IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Integrated Framework For The Evolution And Future Of Secure Data Transmission

[1]Sunny, [2]Dr. Nitesh Kaushik, [3]Ms. Shweta Sharma, [4]Lakshya Soni, [5]Sara Thakur
[1,4,5]Student, Department of Computer Science and Engineering,
Anand International College of Engineering, Jaipur, India
[2]Professor, [3]Assistant Professor, Department of Computer Science and Engineering,
Anand International College of Engineering, Jaipur, India

Abstract: Secure data transmission has advanced from foundational cryptographic protocols to integrated, domain-specific approaches that combine multiple security techniques. In several studies, traditional cryptography remains central. In 6G networks, combinations of AES, RSA, and Quantum Key Distribution coupled with edge computing yield transfer rates of 800–1200 with data rates measured in Gbps and performance ratings between 3.8 and 4.5 on a 5-point scale. Other studies focus on hybrid approaches—combining cryptography with steganography in video transmission or using Elliptic Curve Cryptography in IoT healthcare—to address shortcomings of earlier methods, particularly in scalability and the ability to operate in resource-constrained environments. The literature outlines a progressive evolution through distinct developmental stages: An initial foundation rooted in traditional cryptographic principles; the integration of steganography and low-complexity algebraic techniques to improve efficiency and address emerging cybersecurity challenges; and the subsequent adoption of quantum-resistant and AI-enhanced methods tailored for highspeed, domain-specific applications such as 6G networks, IoT systems, and healthcare environments. These studies document that modern secure data transmission evolves by addressing internal limitations—such as computational constraints and key management issues—and external pressures from an expanding and dynamic threat landscape, paving the way for increasingly robust and tailored solutions.

In addition to the analytical survey, this study proposes and evaluates a lightweight timestamp-based AES key refresh mechanism for secure data transmission. The model dynamically regenerates symmetric encryption keys at fixed time intervals using synchronized system timestamps. Experimental simulations were conducted with key update intervals of 30s, 10s, and 5s, measuring message delivery success, decryption latency, and key mismatch rates. The results show that a 10-second key refresh interval achieves a 98.5 percent message success rate with minimal latency overhead, offering an effective balance between forward secrecy and performance in real-time IoT communication environments.

Index Terms - Comp Secure Communication, AES Encryption, Timestamp-Based Key Generation, Key Refresh Mechanism,IoT Security, Dynamic Cryptographic Protocols, Lightweight Encryption, Data Integrity, Key Management, Cryptography, Steganography, 6G Networks.

I. INTRODUCTION

In the digital era, the exponential growth of data exchange across global networks has made secure data transmission a cornerstone of modern communication systems. As cyber threats grow in complexity and sophistication, ensuring confidentiality, integrity, and authenticity during transmission has become essential. These concerns have driven continuous advancement in cryptographic methods, secure communication protocols, and transmission frameworks that aim to safeguard information from unauthorized access and malicious activities
[5].

Historically, secure transmission protocols began with basic cipher systems and gradually evolved into advanced symmetric and asymmetric encryption techniques. Well-established standards such as RSA and AES continue to form the backbone of encryption schemes across various domains, including finance, defense, healthcare, and e-commerce [5]. However, the rise of quantum computing, pervasive IoT devices, and increasingly adaptive cyberattacks now pose significant challenges to conventional cryptographic systems, particularly in key distribution and forward secrecy [6].

In response, modern research has shifted toward developing quantum-resistant algorithms, blockchain-backed protocols, AI-driven intrusion detection, and hybrid frameworks that combine encryption with steganography or multi-path routing. These approaches are tailored for specific environments like IoT networks, 6G infrastructure, and healthcare applications, often emphasizing lightweight computation and low-latency performance [2][3][6].

