iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.83060

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 V May 2026- Available at www.ijraset.com

Secured Data Transaction by Using ECC Based on Cryptography

R.Lalitha[1], P. Bindhu Priya[2]
[1]*MCA Final Year Student,* [2]*Assistant professor, Master of Computer Applications, Sanketika Vidya Parishad Engineering College, Vishakhapatnam, Andhra Pradesh, India*

Abstract: ***Security and privacy in digital communication have become major concerns in modern network systems, affecting confidentiality and data integrity. This project develops a secure data transmission system using a Hybrid Cryptographic Algorithm that combines Machine Learning-inspired security concepts with advanced cryptographic techniques. Elliptic Curve Cryptography (ECC) is used for secure key exchange, RSA is applied for authentication through digital signatures, and AES-256-GCM is used for fast and secure message encryption. The system enables users to securely register, login, send encrypted messages, and decrypt received messages through a web-based platform. Additionally, automatic message expiry functionality is implemented to enhance privacy and prevent unauthorized access after viewing. The platform also provides secure session handling and database management using PHP, MySQL, and OpenSSL libraries for efficient and reliable communication between users.***

Keywords: Elliptic Curve Cryptography (ECC), RSA, AES-256-GCM, Hybrid Cryptography, Secure Data Transmission, Encryption, Decryption, Digital Signature, Authentication, Confidentiality, OpenSSL, PHP, MySQL, Secure Communication System

I. INTRODUCTION

Secure data transmission has become a critical requirement in modern communication systems, affecting data confidentiality, integrity, and user privacy. This project presents a secure communication system developed using Hybrid Cryptographic techniques to ensure safe and reliable message transmission between users. The system combines Elliptic Curve Cryptography (ECC), RSA, and AES-256-GCM algorithms to provide enhanced security during data exchange. ECC is used for secure key exchange, RSA is applied for authentication and digital signature verification, and AES-256-GCM is used for fast and secure message encryption and decryption. The platform also includes secure user authentication, role-based sender and receiver communication, automatic message expiry after viewing, and database management using PHP and MySQL. With a user-friendly web interface and efficient encryption mechanisms, the system helps protect sensitive information from unauthorized access and cyber threats while ensuring secure and reliable real-time communication.

II. LITERATURE SURVEY

Recent studies highlight the growing importance of Hybrid Cryptographic techniques for ensuring secure data transmission and protecting sensitive information in modern communication systems. Researchers have shown that combining cryptographic algorithms such as ECC, RSA, and AES provides stronger security compared to using individual encryption methods alone[1][3][4]. Studies on Elliptic Curve Cryptography (ECC) demonstrate its efficiency in secure key exchange with smaller key sizes and improved performance[1][2]. Research on RSA-based digital signatures highlights its role in authentication and message verification, ensuring that transmitted data originates from trusted users[3]. Additionally, AES-256-GCM has proven highly effective for fast and secure data encryption while maintaining confidentiality and integrity during communication. Modern web-based secure messaging systems also emphasize features such as secure authentication, encrypted message storage, automatic message expiry, and efficient database management for enhanced privacy protection[6][7][8]. These advancements collectively form the foundation for developing intelligent and reliable secure communication systems that support confidentiality, authentication, integrity, and real-time protected data exchange.

III. CHALLENGES

Implementing a secure data transmission system using Hybrid Cryptographic algorithms involves several technical and practical challenges, mainly related to encryption complexity, key management, and secure system integration[6][7].

One major challenge is securely generating, storing, and managing cryptographic keys, as improper key handling can compromise the entire communication process[12][13]. Ensuring secure and efficient encryption also requires selecting suitable cryptographic algorithms that provide strong security while maintaining good system performance[6][14]. In hybrid cryptography, combining ECC, RSA, and AES-256-GCM requires careful coordination between symmetric and asymmetric encryption techniques to avoid vulnerabilities and ensure reliable data transmission[1][3][4]. Additionally, protecting sensitive user information and preventing unauthorized access remain major concerns in secure communication systems[8][5].

