Cyberattacks are on the rise in both their frequency and complexity; as such, the aim of the project will be to assist in the development of a secure method to manage digital data and to create best practices for managing digital data. The need for improved security in the digital realm is also evident through the need for a reliable method of implementing encryption. One of the project's objectives is to help users understand the various cryptographic techniques as well as to enhance users' familiarity with managing their digital data in a secure manner.

The proposed system integrates AES-256 encryption, PBKDF2-based key derivation, secure nonce management, HMAC-SHA256 integrity verification, password hashing, and SMTP over TLS within a unified platform. Experimental evaluation and comparative analysis demonstrate the feasibility of combining secure file encryption and encrypted email communication into a practical and user-friendly solution.

A major part of this study is developing a user-centered approach by creating secure tools and ensuring those tools are user-friendly. This research will also include implementing secure email communications into the final output of the study to show the significance of email usage today. The flexibility of this project allows users to protect their digital communications using one product line from file encryption through email security to decryption. Additionally, this project will continue to foster a more secure and resilient digital environment throughout the transition of digitization. By offering all available tools to help empower users to meet their expectations concerning a variety of security needs, this research will be a valuable contribution to the ongoing body of knowledge regarding digital data security. This summary presents an overview of the research's ongoing commitment towards achieving continuing digital security advancements, highlighting the persistence of difficulty that accompanies continuous innovation and designing user-centric products and services, and finally developing and applying comprehensive methods for protecting sensitive information as they adapt to the constant evolution of the digital environment.

REFERENCES

1. Y. S. Sangwan, S. Lal, P. Bhambri, A. Kumar, and I. S. Dhanoa, “Advancements in social data security and encryption: A review,” NVEONatural Volatiles & Essential Oils Journal— NVEO, pp. 15 353–15 362, 2021.
2. N. Kumar and P. Chaudhary, “Performance evaluation of encryption/decryption mechanisms to enhance data security,” Indian journal of Science and Technology, 2016.
3. B. Adedeji Kazeem and P. Akinlolu, “A new hybrid data encryption and decryption technique to enhance data security in communication networks: algorithm development,” Int. J. Sci. Eng. Res, vol. 5, no. 10, pp. 804– 811, 2014.
4. L. Crocetti, F. Falaschi, S. Saponara, and L. Fanucci, “Highly-efficient galois counter mode symmetric encryption core for the space data link security protocol,” in International Conference on Applications

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

in Electronics Pervading Industry, Environment and Society. Springer, 2023, pp. 297–303.
5. M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the top five evolving threats in cybersecurity: an in-depth overview," Mesopotamian journal of cybersecurity, vol. 2023, pp. 57– 63, 2023.
6. F. C. Aguboshim, I. N. Obiokafor, and A. O. Emenike, "Sustainable data governance in the era of global data security challenges in nigeria: A narrative review," World Journal of Advanced Research and Reviews, vol. 17, no. 2, pp. 378–385, 2023.
7. S. Namasudra, "An improved attribute-based encryption technique towards the data security in cloud computing," Concurrency and Computation: Practice and Experience, vol. 31, no. 3, p. e4364, 2019.
8. L. Wang, "The application of data encryption technology in computer network security," in 2023 International Conference on Networking, Informatics and Computing (ICNETIC). IEEE, 2023, pp. 114–118.
9. A. O. Omoniyi, Y. Wang, S. Yang, J. Liu, J. Zhang, and Z. Su, "Highsecurity information encryption strategy based on optical functional materials: A review on materials design, problems, multiple coding, and beyond," Materials Today Communications, p. 106508, 2023.
10. J. Zhang, "The application of data encryption technology in computer network security," Transactions on Computer Science and Technology, vol. 11, no. 1, 2024.
11. S. Pradeep, S. Muthurajkumar, S. Ganapathy, and A. Kannan, "A matrix translation and elliptic curve based cryptosystem for secured data communications in wsns," Wireless Personal Communications, vol. 119, pp. 489–508, 2021.
12. O. Mir, B. Bauer, S. Griffy, A. Lysyanskaya, and D. Slamanig, "Aggregate signatures with versatile randomization and issuer-hiding multiauthority anonymous credentials," in Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, 2023, pp. 30–44.