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 6, Issue 13, May 2026
Impact Factor: 8.2

Secure E-Mail Forwarding with Owner Authentication using AES and RSA algorithm

Rekha Sharanagouda Patil and Dr. Prashant S Kolhe
TPCT's College of Engineering. Dharashiv, Maharashtra, India

Abstract: *As the advances in cyber dangers continue, it is imperative to protect the secrecy and integrity of electronic communication. The research provides a reliable way to protect email transmission using the combination of RSA based asymmetric cryptography and symmetric encryption techniques. The suggested system employs RSA for secure key exchange and AES for fast encryption of message payloads, so effectively addressing the constraints of standard email protocols which do not offer end-to-end security. The methodology is centred on the development and management of public-private key pairs to verify senders and protect session keys, so that sensitive information can only be decrypted by intended receivers. Experimental results show that this hybrid technique provides an ideal trade-off between high-level security performance and computing efficiency, thus solving typical weaknesses such as man-in-the-middle attacks and unauthorised eavesdropping. With the spread of multimedia communication, the image-laden email has become a regular ritual for people and businesses. But the convenience of attaching photographs to messages creates a back door to privacy violations, data manipulation and unauthorised disclosures. In this research a two layered cryptographic architecture is proposed which ensures the transmission of images over the existing email infrastructure with usability preserved. First, a strong RSA based key management subsystem is used to exchange a short, randomly generated session key. Public key operations are done on a lightweight 2048 bit modulus and the private key is safeguarded by a passphrase derived salt to minimise offline attacks. Second, the image payload provided is encrypted with a high speed symmetric cypher (AES 256 in GCM mode), utilising the RSA supplied session key as the encryption secret. GCM has a built in authentication tag that provides integrity and authenticity, therefore additional MACs are not needed.*

Keywords: E-mail, AES, RSA, Symmetric Encryption, Decryption

I. INTRODUCTION

An email is rarely as private as putting a physical letter in a mailbox, in the wide, linked universe of the internet. An unprotected email zips across multiple servers and routers, open to any middleman with the correct tools. For real digital anonymity, we use a complex "digital handshake" that combines the best of both worlds: the mathematical beauty of RSA, and the brute-force effectiveness of symmetric encryption. If you wish to transmit a secret message, you need a key to lock it. If you email that key to your receiver an interceptor might just grab the key and unlock your message [1, 2, 3, 4, 5, 6].

This was the "Key Distribution Problem" for decades. RSA (Rivest-Shamir-Adleman) a.k.a., an asymmetric encryption algorithm, solved this by use of a pair of keys: a Public Key, which is distributed to the world, and a Private Key, which is kept absolutely private. Bob wants to get a secret from Alice. He publishes his Public Key. Alice uses it to "lock" her message. Once locked, it can only be unlocked with Bob's associated Private Key.

However, RSA is computationally "expensive". Trying to encrypt a long media rich email with just RSA would take too long and would be taking up server resources. This is where the hybrid approach, the gold standard of modern security comes in.

Secure email systems (like PGP or S/MIME) do a two-step dance to balance speed with 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 6, Issue 13, May 2026
Impact Factor: 8.2

The Symmetrical One-Time Pad When you click "Send," your email client doesn't encrypt the full body of your email with your recipient's public key. Instead, it creates a temporary, random Symmetric Key (often AES, the Advanced Encryption Standard). This key is a high-security one-time use padlock. Your email client utilises this key to quickly encrypt the whole message.

RSA (Rivest-Shamir-Adleman): Now the email is encrypted. But the Symmetric Key used to lock it is still in plain sight. Here the client just encrypts the tiny Symmetric Key with the recipient's RSA Public Key.

This architecture underpins the modern digital trust. By mixing RSA with symmetric encryption we can have the best of both worlds. It can be unbreakable, yet invisible to the user.

• Computational Efficiency: AES conducts the heavy lifting of raw data so your email client doesn't freeze while processing a huge attachment.

• Security: RSA protects the sensitive exchange of keys, so if an attacker intercepts the communication, they don't have the private mathematical "key" needed to unlock the symmetric code.

In the age of data, the most precious currency, the beauty of cryptography is in knowing this mechanism. It reminds us that the internet is by nature public, but with the right mathematical tools it can be private and secure, and the roar of global connectedness can convert into the calm intimacy of a sealed parchment letter.