Another challenge is integrating encryption, authentication, message verification, database management, and automatic message expiry functionalities into a single user-friendly web application[6][9]. The system must efficiently handle real-time encryption and decryption processes without causing noticeable delays in communication[4][5]. Maintaining confidentiality, integrity, and authentication throughout the message transmission process requires continuous monitoring and secure session handling[7][8]. Organizations and developers may also face difficulties in configuring cryptographic libraries, managing secure databases, and ensuring compatibility between backend technologies such as PHP, MySQL, and OpenSSL[9][10][11]. Furthermore, ensuring scalability, maintaining strong security against evolving cyber threats, and providing smooth interaction between the frontend interface and backend cryptographic modules require proper system design, testing, and continuous maintenance.

IV. PROPOSED METHODOLOGY

The proposed methodology for this project uses Hybrid Cryptographic techniques to provide secure and reliable data transmission between users[6][12]. The system combines Elliptic Curve Cryptography (ECC), RSA, and AES-256-GCM algorithms to achieve confidentiality, authentication, and integrity during communication[1][3]. ECC is used for secure key exchange between sender and receiver, RSA is applied for digital signature verification and authentication, and AES-256-GCM is used for fast and secure message encryption and decryption[1][2][3][5]. The system also includes user registration, secure login, sender and receiver modules, secure session handling, and automatic message expiry after viewing to enhance privacy protection[6][8]. All encrypted messages, user details, timestamps, and message status information are securely stored in a MySQL database[10][11]. A PHP-based web application interface is developed to enable safe, efficient, and real-time secure communication between users.

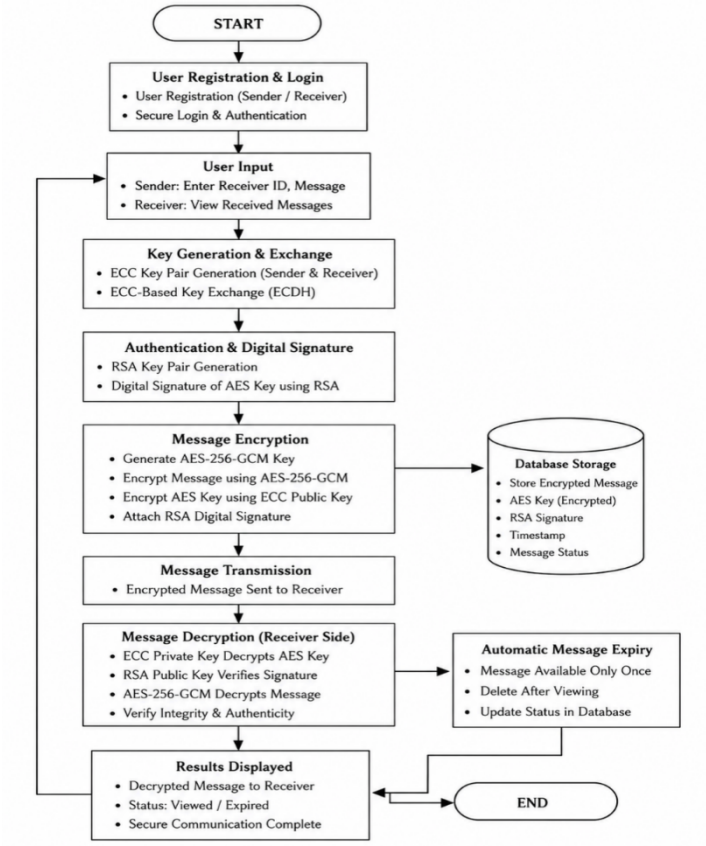


Figure 1: Flow chart of the proposed methodology

V. ALGORITHMS AND TECHNIQUES

The project utilizes Hybrid Cryptography techniques and web technologies to provide secure data transmission and protected communication through a smart web-based system:

1) Elliptic Curve Cryptography (ECC):

Used for secure key generation and key exchange between sender and receiver. ECC provides strong security with smaller key sizes and improves encryption efficiency[1][2].