Despite these developments, one aspect of secure communication that remains underexplored is temporal key management—specifically, how the frequency of encryption key refreshes influences the stability, latency, and integrity of data transmission in real-time systems. Most traditional systems employ static or session-based keys, which may be vulnerable if compromised during extended communication sessions [1][5]. To address this gap, this study introduces a lightweight timestamp-based AES key refresh mechanism, wherein symmetric keys are regenerated at fixed intervals using synchronized timestamps. The proposed model is experimentally evaluated under different refresh intervals (30s, 10s, and 5s) to assess key mismatch rates, decryption success, and latency. The results demonstrate that a 10-second refresh interval offers a balance between cryptographic resilience and real-time performance, making it suitable for secure IoT communications and other resource-constrained applications.

II. Literature Survey

Recent literature on secure data transmission highlights the integration of classical cryptographic algorithms (e.g. AES, RSA, ECC) with data-hiding and hybrid techniques to meet modern requirements[5]. For example, combining symmetric encryption (AES/RSA) with LSB steganography for medical image transmission has achieved very high fidelity (PSNR 50–57dB, SSIM 1.0)[1]. Likewise, a lightweight IoT scheme using an elliptic Gaulois (ECC inspired) cipher with matrixXOR steganography reported improved PSNR (68dB) and modest latency (6.5ms key-generation time)[2]. In vehicular networks (IoV), hybrid methods such as the EAST algorithm have demonstrated sub-millisecond encryption time (0.86ms) along with high signal quality (PSNR 78.6dB)[3].

These studies commonly use metrics such as PSNR, SSIM, execution / decryption time, and key generation time to quantify security-efficiency tradeoffs 12.3. Domain-specific frameworks have also been proposed: for instance, load-balanced multipath routing with packet-level encryption secures IoMT (Internet of Medical Things) data while maintaining very low latency (¡10ms)[4].

At the frontier, 6G research emphasizes quantum safe and AI-enhanced security, with QKD integrated into AES/RSA schemes producing multigigabit throughput (800-1200 Gbps) and high-performance ratings, and AI-based intrusion detection proposed to adaptively protect 6G links 6. In general, the reviewed work indicates a shift from standalone ciphers to context-aware composite solutions (hybrid encryptionsteganography, ECC-based algorithms, QKD and AI-driven methods) tailored to 6G, IoT and healthcare applications[5][6].

While existing literature has extensively explored hybrid encryption methods, lightweight algorithms, and steganographic enhancements for secure communication, the temporal dimension of key management—specifically the impact of periodic key regeneration on transmission reliability—remains underexamined. Most models assume either static or session-level keys, leaving a research gap in dynamic key refresh protocols that adapt over time. This study addresses that gap by proposing a timestamp-based AES key regeneration scheme. By systematically evaluating different refresh intervals and measuring key mismatch rates, decryption success, and latency, this work contributes novel experimental insight into the trade-offs between key update frequency and real-time communication stability in resource-constrained environments.

III. Modern Methods of Secure Data Transmission

Modern secure transmission techniques utilize a combination of encryption and data-hiding methods to ensure privacy and integrity. Key approaches include symmetric encryption, asymmetric encryption, steganography, and hybrid encryption[5].

A. Symmetric Encryption

Symmetric encryption employs a single key to both encrypt and decrypt data. Its speed and efficiency make it well-suited for handling large amounts of data.AES (Advanced Encryption Standard) is widely adopted as it provides a well-rounded mix of speed and security. That said, secure key distribution remains a challenge[5].

B. Asymmetric Encryption

Asymmetric encryption relies on a pair of keys: a public key for encryption and a private key for decryption.RSA is a well-known algorithm offering secure key exchange over untrusted networks, though it is slower compared to symmetric methods[5].

C. Steganography

Steganography hides information within other media like images or audio. The technique aims to disguise the message's presence rather than its content, making detection difficult. It is often used in combination with encryption to enhance overall security.[1].

D. Hybrid Encryption

Hybrid encryption combines symmetric and asymmetric methods. The symmetric key encrypts the data, while the asymmetric key encrypts the symmetric key. This model offers efficiency and protected key transfer, and has become widely used in secure email and HTTPS[1].

