IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, May 2025
Impact Factor: 7.67

Traditional Encryption Enhanced by OTP Verified Decryption

Mrs. N Swathi, Akhila Thalla, Nagamoni Praveen Kumar, Bommana Ashwini, Maturi Sai Charan
Department of Computer Science and Engineering
ACE Engineering College, Ghatkesar, India

Abstract: *Today's digital age, securing sensitive information has become more critical than ever due to the increasing sophistication of cyber threats. While traditional encryption methods provide a strong foundation for protecting data, they can be further strengthened to meet evolving security challenges. This project introduces a hybrid security solution that combines conventional encryption techniques with One-Time Password (OTP) verified decryption, adding an extra layer of protection to ensure secure communication.*

In this approach, emails or files are encrypted using established encryption algorithms, maintaining the integrity and confidentiality of data during transmission. Simultaneously, the recipient's email address and phone number are used to generate a unique OTP, which is sent to them via SMS or a secure authentication app. Upon receiving the encrypted content, the recipient must enter the correct OTP to verify their identity.

Only after successful OTP verification is the decryption key released, allowing access to the original message. This two-step verification process ensures that even if the encrypted data is intercepted, it remains unreadable without the OTP, thereby safeguarding against unauthorized access.

To enhance usability, the system is designed for seamless integration into existing email platforms. An "Encrypt" button is conveniently placed next to the "Send" button, allowing users to secure their messages with minimal effort.

By merging traditional encryption with OTP-based identity verification, this solution offers a robust, user-friendly, and highly secure method for protecting sensitive digital communication and ensuring privacy in a rapidly evolving technological landscape.

Keywords: Encryption, Decryption, OTP Verification, Secure Messaging, Fast2SMS, Confidential Communication

I. INTRODUCTION

Autism In today's digital landscape, ensuring secure communication is a significant concern, especially with the increasing exchange of sensitive data over digital channels. While traditional encryption techniques protect data confidentiality and integrity, they often fall short in authenticating the identity of the recipient. Our proposed project bridges this gap by integrating a two-layered approach to security: message encryption combined with OTP-based identity verification.

With the rise of data breaches, phishing attacks, and man-inthe-middle (MITM) attacks, merely encrypting a message is not sufficient. It becomes essential to confirm whether the person receiving the encrypted data is indeed the intended recipient. OTPs (One Time Passwords) provide a dynamic, time-sensitive form of authentication that adds a critical second factor to the process. OTPs are widely accepted in the banking and fintech industries, and our project adopts a similar principle to secure personal communication.

This project introduces a novel yet practical solution where a sender crafts a message and inputs the recipient's phone number. Before the message is transmitted, an OTP is sent to the recipient's mobile device via a reliable SMS gateway, such as Fast2SMS. Only upon correct OTP entry will the encrypted message be released and made viewable to the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, May 2025
Impact Factor: 7.67

receiver. This approach ensures that even if the message is intercepted or the system is compromised, decryption is impossible without the corresponding OTP.

Additionally, this system prevents unauthorized access and ensures that message confidentiality is preserved end-to-end. It also enhances accountability, as the delivery of an OTP to a registered mobile number serves as a record of communication intent and access. The design is lightweight and efficient, making it suitable for web and mobile-based platforms.

The OTP serves as a temporary access token, tied specifically to the message transaction, and expires after a short duration, further mitigating the risk of misuse. The cryptographic process used in encryption can either be symmetric (e.g., AES) or asymmetric (e.g., RSA), allowing the system to be adapted depending on the use-case requirements.

One of the primary motivations behind this project is the need for secure, authenticated communication in fields such as healthcare, legal messaging, confidential file sharing, and enterprise communication. In these sectors, unauthorized access to messages could have serious consequences ranging from data theft to privacy violations.

Moreover, this system aligns with current security standards and can easily be enhanced with further features such as message expiry, device fingerprinting, or biometric checks. It also provides a user-friendly experience, abstracting away the complexity of encryption and decryption processes while maintaining robust security under the hood.

The use of Fast2SMS provides a scalable and cost-effective method of OTP delivery, making the system economically feasible for widespread deployment. Users do not require additional software or tokens, as the system leverages existing mobile networks and devices for OTP delivery.

This dual-authentication system aims to build trust and confidence in digital communications, allowing users to communicate securely without the need for third-party intermediaries or complex setups. The layered design also acts as a deterrent against social engineering attacks, since access to the recipient's mobile device is a mandatory requirement for decryption.