2) • RSA Algorithm:

Used for authentication and digital signature verification. It ensures message authenticity and verifies that the data is transmitted from a trusted sender[3][12].

3) • AES-256-GCM Encryption:

Used to encrypt and decrypt the actual message content securely. It provides confidentiality, integrity, and protection against data tampering during transmission[4][5].

4) • OpenSSL Cryptographic Library:

Used for implementing ECC, RSA, and AES-256-GCM encryption functionalities within the PHP application for secure communication[9].

5) • PHP Web Framework and Backend:

Serves as the backend technology for handling user registration, login authentication, sender-receiver communication, encryption, decryption, and message expiry functionalities[10].

6) • Database Management Techniques:

MySQL database is used for securely storing user details, encrypted messages, timestamps, digital signatures, and message status information for efficient management and retrieval[11].

7) Secure Session Handling:

PHP session management is used to maintain secure user authentication and prevent unauthorized access to the system[10][13].

8) • XAMPP Server Environment:

Used to run Apache server and MySQL database locally for developing and testing the secure communication system efficiently[6][7].

VI. ARCHITECTURE

The system architecture of this project integrates a web-based interface with Hybrid Cryptographic modules to provide secure data transmission and protected communication between users[6][8]. The frontend is developed using HTML, CSS, Bootstrap, and JavaScript to create interactive pages for user registration, login, sender, and receiver communication, while the backend is built using PHP for handling routing, authentication, encryption, decryption, session management, and communication between system components[9][10]. Elliptic Curve Cryptography (ECC) is used for secure key exchange, RSA is used for digital signature verification and authentication, and AES-256-GCM is used for secure message encryption and decryption[1][2][3][4][5]. OpenSSL libraries are integrated to perform cryptographic operations efficiently, and all user details, encrypted messages, timestamps, and message status information are securely stored in a MySQL database[9][11]. The complete architecture supports secure real-time communication, confidentiality, integrity verification, authentication, and automatic message expiry through a centralized web-based system.