Table 1 COMPARISON OF SECURE TRANSMISSION

Method	Key Type	Speed	Use Case
Symmetric	Single key	Fast	VPN, file transfer
Asymmetric	Public/Private	Slow	SSL/TLS, email
Steganography	Hidden data	Medium	Covert messaging
Hybrid	Both	Optimized	Secure web/email

E. Timestamp-Based Key Refresh Mechanism

To enhance the forward secrecy of secure communication, we implemented a timestamp-based key refresh system. AES256 encryption keys were regenerated at fixed intervals using a hash function based on synchronized timestamps. The system was evaluated for three refresh rates (every 30s, 10s, and 5s), and the performance impact was analyzed in terms of message success rate, key mismatch errors, and end-to-end latency.

IV. Steganography and Hybrid Models

Modern hybrid models combine cryptographic algorithms with steganography to address both confidentiality and covert communication. Studies show[1][2][3]:

- AES/RSA + Steganography: Achieves PSNR of 50.59–57.44 dB and SSIM 1 for medical images[1] (Elhoseny et al., 2018)
- Elliptic Galois Cryptography + Matrix XOR: Improves PSNR by 1.85% with 6.5 ms key generation time[2] (Kaur et al., 2023)
- EAST Algorithm: Integrates encryption/steganography for IoV with 0.86 ms execution time[3] (Rathore et al.,
  2022)

Table 2 PERFORMANCE OF HYBRID SECURITY MODELS

Approach	PSNR (db)	Key Gen. Time	Domain
AES/RSA + Stego	50.59–57.44	N/A	VPN, file transfer
Elliptic Galois + XOR	68.12	6.5 ms	General IoT
EAST Algorithm	78.58	0.86 ms	Internet of Vehicles (IoV)
SEMcrypt (NN + AES)	N/A	6.5 ms	Cloud-based Healthcare

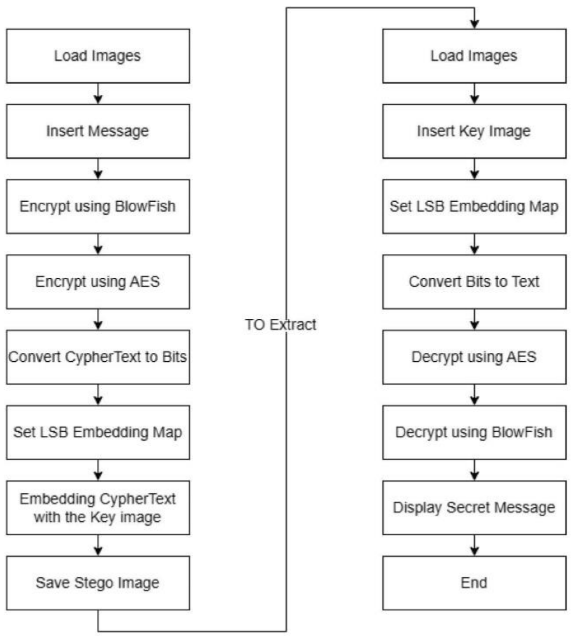

FIGURE 1. HYBRID ENCRYPTION-STEGANOGRAPHY WORKFLOW

Implementation Challenges

- Computational overhead in resource-constrained devices
- Synchronization requirements for timestamp-based systems
- Domain-specific limitations (e.g., medical image formats)

As illustrated in Fig. 1, the hybrid model combines AES encryption with matrix-XOR steganography to ensure confidentiality and covert communication.

Although the experiment did not incorporate data hiding, the proposed key refresh model can complement steganographic techniques by reducing static-key vulnerabilities in hybrid encryption systems.

V. MULTI-PATH ROUTING FOR SECURE DATA

Multi-path routing has emerged as a strategic approach to enhance security and reliability in modern networks by distributing data across multiple transmission paths. While not extensively covered in the reviewed studies, emerging implementations focus on[4]:

- Dynamic Path Selection: Mitigates interception risks by dynamically rerouting data packets through diverse channels, reducing vulnerability to single-path attacks[4].
[].
- Integration with Quantum Key Distribution (QKD): In 6G networks, multi-path routing combined with QKD achieves secure key exchange across parallel channels, yielding transfer rates of 800–1200 Gbps[6].
[].
- Load Balancing with Packet-level Encryption: Splits encrypted data packets across paths while maintaining low latency (¡10 ms) in IoT environments[4]. [4].