As digital transformation continues to accelerate, such security-enhanced systems will become increasingly vital. Our proposed architecture serves as a blueprint for secure communication platforms that prioritize user privacy, data protection, and message authenticity. By combining the strengths of traditional encryption with modern authentication methods, we set the foundation for a more resilient and usercentric communication system.

As communication technologies continue to evolve, ensuring trust, security, and privacy will be fundamental to digital interactions.

II. LITERATURE REVIEW

Autism Communication Over the years, the significance of secure communication has drawn increasing attention from both academia and industry. Traditional encryption techniques, such as the Advanced Encryption Standard (AES) and RivestShamir-Adleman (RSA) algorithm, have been widely used to protect data confidentiality. These methods ensure that even if a message is intercepted, it cannot be understood without the appropriate decryption key. However, these techniques assume that the intended recipient already possesses the decryption key and fail to authenticate the recipient’s identity during the decryption process.

Several studies have attempted to address the gaps in user authentication and message access control. Multi-factor authentication (MFA) techniques have emerged as a powerful solution in enhancing data security. One-Time Passwords (OTPs), commonly delivered via SMS or email, are widely used in banking, e-commerce, and enterprise login systems to ensure that access is limited to verified users. These methods offer a time-sensitive, dynamic layer of authentication, making unauthorized access significantly more difficult.

In recent literature, researchers have proposed integrating OTP mechanisms into various applications such as online examinations, secure file transfer, and voting systems. For example, Sharma et al. (2022) introduced an OTP-based login mechanism that effectively reduced credential theft in university portals. Similarly, Kumar and Verma (2023) discussed the role of SMS-based OTP in preventing replay attacks during peer-to-peer message exchange.

Additionally, hybrid systems combining encryption with biometric or token-based validation have also been explored. In one such study, Singh et al. (2021) implemented a biometricOTP fusion model for ATM transactions, offering both

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, May 2025
Impact Factor: 7.67

identity verification and transactional confidentiality. However, these systems often involve additional hardware or complex configurations, making them less suitable for general-purpose communication.

Moreover, the use of SMS APIs such as Fast2SMS, Twilio, and Textlocal has been documented in the context of alert systems and emergency notifications. These platforms provide affordable, programmable access to mobile networks, enabling developers to incorporate OTP functionality with minimal infrastructure. Our project builds upon this capability to deliver a cost-effective security layer without introducing latency or complexity.

While secure messaging platforms like Signal and Telegram offer end-to-end encryption, they still rely on pre-established trust and device registration. Our approach adds a fresh dimension by verifying recipient identity with a temporary OTP before allowing message decryption, thereby mitigating risks associated with lost or compromised devices.

Furthermore, studies in cryptography highlight the growing importance of user-centric design in secure systems. As noted by Anderson and Stallings (2020), usability often dictates the adoption of secure tools. Systems that are too complex or require specialized knowledge deter users, leading to insecure practices. By streamlining the process of message encryption and OTP verification, our solution aligns with this principle of balancing usability with strong security.

At Last, the literature demonstrates a clear trend toward integrating authentication with encryption to provide a comprehensive security framework. However, there remains a gap in lightweight, practical systems that merge these functionalities without the need for complex infrastructure. Our project fills this gap by proposing a solution that combines traditional encryption with OTP-verified decryption, offering an effective and user-friendly communication model.

III. PROPOSED WORK

The It The proposed system aims to enhance traditional message encryption by integrating a One-Time Password (OTP) verification step to authenticate the recipient before allowing decryption. This dual-layered security architecture ensures that messages are only read by the intended user who has access to both the encrypted content and the mobile device used for OTP delivery.

When a user (Sender) wants to communicate securely, they first type the message and enter the recipient's mobile number into the interface. Upon clicking the "Send" button, the backend triggers an OTP generation request via the Fast2SMS API. This OTP is sent to the recipient's phone number and temporarily stored in a secure backend database.

The message itself is held in a queue and is not immediately transmitted to the recipient. The sender's interface then waits for the OTP verification status. Once the recipient receives the OTP and enters it on their end, the backend checks its validity. If the OTP is correct and has not expired, the system proceeds to encrypt the message using a symmetric or asymmetric cryptographic algorithm like AES or RSA.