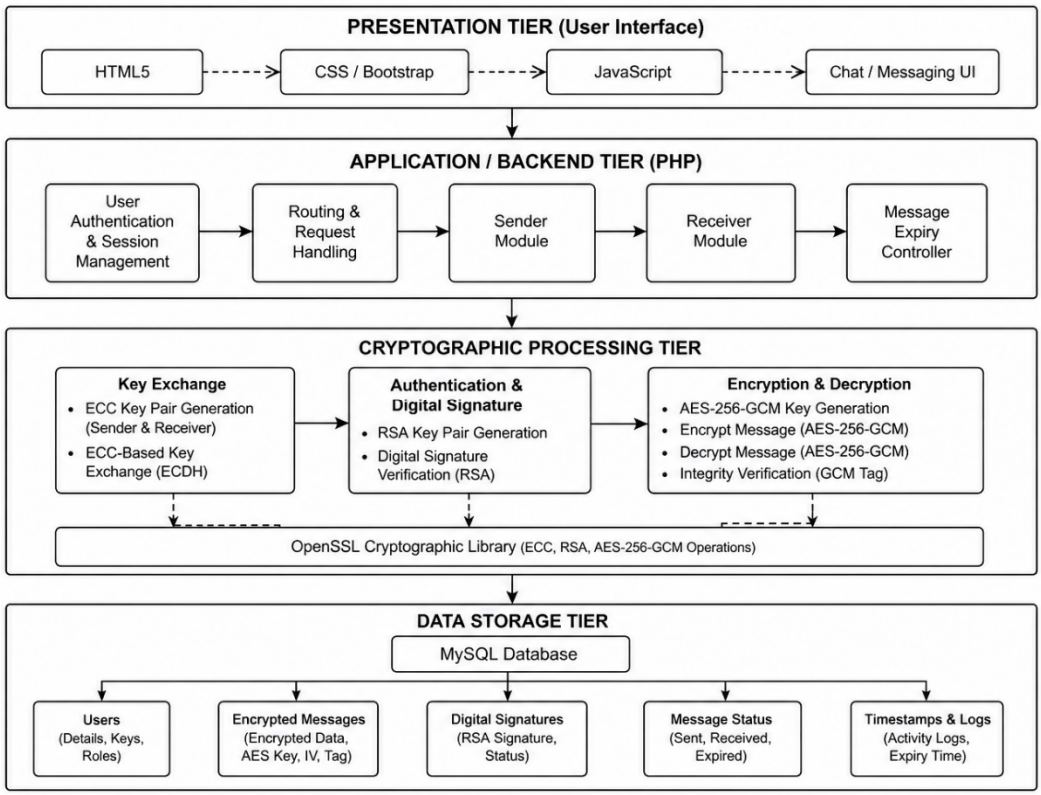
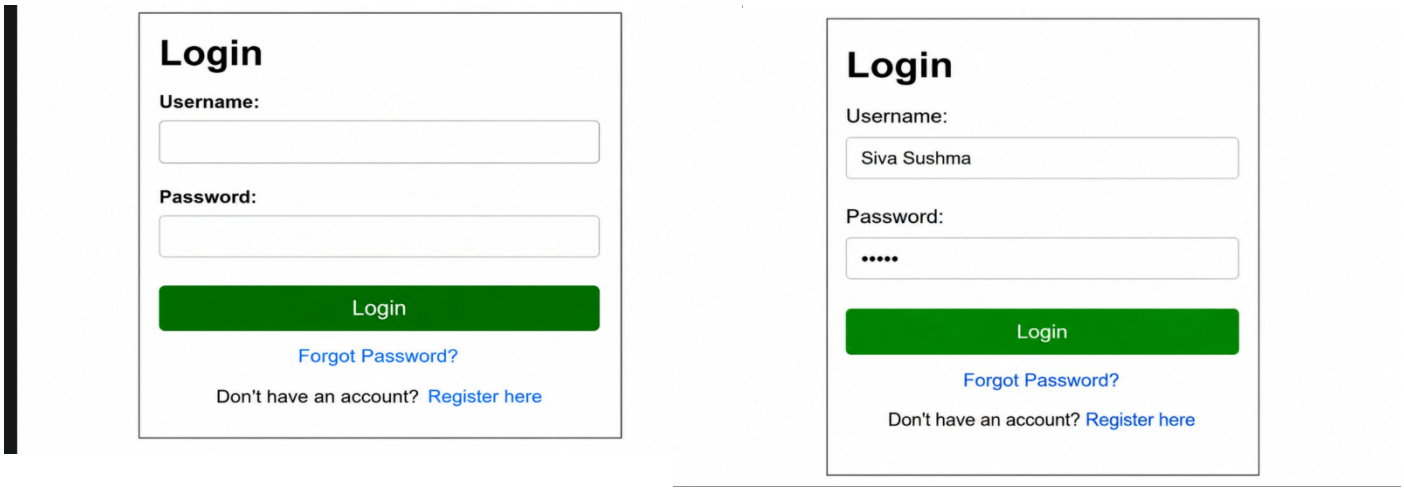