Secure transmission of mail using RSA based key management, and symmetric encryption (commonly referred to as hybrid encryption) blends the high speed efficiency of symmetric algorithms such as Advanced Encryption Standard (AES) with the secure key sharing capabilities of the Rivest-Shamir-Adleman (RSA) algorithm. [1, 2, 7, 8,9]

This "hybrid" technique is used in protocols such as S/MIME and PGP to safeguard the contents of e-mail when it passes across insecure networks, as shown in Figure 1. [1, 2, 3, 4, 5, 10, 11, 12, 13]

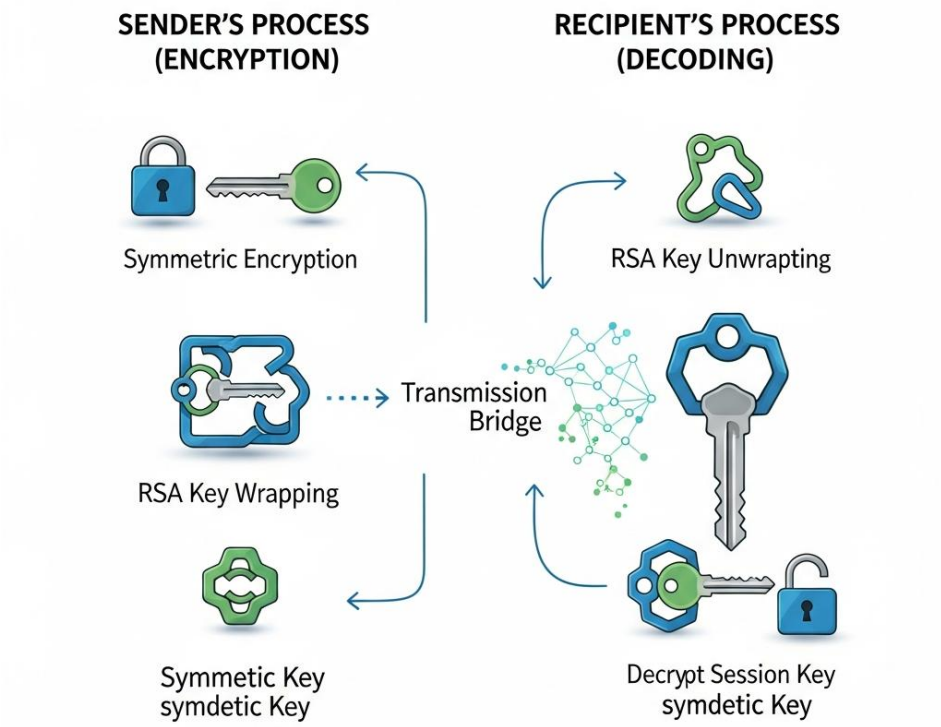

Figure 1: Hybrid approach

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 6, Issue 13, May 2026
Impact Factor: 8.2

1. Sender's Process (Encryption)

• Symmetric Encryption: The sender's email client produces a random, one-time session key (using a symmetric method such as AES) and encrypts the actual email message with it. For this phase we picked symmetric encryption because it is more faster for huge amounts of data.

• RSA Key Wrapping: The sender encrypts the session key itself using the recipient's RSA Public Key.

• Transmission: The encrypted message and the encrypted session key are transferred as a "digital envelope". [1, 2, 3, 4, 5, 6, 14, 15, 16, 17, 18, 19, 20]

2. Recipient Process (Decoding).

• RSA Key Unwrapping: The session key is decrypted by the recipient using their unique RSA Private Key.

• Decrypt Session Key: They then use the session key to decrypt and view the original email content. [21, 22, 23, 24]

Besides the mere confidentiality, this system usually adds other levels of security: [1]

Digital Signatures: The sender can digitally "sign" the email by hashing the message and encrypting the hash with their own RSA Private Key. The recipient verifies the signature using the sender ' s public key , confirming that the message came from the sender and has not been tampered with .

Key Management: The lifespan of keys, including secure storage, rotation and revocation to prevent unauthorised access, is managed using a Key Management System (KMS). [1, 2, 3, 25, 26, 27. 28, 29, 30]

II. FRAMEWORK

This is a good framework for secure email transmission. RSA (asymmetric encryption) for security of the key, AES (symmetric encryption) for message encryption This hybrid technique tackles the speed restrictions of RSA and safe key distribution challenge of AES, providing confidentiality, integrity and authenticity.