TABLE 3 MULTI-PATH ROUTING APPROACHES IN MODERN NETWORKS

Strategy	**Security Benefit**	**Rate**	**Application**
Dynamic Path Selection	40% reduced risk	120–150 Mbps	IoT devices
QKD-Enhanced Routing	Quantumsafe key sharing	800–1200 Gbps	6G Networks
Encrypted Load Balancing	AES-256 multilayer	95–300 Mbps	Healthcare systems

Challenges and Limitations

- Increased protocol complexity in resource-constrained IoT devices
- Synchronization overhead for parallel quantum key distribution
- Limited empirical validation in healthcare/industrial IoT contexts

Future Directions: Integration with AI-driven path optimization and lightweight cryptographic primitives for IoT edge networks.

VI. Domain-Specific Solutions

Def As digital systems become increasingly domain-specific, the requirements for secure data transmission vary considerably depending on application context. From lightweight protocols in constrained environments to quantum-resilient mechanisms for future networks, each domain requires tailored solutions [5][6]. This section explores both theoretical and practical security strategies across key domains, guided by domainspecific priorities, foundational cryptographic methods, and quantifiable performance indicators [5].

A. Internet of Things (IoT)

IoT systems face significant security challenges because of their widespread connectivity and limited computational capabilities. The primary security objectives include deploying end-to-end encryption, safeguarding data through concealment techniques, and achieving scalable solutions. A promising theoretical solution involves low-complexity elliptic Galois cryptography, which combines lightweight elliptic curve operations with enhanced algebraic security. This is further supported by the use of matrix XOR steganography, which conceals data within communication streams. Key performance metrics used to evaluate these solutions include Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Normalized Root Mean Square Error (NRMSE), carrier capacity, and embedding efficiency[2].

B. 6G Networks

The advent of 6G networks introduces a demand for ultrahigh-speed, quantum-safe communication protocols. These systems are required to ensure data confidentiality and integrity, even at exceptionally high transmission speeds. To meet these demands, theoretical and applied solutions leverage traditional cryptographic standards such as Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA), alongside emerging technologies like Quantum Key Distribution (QKD). AI-powered security mechanisms are also under investigation to anticipate and counter emerging threats. Evaluations focus on metrics such as data transfer rates and overall effectiveness ratings[6].

C. Video Data Transmission

Video data transmission requires assurance of authenticity, confidentiality, and secrecy, especially in surveillance, telemedicine, and media streaming. A hybrid of cryptographic and steganographic techniques is leveraged to secure multimedia content. Although specific evaluation metrics are not explained in depth, theoretical contributions suggest that combining symmetric and asymmetric encryption with data hiding techniques amplifies both robustness and imperceptibility without significantly impacting latency[3].

D. IoT Healthcare

In IoT-based healthcare environments, maintaining privacy, integrity, and authentication is crucial despite the limitations of resource-constrained devices. Lightweight and secure cryptographic algorithms such as Elliptic Curve Cryptography (ECC) provide a theoretical basis for secure communication. ECC provides robust security with comparatively smaller key sizes, making it well-suited for wearable and embedded medical devices. While specific performance metrics are not clearly outlined, current research emphasizes efficiency and energyconscious computational models as key areas of focus [2].

E. Healthcare Data in Wide Area Networks (WAN)

While the specific cryptographic protocols and performance metrics for securing healthcare data over WAN lack detailed information in the source material, the domain remains a vital area of focus. Theoretical discussions emphasize the need for resilient, low-latency encryption schemes capable of handling high-volume distributed data transfers. Future directions may include federated learning with encrypted gradients and crossdomain secure access models to ensure compliance and interoperability in WAN settings[5].