Figure 2: Architecture System

VII. OUTPUT SCREEN

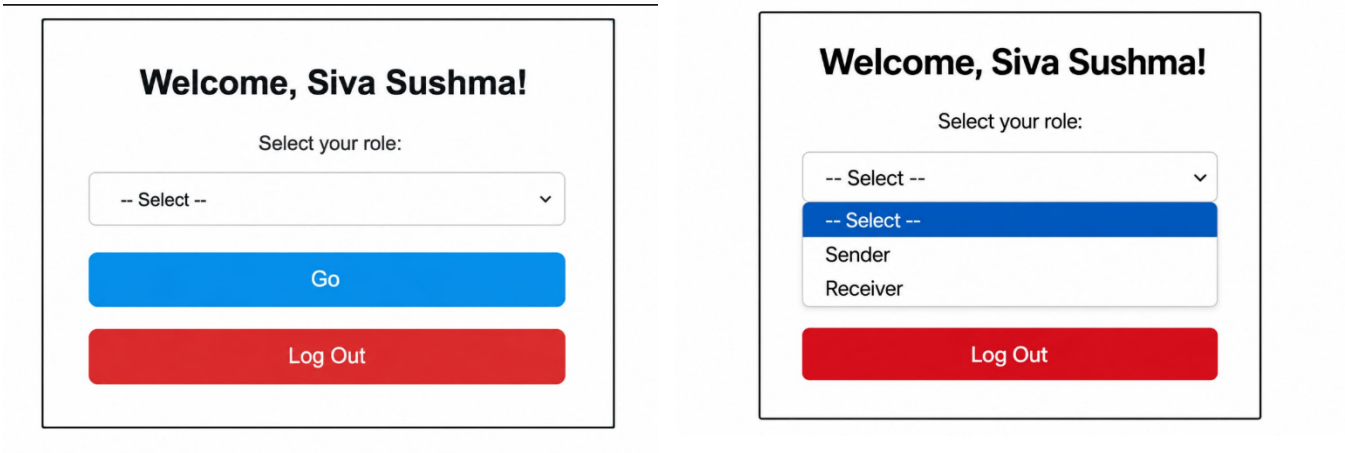
The Register Page is the initial interface of the secure data transmission system that allows new users to create an account securely[6][8]. Users are required to enter details such as username and password, which are securely stored in the MySQL database after validation and encryption processes[10][11]. The page is developed using HTML, CSS, Bootstrap, and PHP to provide a simple, user-friendly, and responsive interface[9][10]. It also ensures secure user authentication and prevents unauthorized access to the communication system[3][7]. Once registration is completed successfully, users can log in and access secure message encryption and decryption functionalities.