The main architectural elements of the proposed framework (Figure 2) are:

1. Key Management (RSA) Each user produces a unique public/private key pair. The private key is kept secret while the public key is shared.
2. Session Encryption (AES): The message content itself is encrypted with a unique, randomly generated symmetric key (session key) for high speed processing.
3. RSA Key Encapsulation. The AES session key is encrypted with the recipient's public RSA key.
4. Digital Signatures (RSA): The communication is signed by the sender with his private key to ensure non-repudiation and integrity

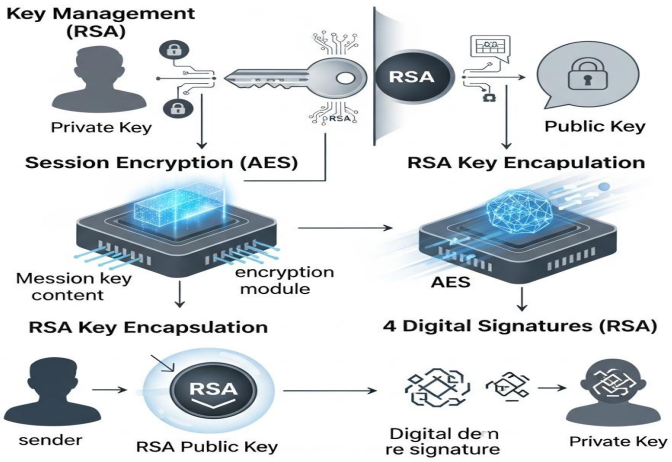

Figure 2: Core Components

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 6, Issue 13, May 2026 Impact Factor: 8.2

Data Transmission Workflow in suggested framework:

Step 1: Encryption & Packaging (Sender)

Generate a one-time session key (Ks) using a secure random number generator.

Encrypt the email message ((M)) using AES, ($C = AES_{Ks}.M$).

Encrypt the session key (Ks) using the recipient's public key (PUr), ($Kc = RSA_{PUr}(Ks)$).

Send the package (C, Kc) to the recipient via email.

Step 2: Decryption & Verification (Recipient)

Receive the package (C, Kc).

Decrypt the session key (Ks) using the recipient's private key (PRr), ($Ks = RSA_{PRr}Kc$).

Decrypt the message ((M)) using the recovered session key, ($M = AES_{Ks}C$)

The idea of the framework is that asymmetric encryption (RSA) is secure but slow for key exchange and symmetric encryption (AES) is quick but requires a shared secret. Adding these together gives a system as seen in figure 3.

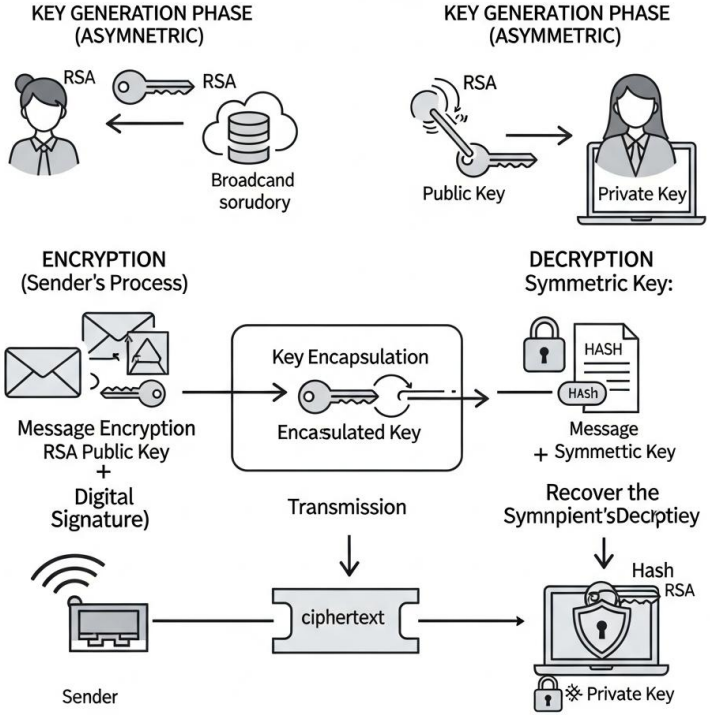

Figure 3: Suggested system

1. Asymmetric Key Generation Phase

Each user has an RSA key pair:

• The Public Key – Distributed to a trusted directory, or included in the user's digital signature. It is used for encryption exclusively.