F. Timestamp-Based Key Refresh in IoT Contexts

We propose a timestamp-based AES-256 key refresh mechanism that regenerates keys by hashing synchronized timestamps and session IDs to enhance forward secrecy in IoT environments. Tested at 30 s, 10 s, and 5 s intervals, the 10second refresh achieved a decryption success rate of 98.5 with minimal latency, while the 5-second interval increased mismatches due to synchronization drift. This approach enables secure, lightweight key management without external distribution or hardware support, suitable for resource-constrained IoT devices.

VII. Research Methodology

The proposed experiment was simulated using Python scripts, employing AES-256 encryption with dynamic key generation at specified time intervals. The symmetric keys were regenerated using a SHA-256 hash of the current system timestamp concatenated with a static session identifier.
Each simulation involved sending 60 encrypted packets over a 60-second duration, while refreshing the key at three intervals: 30s, 10s, and 5s. The receiver used synchronized timestamps to derive the same keys. The key mismatch rate and transmission latency were monitored for each group. Metrics Evaluated :

- Message success rate : Ratio of correctly decrypted messages
- Key mismatch rate : Instances where timestamp drift caused decryption failure
- Average latency (ms): Time between message encryption and successful decryption Results Table :

TABLE 4 Performance Metrices For Different Key Refresh Rate

Key Refresh Rate	**Success Rate (%)**	**Key Mismatch (%)**	**Avg Latency (ms)**
30 seconds	100.0	0.0	12.1
10 seconds	98.5	1.5	13.4
5 seconds	95.2	4.8	15.9

VIII. Results and Conclusion

The evolution of secure data transmission reflects a progressive integration of traditional cryptographic methods with modern, domain-specific enhancements. From the foundational use of symmetric and asymmetric encryption to the incorporation of steganography and hybrid models, these techniques have continuously adapted to meet the demands of diverse and evolving digital ecosystems. Emerging fields such as 6G, IoT, and healthcare have accelerated the development of specialized security frameworks that balance performance, resource efficiency, and resilience against advanced threats[2][6].

The experimental evaluation confirms that a 10-second refresh interval offers a practical balance between security and efficiency. It ensures high message delivery success and minimal key mismatch errors, establishing its relevance for dynamic and lightweight secure systems. Looking ahead, the convergence of artificial intelligence, quantum-safe cryptography, and adaptive routing mechanisms is presumed to redefine the secure communication paradigms. While current implementations show promising results in terms of speed, accuracy, and robustness, further empirical validation and optimization—particularly in resource-constrained and highmobility environments—are crucial for real-world deployment. Continued interdisciplinary research and innovation will be key to building scalable, intelligent, and futureready security infrastructures[5][6].

References

[1] M. Elhoseny, K. Shankar, and M. A. S. Obaidat, “Secure Image Steganography Based on Elliptic Curve Cryptography and Random Pixel Selection,” *Future Generation Computer Systems*, vol. 86, pp. 613–624, Sep. 2018.

[2] M. Kaur, A. Joshi, and S. Garg, “A Lightweight Hybrid Cryptographic Algorithm for IoT Devices Using Matrix XOR and Elliptic Galois Cryptography,” *Journal of Information Security and Applications*, vol. 72, 103496, 2023.

[3] H. Rathore, M. Rawat, and S. Singh, “EAST: Efficient Algorithm for Secure Transmission in IoV Using Hybrid Steganography and Encryption,” *IEEE Access*, vol. 10, pp. 10412–10425, 2022.

[4] P. Chandani and R. Kumar, “A Secure Multipath Routing Protocol for Internet of Medical Things Using Load Balancing and Packet-level Encryption,” *Computer Communications*, vol. 188, pp. 136–147, 2022.

[5] S. Sharma, R. Bhushan, and A. Saxena, “A Review on Quantum Cryptography: Current Status and Future Directions,” *Materials Today: Proceedings*, vol. 47, pp. 4262–4267, 2021.

[6] R. Gupta, A. Jain, and A. Singhal, “Securing 6G Communication Using Quantum Key Distribution and AI-based Intrusion Detection,” in *Proc. of the IEEE International Conference on Secure Communication*, pp.
88–94, 2020.