Screenshot Of RegisterPage

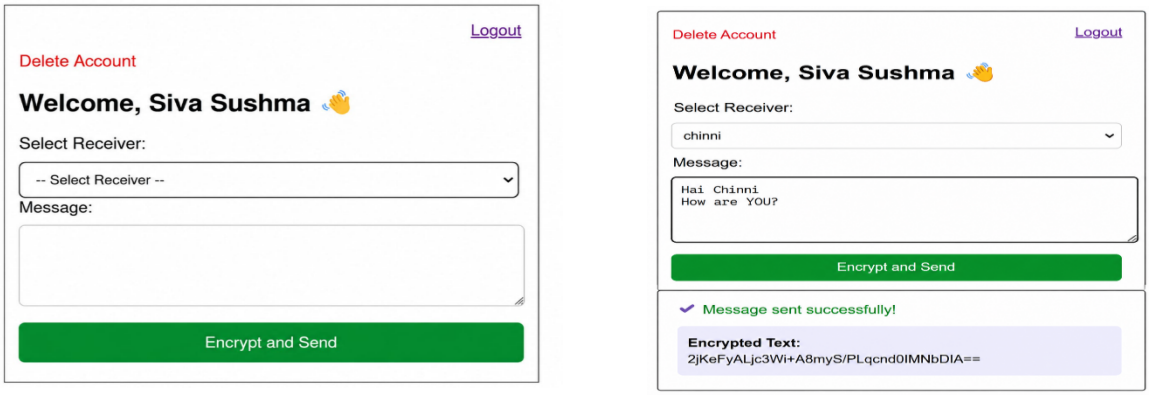


Screenshot Of Login Page

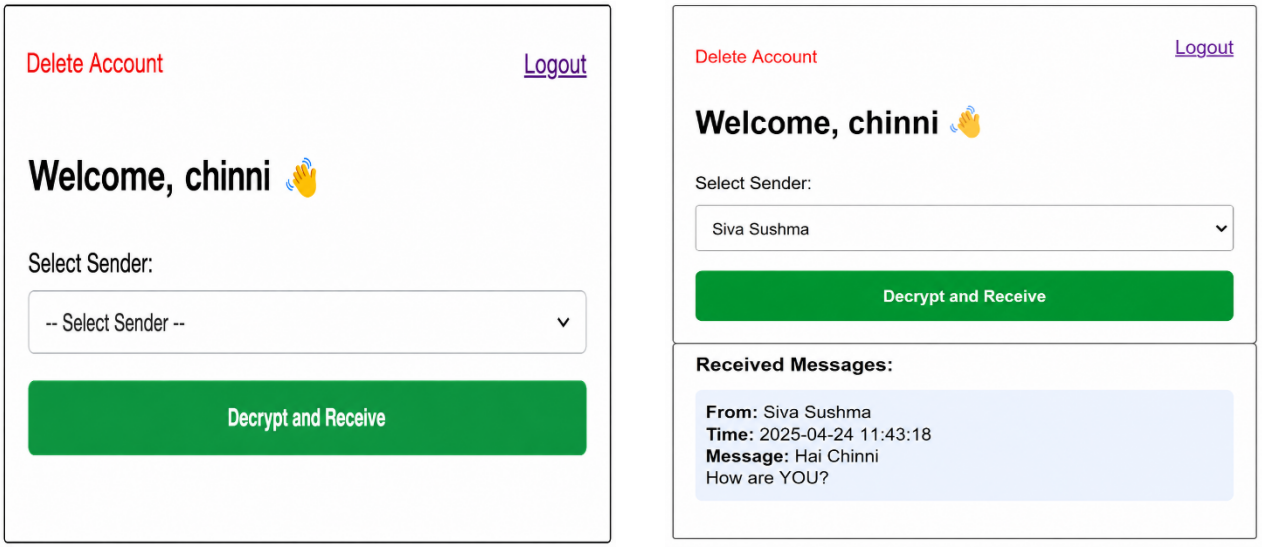
The Dashboard is the main interface of the secure data transmission system that allows users to access all communication and security functionalities in one place[6][8]. It provides options for sending encrypted messages, receiving decrypted messages, managing user sessions, and monitoring communication status[7][12]. The dashboard is developed using HTML, CSS, Bootstrap, JavaScript, and PHP to provide a secure, user-friendly, and responsive interface for real-time secure communication[9][10].