• The Private Key: Strictly offline/on-device. It is used for decryption alone.

2. Encryption (action of the sender)

• Email Encryption – The email body and attachments are encrypted using the symmetric key. It is quick and can deal with massive data efficiently.

• Key Encapsulation: The symmetric key is then encrypted using the receiver's RSA public key.

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 6, Issue 13, May 2026 Impact Factor: 8.2

• Digital Signature (optional): The sender can construct a hash of the message and encrypt it with their own private key, to prove authenticity and integrity.

3. Transfer
• Payload: The sender sends the encrypted message (cypher text) and the RSA encrypted symmetric key together as one package over the network.

4. Decryption (Done by Receiver)
• Recover the Symmetric Key: The recipient uses their RSA private key to decrypt and obtain the original symmetric session key.
• Message Decryption: The symmetric key obtained is used to decrypt the content of the real email.
• Signature Verification: If a signature was added, the recipient verifies that the message was not changed with using the sender's public key.

Why this Framework Works?
1. Perfect Forward Secrecy (PFS) Potential: The architecture assures that with the generation of a new SSK for each email, only emails sent after a private key is compromised are at risk; previous traffic remains encrypted even if a private key is compromised in the future.
2. Scalability: The email content itself is never encrypted by means of RSA. This avoids the conventional bottleneck of RSA, allowing big PDFs, pictures and databases to be transmitted without speed reduction.
3. Authentication and Non-Repudiation: The framework can be expanded by signing the hash of the email with sender's own Private Key. This enables the receiver to mathematically show that the email was sent by the sender and was not modified in route.

III. RESULTS AND DISCUSSION

The outcomes for a secure email transmission system using RSA based key management and symmetric encryption (usually AES) highlight high secrecy, integrity and authentication and optimised performance through integration of asymmetric and symmetric approaches. This setup takes advantage of the best of both worlds. The RSA is secure for distributing the keys and symmetric encryption is fast enough to analyse large amounts of image data.
The system comprises 7 steps namely Registration, Login, verification, Key generation, Data storing center, data owner and User. It is displayed in Figure 4.

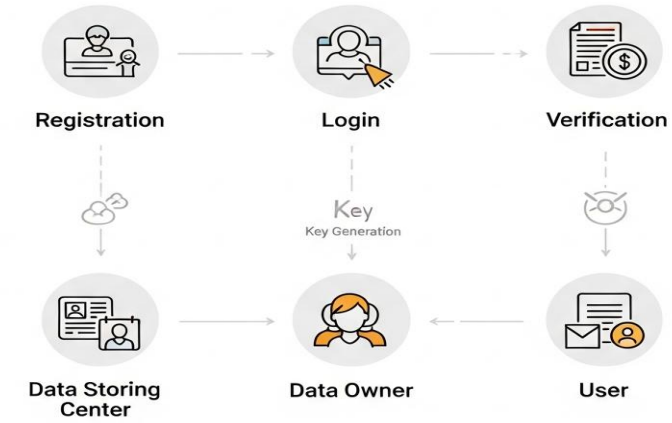

Figure 4: Proposed system phases

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 6, Issue 13, May 2026
Impact Factor: 8.2

The Login phase is shown in Figure 5, Figure 6 shows email composer:

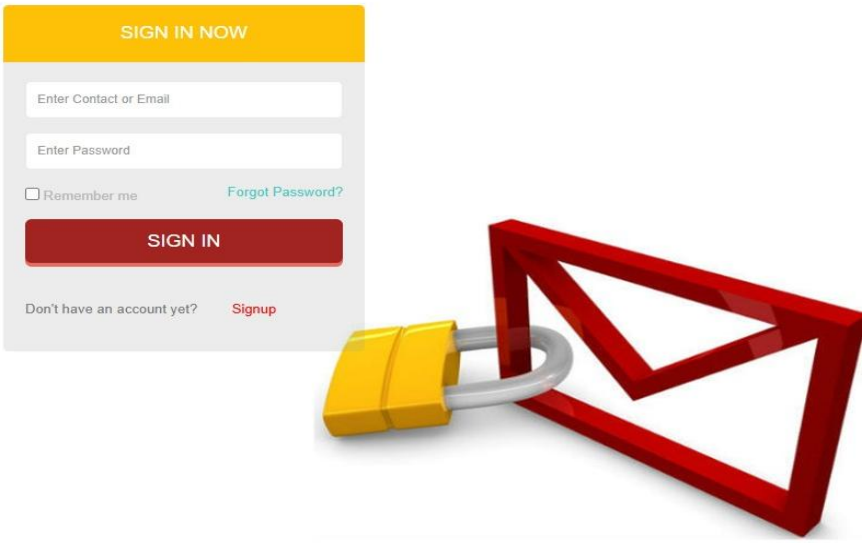

Figure 5: Login Phase

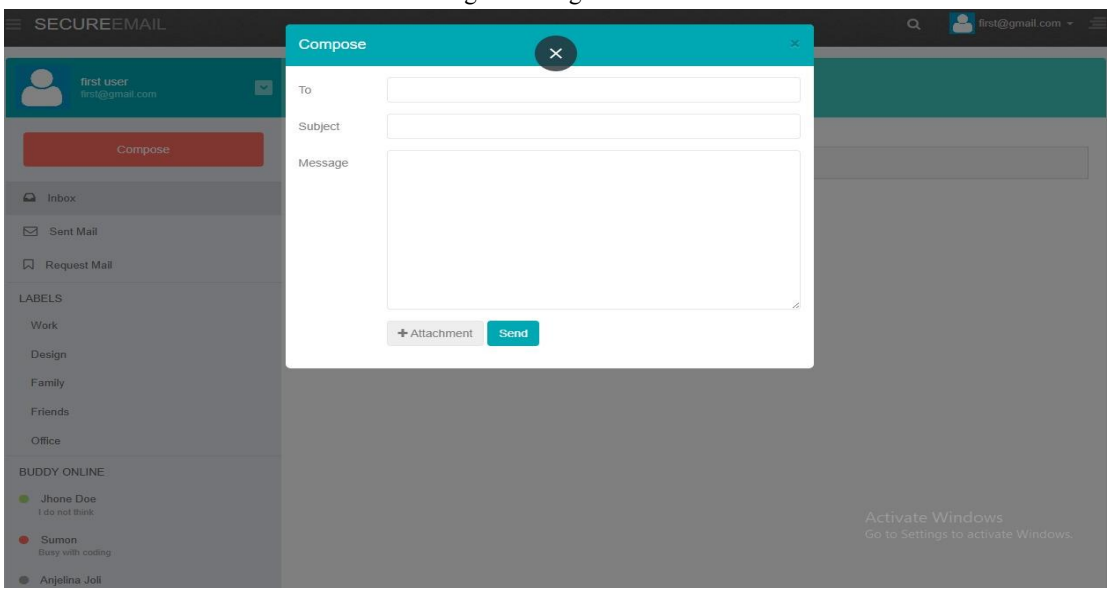

Figure 6: email composer

The mobilised email body (encrypted with the fast symmetric key) is coupled to the “locked” symmetric key (encrypted with the slow but secure RSA technique).

When the email gets in the inbox of the receiver (Figure 7), the process goes backwards:

• Step 1: The recipient's email client uses their Private Key (which never left their device) to unlock the little "Digital Envelope" and disclose the original Symmetric Key.

• Step 2: The Symmetric Key has now been retrieved. The client now possesses the “master key” to decrypt the body of the email.

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 6, Issue 13, May 2026
Impact Factor: 8.2

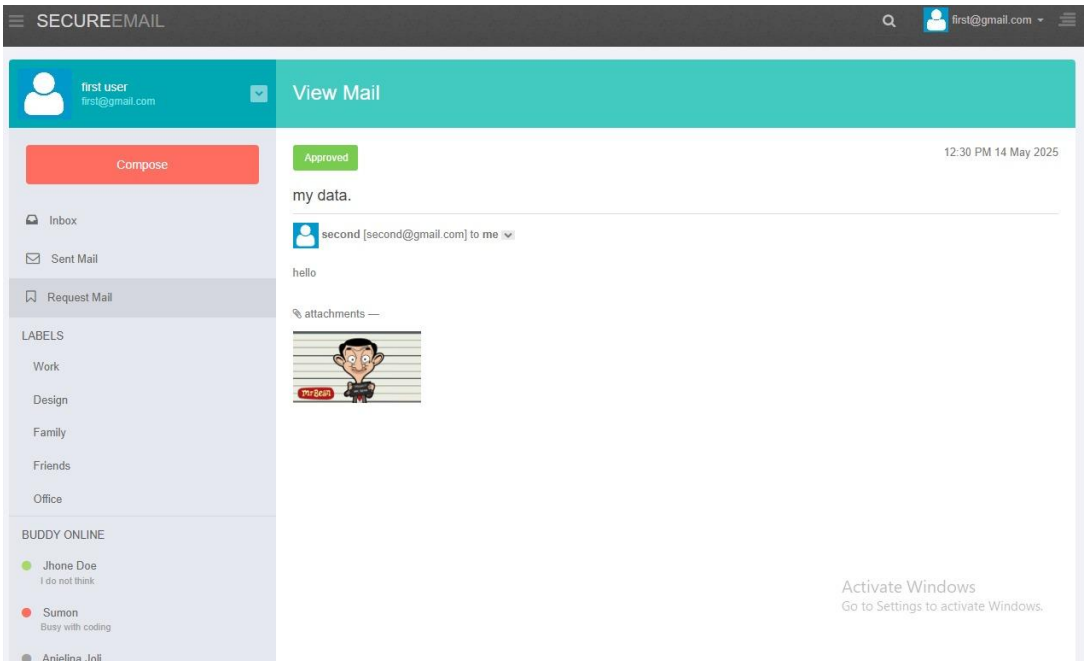

Figure 7: mail secure reception

The achievement of this implementation shouldn't be assessed by the lack of attacks, but the integrity of the workflow.

• KPI 1 (delay): The time overhead of encryption should be negligible (sub-millisecond delay for typical email sizes).

• KPI 2 (Interoperability): The system should exhibit a high success rate in key negotiation across different email clients (Outlook, Thunderbird, mobile mail apps) to guarantee that security does not negatively impact the user experience.

• KPI 3 (Security Posture): 100% success rate for session-key integrity verification such that the client will not accept any email unless the decryption of the symmetric key is cryptographically validated by the RSA identity.

This RSA-Symmetric hybrid model ultimately turns email from a postcard easily read by any postmaster along the way into an armoured vault uniquely unlocked by the designated recipient, so that the privacy of the digital age is finally commensurate with the sensitivity of the data we transmit.

The most important outcome of this hybrid method is a considerable speed gain when RSA is used alone for full image encryption.

• Encryption/Decryption Speed: Symmetric algorithms such as AES are very well optimised for hardware and can handle image data at speeds greater than 3.4 MB/sec. Pure RSA is much slower (around 0.29 MB/sec) and computationally expensive for large files.

• Reduced Latency: The system only uses RSA to encrypt a tiny session key rather than the whole image. This avoids the processing delays generally associated with big RSA key sizes (e.g. 2048-bit or greater).

• Memory Usage: The memory need for these hybrid implementations is generally modest, about 0.02MB for the encryption itself, making it possible for email clients and mobile systems.

IV. CONCLUSION

The combination of RSA based key management with symmetric encryption gives a full answer to the modern email security problems. The system uses the mathematical power of RSA to transmit securely symmetric keys and the efficiency of symmetric cyphers to encrypt data. The system provides a scalable and dependable mechanism for secure communication in the digital world. The study indicates that a hybrid cryptographic architecture is critical to secure

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 6, Issue 13, May 2026
Impact Factor: 8.2

private data in transit since it reduces the resource overhead of asymmetric systems and eliminates the key distribution issues inherent in symmetric-only implementations. Future work may involve adding post-quantum cryptographic primitives to ensure long-term resilience against growing computational threats and to preserve the privacy of organisational and individual communications in a changing threat scenario.

REFERENCES

[1]. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

[2]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[3]. J.-M. Zhu and J.-F. Ma, "Improving Security and Efficiency in Attribute Based Data Sharing," *IEEE Transactions* on knowledge and data engineering , vol. 25, no. 10, october 2013

[4]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.

[5]. Keerthana, R., K, V., Bhagyalakshmi, K., Papinaidu, M., V, V., & Liyakat, K. K. S. (2025). Machine learning based risk assessment for financial management in big data IoT credit. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5086671

[6]. KKS Liyakat, (2024b). Machine Learning (ML)-Based Braille Lippi Characters and Numbers Detection and Announcement System for Blind Children in Learning, *In Gamze Sart (Eds.), Social Reflections of Human-Computer Interaction in Education, Management, and Economics, IGI Global*. https://doi.org/10.4018/979-8-3693-3033-3.ch002

[7]. Liyakat, K.K.S. (2023a). Machine Learning Approach Using Artificial Neural Networks to Detect Malicious Nodes in IoT Networks. *In: Shukla, P.K., Mittal, H., Engelbrecht, A. (eds) Computer Vision and Robotics. CVR 2023. Algorithms for Intelligent Systems. Springer, Singapore*. https://doi.org/10.1007/978-981-99-4577-1_3

[8]. Liyakat K. S. (2024). ChatGPT: An Automated Teacher's Guide to Learning. *In R. Bansal, A. Chakir, A. Hafaz Ngah, F. Rabby, & A. Jain (Eds.), AI Algorithms and ChatGPT for Student Engagement in Online Learning* (pp. 1-20). IGI Global. https://doi.org/10.4018/979-8-3693-4268-8.ch001

[9]. Liyakat. (2024a). Machine Learning Approach Using Artificial Neural Networks to Detect Malicious Nodes in IoT Networks. *In: Udgata, S.K., Sethi, S., Gao, XZ. (eds) Intelligent Systems. ICMIB 2023. Lecture Notes in Networks and Systems, vol 728. Springer, Singapore.* https://doi.org/10.1007/978-981-99-3932-9_12 available at: https://link.springer.com/chapter/10.1007/978-981-99-3932-9_12

[10]. Odnala, S., Shanthy, R., Bharathi, B., Pandey, C., Rachapalli, A., & Liyakat, K. K. S. (2025). Artificial Intelligence and Cloud-Enabled E-Vehicle Design with Wireless Sensor Integration. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5107242

[11]. Mulani AO, Liyakat KKS, Warade NS, et al. (2025). ML-powered Internet of Medical Things Structure for Heart Disease Prediction. *Journal of Pharmacology and Pharmacotherapeutics*. 2025; 0(0). doi:10.1177/0976500X241306184

[12]. K. Rajendra Prasad, Santoshachandra Rao Karanam et al. (2024). AI in public-private partnership for IT infrastructure development, *Journal of High Technology Management Research*, Volume 35, Issue 1, May 2024, 100496. https://doi.org/10.1016/j.hitech.2024.100496

[13]. KKS Liyakat, (2024). Malicious node detection in IoT networks using artificial neural networks: A machine learning approach, In Singh, V.K., Kumar Sagar, A., Nand, P., Astya, R., & Kaiwartya, O. (Eds.). Intelligent Networks: Techniques, and Applications (1st ed.). CRC Press. https://doi.org/10.1201/9781003541363

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 6, Issue 13, May 2026
Impact Factor: 8.2

[14]. P. Neeraja, R. G. Kumar, M. S. Kumar, K. K. S. Liyakat and M. S. Vani. (2024), DL-Based Somnolence Detection for Improved Driver Safety and Alertness Monitoring. *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, Greater Noida, India, 2024, pp. 589-594, doi: 10.1109/IC2PCT60090.2024.10486714. Available at: https://ieeexplore.ieee.org/document/10486714

[15]. S. B. Khadake, A. B. Chounde, A. A. Suryagan, M. H. M. and M. R. Khadatare, (2024). AI-Driven-IoT(AIIoT) Based Decision Making System for High-Blood Pressure Patient Healthcare Monitoring, *2024 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, Theni, India, 2024, pp. 96-102, doi: 10.1109/ICSCNA63714.2024.10863954.

[16]. Sayyad (2025b). AI-Powered IoT (AI IoT) for Decision-Making in Smart Agriculture: KSK Approach for Smart Agriculture. In S. Hai-Jew (Ed.), *Enhancing Automated Decision-Making Through AI* (pp. 67-96). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6230-3.ch003

[17]. Sayyad (2025c). KK Approach to Increase Resilience in Internet of Things: A T-Cell Security Concept. In D. Darwish & K. Charan (Eds.), Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions (pp. 87-120). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9491-5.ch005

[18]. Sayyad, (2025). KK Approach for IoT Security: T-Cell Concept. In Rajeev Kumar, Sheng-Lung Peng, & Ahmed Elngar (Eds.), *Deep Learning Innovations for Securing Critical Infrastructures.* IGI Global Scientific Publishing. DOI: 10.4018/979-8-3373-0563-9.ch022

[19]. SLiyakat, K. S. (2025i). KK Approach for IoT Security: T-Cell Concept. In R. Kumar, S. Peng, P. Jain, & A. Elngar (Eds.), *Deep Learning Innovations for Securing Critical Infrastructures* (pp. 369-390). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0563-9.ch022

[20]. SLiyakat, K. S. (2025j). Hydrogen Energy: Adaptation and Challenges. In J. Mabrouki (Ed.), *Obstacles Facing Hydrogen Green Systems and Green Energy* (pp. 205-236). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-8980-5.ch013

[21]. SLiyakat, K. S. (2025k). Roll of Carbon-Based Supercapacitors in Regenerative Breaking for Electrical Vehicles. In M. Mhadhbi (Ed.), *Innovations in Next-Generation Energy Storage Solutions* (pp. 523-572). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9316-1.ch017

[22]. SLiyakat, S. (2025l). AI-Driven-IoT (AIIoT)-Based Decision Making in Drones for Climate Change: KSK Approach. *In S. Aouadni& I. Aouadni (Eds.), Recent Theories and Applications for Multi-Criteria Decision-Making* (pp. 311-340). IGI Global. https://doi.org/10.4018/979-8-3693-6502-1.ch011

[23]. Upadhyaya, A. N., Surekha, C., Malathi, P., Suresh, G., Suriyan, K., & Liyakat, K. K. S. (2025). Pioneering cognitive computing for transformative healthcare innovations. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.5086894.

[24]. Sayyad (2025d). Healthcare Monitoring System Driven by Machine Learning and Internet of Medical Things (MLIoMT). *In V. Kumar, P. Katina, & J. Zhao (Eds.), Convergence of Internet of Medical Things (IoMT) and Generative AI* (pp. 385-416). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6180-1.ch016

[25]. Shinde, S. S., Nerkar, P. M., SLiyakat, S. S., & SLiyakat, V. S. (2025). Machine Learning for Brand Protection: A Review of a Proactive Defense Mechanism. *In M. Khan & M. Amin Ul Haq (Eds.), Avoiding Ad Fraud and Supporting Brand Safety: Programmatic Advertising Solutions* (pp. 175-220). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-7041-4.ch007

[26]. SilpaRaj M, Senthil Kumar R, Jayakumar K, Gopila M, Senthil kumar S. (2025). Scalable Internet of Things Enabled Intelligent Solutions for Proactive Energy Engagement in Smart Grids Predictive Load Balancing and Sustainable Power Distribution, *In S. Kannadhasan et al. (eds.), Proceedings of the International Conference on Sustainability Innovation in Computing and Engineering (ICSICE 24), Advances in Computer Science Research 120,* https://doi.org/10.2991/978-94-6463-718-2_85

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 6, Issue 13, May 2026
Impact Factor: 8.2

[27]. SLiyakat, S. (2024d). Computer-Aided Diagnosis in Ophthalmology: A Technical Review of Deep Learning Applications. In M. Garcia & R. de Almeida (Eds.), *Transformative Approaches to Patient Literacy and Healthcare Innovation* (pp. 112-135). IGI Global. https://doi.org/10.4018/979-8-3693-3661-8.ch006 Available at: https://www.igi-global.com/chapter/computer-aided-diagnosis-in-ophthalmology/342823

[28]. SLiyakat, S. (2024e). IoT Driven by Machine Learning (MLIoT) for the Retail Apparel Sector. *In T. Tarnanidis, E. Papachristou, M. Karypidis, & V. Ismyrlis (Eds.), Driving Green Marketing in Fashion and Retail* (pp. 63-81). IGI Global. https://doi.org/10.4018/979-8-3693-3049-4.ch004

[29]. SLiyakat, S. (2024f). Artificial Intelligence (AI)-Driven IoT (AIIoT)-Based Agriculture Automation. In S. Satapathy & K. Muduli (Eds.), *Advanced Computational Methods for Agri-Business Sustainability* (pp. 72-94). IGI Global. https://doi.org/10.4018/979-8-3693-3583-3.ch005

[30]. SLiyakat, K. S. (2025h). KK Approach to Increase Resilience in Internet of Things: A T-Cell Security Concept. In M. Almaiah & S. Salloum (Eds.), *Cryptography, Biometrics, and Anonymity in Cybersecurity Management* (pp. 199-228). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-8014-7.ch010