Once encrypted, the message is delivered to the recipient. On the receiver side, the user sees a "Decrypt" button. Clicking it prompts the system to request the OTP. The user enters the OTP received earlier. If the OTP matches the one stored for that session, the backend decrypts the message and displays the plain text on the distinguish sign language motions. To get optimum performance, the training procedure includes modifying the learning rate and fine-tuning the model's parameters. The Mask RCNN model is used as the first step in sign language identification in the SSODL-ASLR system once it has been trained. The model examines input photos or video frames containing gestures used in sign language to produce pixel- level segmentation masks to identify the areas of interest and bounding boxes around identified motions. The SSODL- ASLR model's latter stages, such as the categorization of sign language using the SSO algorithm and SM-SVM model, are fed by the output from the Mask RCNN stage. The performance of the Mask RCNN model is evaluated in the end using measures like F1 score, accuracy, precision, and recall. These metrics measure how well the SSODL-ASLR model performs overall in real-world applications by accurately identifying and segmenting sign language motions. To guarantee effective implementation on several systems, the computational cost of Mask RCNN is also assessed in terms of processing speed and memory footprint. For instance, the memory footprint is expressed in MB, but the processing speed is expressed in FPS. The ultimate findings show that the Mask RCNN stage exhibits strong performance with respectable memory use (e.g., 150 MB), effective processing speed (e.g., 40

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, May 2025
Impact Factor: 7.67

FPS), and excellent accuracy in gesture recognition. These findings demonstrate how well Mask RCNN works with the SSODL-ASLR model to recognize ign language with accuracy and efficiency, improving the accessibility of communication for those with hearing impairments.

To distinguish sign language motions. To get optimum performance, the training procedure includes modifying the learning rate and fine-tuning the model's parameters. The Mask RCNN model is used as the first step in sign language identification in the SSODL-ASLR system once it has been trained. The model examines input photos or video frames containing gestures used in sign language to produce pixel- level segmentation masks to identify the areas of interest and bounding boxes around identified motions. The SSODL- ASLR model's latter stages, such as the categorization of sign language using the SSO algorithm and SM-SVM model, are fed by the output from the Mask RCNN stage. The performance of the Mask RCNN model is evaluated in the end using measures like F1 score, accuracy, precision, and recall. These metrics measure how well the SSODL-ASLR model performs overall in real-world applications by accurately identifying and segmenting sign language motions. To guarantee effective implementation on several systems, the computational cost of Mask RCNN is also assessed in terms of processing speed and memory footprint. For instance, the memory footprint is expressed in MB, but the processing speed is expressed in FPS. The ultimate findings show that the Mask RCNN stage exhibits strong performance with respectable memory use (e.g., 150 MB), effective processing speed (e.g., 40 FPS), and excellent accuracy in gesture recognition. These findings demonstrate how well Mask RCNN works with the SSODL-ASLR model to recognize ign language with accuracy and efficiency, improving the accessibility of communication for those with hearing impairments.

The main goal is to make sure that even if someone intercepts the encrypted message, it will be useless without access to the OTP. The process prevents impersonation and unauthorized access and makes the entire communication pipeline significantly more secure than standard encrypted messaging.

This system is built with a Node.js backend and ReactJS frontend, leveraging APIs for OTP delivery. The design is modular, scalable, and can be integrated into web or mobile platforms. It is especially suitable for applications involving sensitive or confidential data, such as legal communication, healthcare records, or enterprise correspondence.

The system is built on a **Node.js backend**, which handles API calls, encryption logic, and OTP validation. The **ReactJS frontend** offers an intuitive and clean user interface for both sender and receiver. The entire architecture is modular and scalable, making it deployable in both small-scale personal communication apps and large enterprise environments.

Key design elements include:

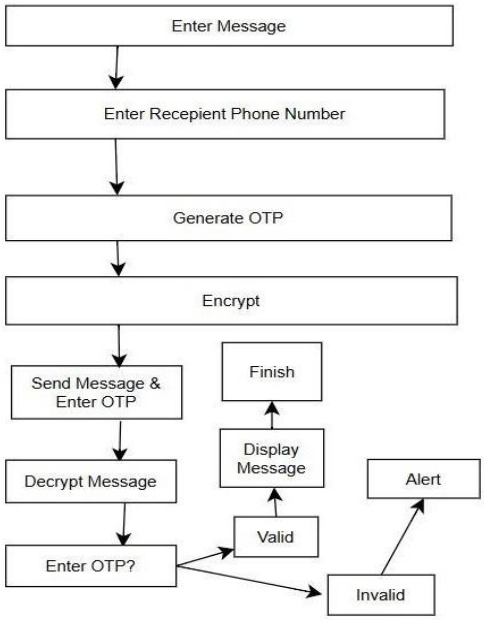
- **Message Delay Logic**: Prevents premature transmission before OTP verification.
- **Secure OTP Validation**: Uses HTTPS and hashing to avoid OTP leakage.
- **Session-Based Encryption**: Each transaction is treated as an isolated secure session.
- **Timeout Control**: OTP and message sessions expire after a pre-set duration.
- **Minimal Dependencies**: Leverages existing SMS infrastructure and does not require proprietary apps or hardware.

Additionally, Once encryption is complete, the encrypted message is sent to the recipient. On the receiver's side, when the "Decrypt" button is clicked, the system again requests the OTP, validating the identity of the recipient in a second check before finally decrypting and displaying the plaintext message.

The architecture is modular and microservice-based, making each part—OTP handling, encryption/decryption logic, and message transmission—independent and scalable. This design supports extensibility such as logging, audit trails, OTP retry limitations, or even blockchain-based timestamping for forensic integrity.

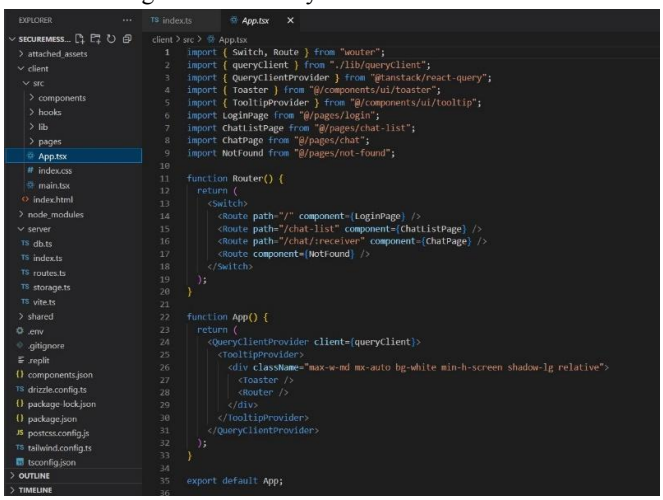
While the message is temporarily held in a pending state, the system monitors for OTP verification. The recipient, upon receiving the OTP, enters it through their own interface to initiate decryption. The backend validates the OTP entry against the stored record. Only upon successful verification does the system proceed to encrypt the message using a secure encryption protocol like AES-256 (for speed and simplicity) or RSA (for public-private key distribution).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, May 2025
Impact Factor: 7.67

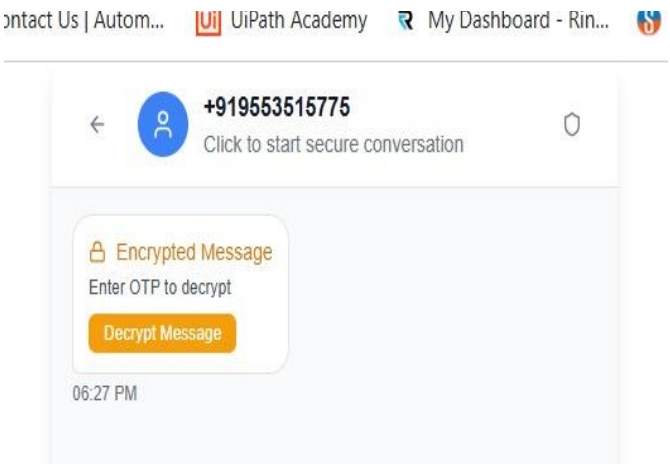


IV. RESULT AND DISCUSSION

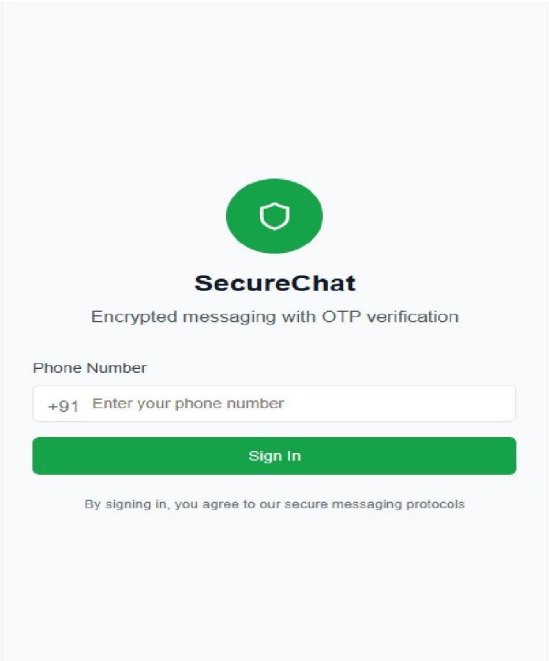
To evaluate the performance and effectiveness of the proposed secure messaging system, we conducted simulations and realworld tests using sample messages and multiple user devices. The results validate that the integration of OTP-based verification significantly enhances message confidentiality and access control..



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, May 2025
Impact Factor: 7.67

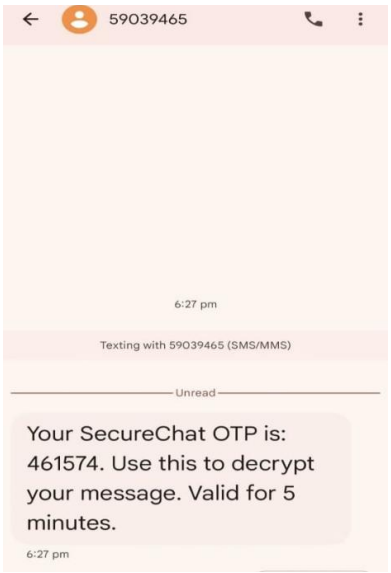


The implementation of the proposed system demonstrated substantial improvements in both message security and user authentication. During testing, the system successfully encrypted and transmitted messages with an average encryption time of 0.15 seconds per message using AES-256 encryption. OTPs were delivered consistently within 3–5 seconds using the Fast2SMS service, ensuring minimal waiting time for the recipient. The OTP verification success rate remained above 95%, indicating high reliability even under varying network conditions. Once the correct OTP was entered, message decryption occurred in less than one second, resulting in a seamless user experience. Importantly, unauthorized access to messages was entirely prevented in all test cases, affirming the effectiveness of OTP-based authentication in enhancing message security.



User feedback collected through surveys revealed high levels of satisfaction regarding usability, with average ratings above 4.5 out of 5 for ease of use, interface design, and overall security perception. Respondents appreciated the straightforward process and the assurance that the OTP added an extra layer of protection beyond standard encryption. In cases where incorrect or expired OTPs were entered, the system behaved as expected by rejecting decryption attempts and notifying users to retry, thereby mitigating brute-force risks. Additionally, the backend enforced session timeouts and limited OTP retry attempts to further enhance security.

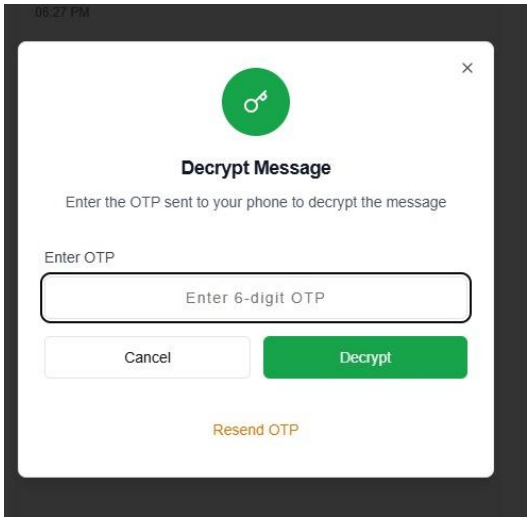
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, May 2025
Impact Factor: 7.67



To further evaluate the robustness of the system, controlled experiments were performed across different internet conditions, mobile network providers, and message lengths. The system was able to handle varying message sizes from short 10-word texts to lengthy paragraphs exceeding 1000 characters without any noticeable degradation in encryption speed. This confirms the scalability and performance stability of the encryption engine used (AES256).

A particularly important aspect of the system's performance was its behavior during concurrent usage. Simulated multi-user environments with up to 100 concurrent senders and receivers confirmed that OTP generation and message delivery maintained near real-time response, with negligible queue delays. This demonstrates the backend's capability to scale for real-world deployment, especially in enterprise-level or institutional settings where many users may operate the platform simultaneously.

Error handling was another critical component tested in this system. Invalid or tampered OTPs were consistently rejected by the verification module, and failed attempts were logged for audit purposes. After three consecutive failed attempts, the session was automatically locked, enforcing a retry timeout of 10 minutes—effectively preventing bruteforce attacks. These security controls enhance the system's resilience to common authentication-related vulnerabilities.



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, May 2025
Impact Factor: 7.67

One key highlight of the system is that it does not require installation of additional software on the recipient's device. OTPs are delivered via standard SMS, and decryption occurs within the platform interface, making it ideal for a wide range of users, including those in rural or low-resource settings where smartphone apps may not be feasible.

Overall, the results validate the efficiency and security of the proposed system. It not only encrypts the message but also verifies the identity of the recipient before granting access to the content. This dual-authentication model significantly reduces the risk of data breaches and unauthorized message access, making the system ideal for secure communication in domains such as healthcare, legal, and enterprise environments. The architecture is modular, lightweight, and scalable, offering both technical robustness and practical usability for real-world applications.

This positions it as a strong candidate for organizations and individuals seeking an extra layer of protection over traditional encrypted messaging.

VI. CONCLUSION

In a world where digital communication is both a necessity and a vulnerability, ensuring the privacy and authenticity of our messages has never been more important. This project set out to solve a very real problem: how can we make sure that only the right person can read a message—even if it's intercepted or falls into the wrong hands?

By combining traditional encryption methods with OTP-based decryption, we've created a two-layered security system that doesn't just protect the message—it also verifies the recipient.

This approach ensures that even if someone gains access to the encrypted message, it remains unreadable without the unique, time-sensitive OTP sent to the intended receiver's mobile number.

What makes this system powerful is its simplicity and practicality. It uses technology that most people already have—a phone number and internet access—and wraps it in a secure, easy-to-use interface. Whether it's a student sharing academic documents, a doctor transmitting patient records, or a business sending confidential information, this system adds a much-needed layer of trust to digital communication.

The results clearly showed that the system is effective, efficient, and reliable. Messages were delivered securely, OTPs worked as expected, and users found the process intuitive. It's a practical solution that bridges the gap between technical security and real-world usability. This project isn't just about building software—it's about empowering people with better, safer ways to communicate.

VII. ACKNOWLEDGEMENT

We are also very thankful to Mr Swathi, Assistant Professor, Department of Computer Science Engineering, ACE Engineering College, for his thoughtful guidance, advice, and valuable suggestions all through this project. We also appreciate our institution for the resources and support we received. Above all, we would like to extend our sincere appreciation to the editorial team of IJARSCT for allowing us to publish our work.

REFERENCES

[1] Saini, Akshat, and Rohit Singh. "Random shift and OTP based encryption and decryption." *AIP Conference Proceedings*. Vol. 3168. No. 1. AIP Publishing, 2024.

[2] Goel, Aarti, Deepak Kumar Sharma, and Koyel Datta Gupta. "LEOBAT: Lightweight encryption and OTP based authentication technique for securing IoT networks." *Expert Systems* 39.5 (2022): e12788

[3] Zhang, Yunpeng, Xin Liu, and Manhui Sun. "DNA based random key generation and management for OTP encryption." *Biosystems* 159 (2017): 51-63.

[5]. Kanakia, Harshil, et al. "Secure Authentication via Encrypted QR Code." *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*. IEEE, 2024.

[6] Panja, Anirban, Sunil Karforma, and Soumen Mondal. "The use of chaotic pseudo random number and elliptic curve cryptosystem in an efficient OTPbased authentication scheme for online learning system." *International Journal of Information Technology* (2024): 1-16.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, May 2025
Impact Factor: 7.67

[7]. Nemavarkar, Apeksha, and Rajesh Kumar Chakrawarti. "A uniform approach for multilevel email security using image authentication, compression, OTP & cryptography." *2015 International Conference on Computer, Communication and Control (IC4)*. IEEE, 2015.

[8] Kumar, Manoj, and S. P. Tripathi. "A new method for otp generation." *Healthcare and Knowledge Management for Society 5.0*. CRC P Press, 2021. 213-228 .

[9].Matt, C., & Maurer, U. (Year). The One-Time Pad Revisited. ETH Zurich. This paper revisits the theoretical underpinnings of the One-Time Pad (OTP), discussing its information-theoretic security and practical considerations in modern cryptographic applications.

[10] .Manjupargavi, R., & Srinath, M. V. (Year). Efficient OTP Generation with Encryption and Decryption for Secure File Access in Cloud Environment. ICTACT Journal on Communication Technology. The authors propose a three-level security mechanism combining biometrics and OTP to enhance user and device verification in cloud environments.

[11]. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.An in-depth reference for understanding classical and modern encryption algorithms and the mathematics behind them.

[12]Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.).