Screenshot Of Dash Board



Screenshot Of Sender Page



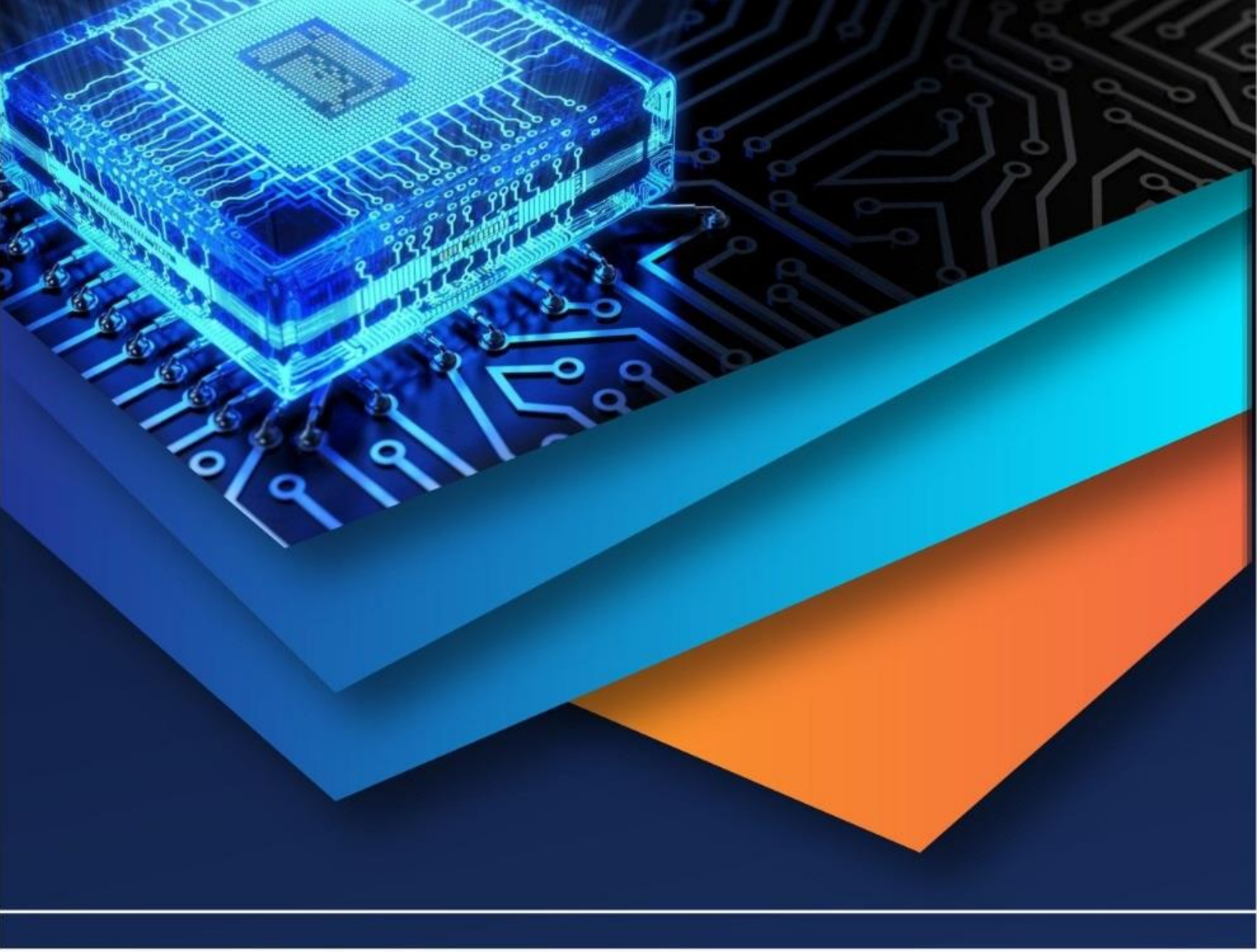
Screenshot Of Receiver Page

VIII. CONCLUSION

In conclusion, the Secure Data Transmission System provides an intelligent and reliable solution for protecting sensitive information using Hybrid Cryptographic techniques. The system combines Elliptic Curve Cryptography (ECC), RSA, and AES-256-GCM algorithms to ensure secure communication, confidentiality, authentication, and data integrity during message transmission. By implementing secure key exchange, digital signature verification, message encryption, and automatic message expiry functionalities, the application helps prevent unauthorized access and enhances user privacy. The web-based interface makes secure communication simple and efficient for users, while the integration of PHP, MySQL, and OpenSSL ensures reliable system performance. Overall, the project supports secure real-time communication and strengthens data protection through advanced cryptographic mechanisms.

REFERENCES

[1] V. Miller, “Use of Elliptic Curves in Cryptography,” Advances in Cryptology – CRYPTO ’85, Springer, 1986.
[2] N. Koblitz, “Elliptic Curve Cryptosystems,” Mathematics of Computation, Vol. 48, No. 177, pp. 203–209, 1987.
[3] 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, 1978.
[4] J. Daemen and V. Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard, Springer, 2002.
[5] National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES),” FIPS PUB 197, 2001.
[6] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson Education, 2017.
[7] Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Education, 2015.
[8] William Stallings, Network Security Essentials: Applications and Standards, Pearson, 2018.
[9] OpenSSL Software Foundation, “OpenSSL Cryptography Library Documentation,” Available: https://www.openssl.org/
[10] The PHP Group, “PHP: Hypertext Preprocessor Documentation,” Available: https://www.php.net/
[11] Oracle Corporation, “MySQL Database Reference Manual,” Available: https://dev.mysql.com/doc/
[12] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[13] D. R. Stinson, Cryptography: Theory and Practice, CRC Press, 2005.
[14] Christof Paar and Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010.
[15] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley India, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY