WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

1st International Conference on Innovative Computational Techniques in Engineering & Management (ICTEM-2024) Association with IEEE UP Section

R.A.K.S.H.I.T.: Robust Application for Keeping Security through Hybrid Encoding in IT Ecosystem using Python and Assessment of Legal Framework

Dhairya Sarswat[1], Utkarsh Saxena[2], Akshdeep Singh[3], Kanchan Rani[4], Prachi Agarwal[5], Shiwani Agarwal[6]

[1,2,3,4,5,6]Computer Science and Engineering Department, Moradabad Institute of Technology Moradabad, India
[1]dhairyasarswatwork2005@gmail.com, [2]saxenautkarsh144@gmail.com, [3]akshsingh977@gmail.com, [4]kanchansinghcs@gmail.com
[5]reachtoprachi@gmail.com, [6]shiwani.agarwal91@gmail.com
DOI: https://doi.org/10.55248/gengpi.6.sp525.1955

Abstract

With advancements in the digital landscape the emphasis of netizens on privacy and informational security, and secure data transmission methods, have become a top priority. This paper presents a comprehensive study and a system designed for secure data transmission with multiple modules such as cryptography, steganography, and hybrid encryption. R.A.K.S.H.I.T. is a novel application designed to enhance data security using a hybrid approach combining cryptography and steganography. The system provides users with the ability to select their preferred method for securing data based on the sensitivity of information. The system employs a combination of cryptographic algorithms to encrypt data, while also utilising steganographic techniques to embed encrypted information within multimedia files, ensuring that data remains concealed against unauthorised access. Integration of these two security layers enhances data confidentiality and mitigates the risk of detection in transmission. The initial results from the implementation of the system demonstrate its effectiveness in securely encrypting and embedding data, securely.

Keywords *Data Security, Cryptography, Steganography, Secure Data Transmission, Modular Application*

1 Introduction

1.1 Background

In today's interconnected world, secure communication has become paramount. There has been significant growth in the exchange of data across all digital platforms, thereby ensuring both data privacy and security has become critical. A recent report conducted by IBM in collaboration with the Ponemon Institute, known as the "Cost of a Data Breach Report 2024" revealed that the global cost of an average data breach has risen to USD 4.88 million in 2024, marking a 10% increase from the previous year, which is the highest cost recorded so far. It was also revealed that the organisations that utilized security AI and automation extensively in breach prevention saved an average of USD 2.22 million compared to those that did not. Furthermore, 40% of the breaches involved data stored across multiple environments. Breached data stored in public clouds incurred the highest average breach cost at USD 5.17 million.

Table 1 Key Data from the Cost of a Data Breach Report 2024

Key Data	Value
Global Average Cost of a Data Breach	USD 4.88M
Increase from last year	10%
Breaches Involving Shadow Data	33%
Cost Savings with AI	USD 2.22M
Highest Cost (Public Cloud)	USD 5.17M
Secured Gen AI Initiatives	24%
Post-Breach Response Cost Impact	75% increase
Breaches Across Multiple Environments	40%
AI & Automation Cost Reduction	USD 2.22M

As shown in Table 1, industries need to invest heavily in AI, automation, and post-breach response preparedness to reduce the financial impact of breaches and enhance their overall security posture.

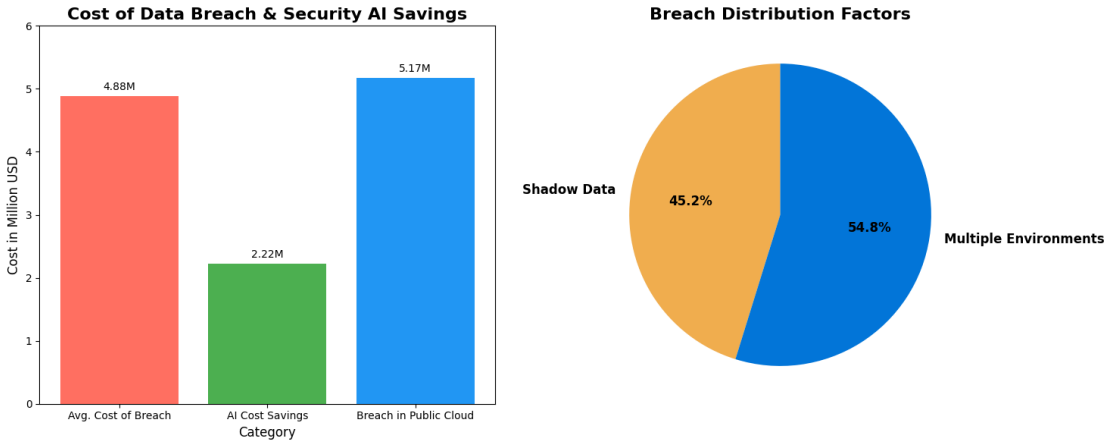

Figure 1 Cost of Data Breach and Security AI Savings. Left: Average breach costs, AI savings, and cloud breach costs. Right: Distribution of breaches involving shadow data and multiple environments.

As we already know cyber attacks have become a dominant form of warfare, with state-sponsored groups targeting critical sectors. These cyber operations, often involve highly sophisticated and persistent threats and are designed to disrupt essential infrastructure, steal sensitive information, and destabilize political and economic systems. The energy, telecommunications, healthcare, and defence sectors are particularly vulnerable, as a successful attack can not only cause financial damage but also pose significant national security risks. The growing trend of digital warfare underscores the necessity of robust cybersecurity frameworks and international cooperation to mitigate these evolving threats.

The role of encryption and data protection in preventing unauthorized access and ensuring data confidentiality is crucial in maintaining the integrity and privacy of sensitive information. The encryption process transforms data into an unreadable format, which can only be reversed by authorized users with the appropriate decryption key. This process ensures that even if data is intercepted during transmission or accessed by unauthorized individuals, it remains protected and unusable. Data protection mechanisms, such as secure access controls, multi-factor authentication, and robust encryption standards, act as barriers against cyberattacks and data breaches. By implementing these measures, organizations can reduce the risk of data leakage and mitigate the potential damage caused by unauthorized access. In sectors like finance, healthcare, government, and communication, where data breaches can have severe legal, financial, and reputational consequences, encryption and data protection are the need of the hour. These tools not only safeguard against external threats but also help organizations comply with data privacy regulations, such as GDPR or HIPAA, ensuring that they meet legal requirements while protecting individuals' sensitive information.

1.2 Problem

Despite the advancements in cybersecurity technologies and applications, the rapid evolution of attack methods such as phishing, and advanced persistent threats (APTs), poses a significant risk against the defensive measures put in place by many organizations. In addition to external threats, the rise of insider threats and vulnerabilities due to insufficient employee training, inadequate access controls, and misconfigured systems deepens the problem.

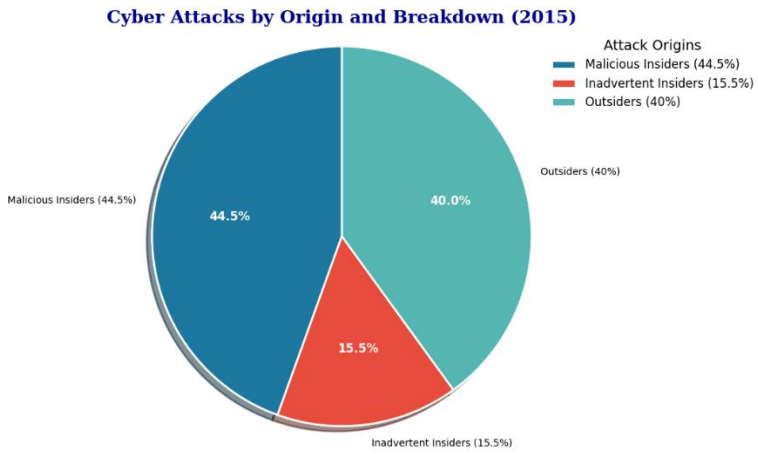

Figure 2 Distribution of Cyber Attacks by Origin of Attacker (2015)

Figure 2 shows that, as per Statista, the origin of cyber attacks in 2015, highlights the significant role of insiders in these breaches. According to the data, 60% of cyber attacks were perpetrated by insiders, with 44.5% being malicious insiders and 15.5% caused by inadvertent actors. In contrast, outsiders accounted for 40% of the attacks. This breakdown emphasizes the need for robust internal security measures and a deeper focus on monitoring and controlling access within organizations, as insiders are often in a unique position to exploit vulnerabilities. The visual representation helps underscore the importance of addressing insider threats as a critical aspect of cybersecurity strategy.

This analysis therefore underscores the critical need for multifaceted approaches to cybersecurity, such as those proposed in R.A.K.S.H.I.T., where hybrid techniques like the integration of cryptography and steganography can not only secure data against external threats but also mitigate risks from insider actors. By embedding data within multimedia and applying robust encryption methods, the system addresses vulnerabilities that could otherwise be exploited by insiders since they have easy access to sensitive information. This approach highlights the importance of incorporating advanced security systems into organizational cybersecurity strategies to safeguard data against both internal and external threats.

1.3 Contribution

This paper presents a modular system developed using Python technology which combines cryptography and steganography into a user-friendly environment for secure data transmission. By providing a streamlined, accessible and responsive GUI, the system allows its users to achieve high levels of security through a hybrid technique without the requirement of any extensive technical knowledge. The system encrypts messages with robust cryptographic algorithms and subsequently embeds this encrypted data within a carrier file, such as an image, to protect against detection and decryption attempts.

The system in itself is a comprehensive integration of selectable modules where users can select their preferred data security methods (e.g., AES, RSA, or LSB encoding) based on the sensitivity and context of their data. Thus by combining encryption and steganographic embeddings, we created a dual-layered security framework that enhances data confidentiality and reduces the risk of unauthorized detection. Moreover, this study analyzes and provides insights into the current state of cyber laws, highlighting gaps, and recommending legal measures to better protect encrypted and steganographically hidden data.

It also functions as the groundwork for further enhancements in the field, including potential integration with emerging technologies like blockchain for data integrity and AI for threat detection. This solution is suitable for a wide range of applications, from secure military communications to safeguarding sensitive corporate data, providing a practical tool that demonstrates both robust protection and accessibility in secure data transmission.

2 Relate Work

2.1 Existing Research

In our study, we analyzed over 30 research papers from various sources to gain insights into the current landscape of cybersecurity, cryptography, and related technologies. The majority of the research emphasizes advancements in cryptographic techniques, with a growing focus on post-quantum cryptography and AI-driven cybersecurity solutions. Quantum computing has emerged as a key area of interest, especially regarding its implications for existing encryption methods and the development of quantum-resistant systems.

Table 2 Classification of Research Papers

Field	Number of Papers
Cryptography and Algorithms	12
Artificial Intelligence in Cybersecurity	11
Quantum Computing and Security	10
Cybersecurity Applications	7
Education and Workforce Development	1

From the above table, it can be concluded that cryptography and algorithms are the most heavily explored areas, which is an indication of a significant focus on cryptographic techniques, algorithms, and their applications in enhancing cybersecurity and a secure and robust data transmission process. Artificial Intelligence in Cybersecurity also represents a major area of interest. This suggests a growing trend of integrating AI and machine learning to improve security measures, identify threats, and automate decision-making in cybersecurity.

Meanwhile, Quantum Computing and Security is another prominent area. This reflects the increasing importance of quantum technologies in addressing the challenges posed by traditional cryptographic systems, particularly in the context of post-quantum cryptography. While Education and Workforce Development has the least number of papers, this suggests an opportunity for growth and future potential. As cybersecurity continues to evolve rapidly, the demand for skilled professionals and comprehensive training programs will likely increase.

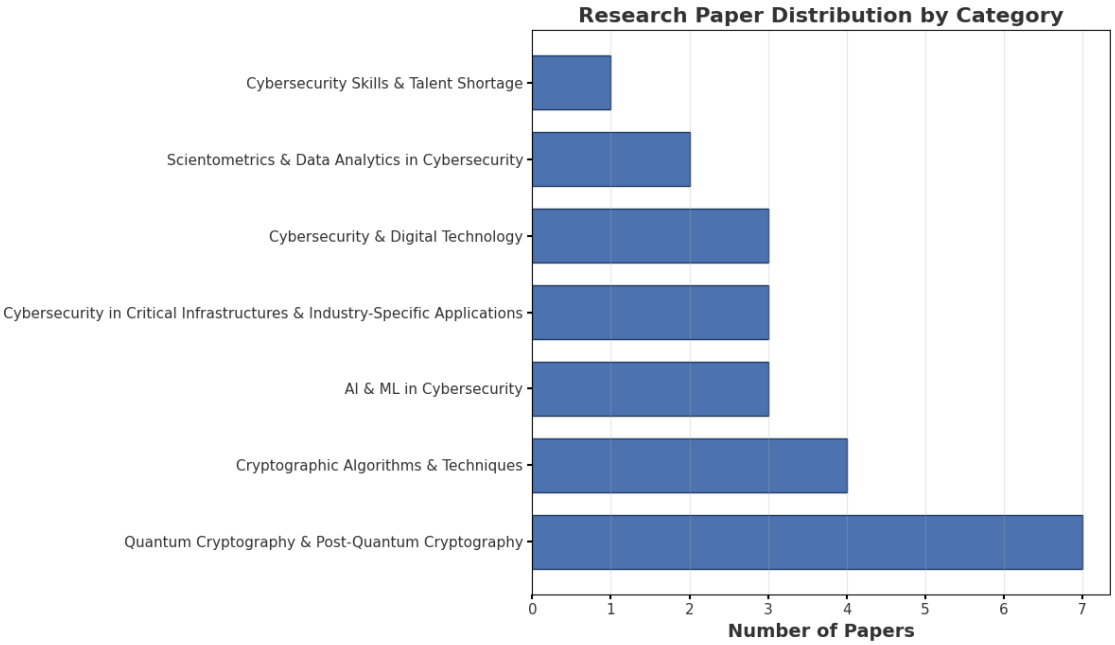

Figure 3 Distribution of Research Papers by Category in Cybersecurity

Table 3 Classification of Research Papers (1-6)

ID	Focus Area	Technologies/Methods
1	Quantum Computing	Cryptography, Quantum Security
2	Critical Infrastructure	Cryptography Frameworks
3	Post-Quantum Cryptography	Post-Quantum Cryptography
4	Cryptography	Quantum Computing, Cryptography
5	AI, Cryptography	AI, Blockchain, Cryptography
6	Cybersecurity	Post-Quantum Cryptography

Table 4 Classification of Research Papers (7-12)

ID	Focus Area	Technologies/Methods
7	Quantum Computing	Quantum Computing, Cryptography
8	AI, Quantum Computing	AI, Quantum Security
9	Industrial Sector	Cryptography Algorithms
10	Information Security	Advanced Digital Technologies
11	Cyber-Attacks, Power Systems	Cyber-Attacks, Detection
12	AI, Quantum Computing	AI, Quantum Computing

Table 5 Classification of Research Papers (13-18)

ID	Focus Area	Technologies/Methods
13	Artificial General Intelligence	AI, AGI
14	Cybersecurity	Post-Quantum Cryptography
15	Quantum Computing	Quantum Encryption
16	AI, Cryptography	AI, Cyber Defense
17	Post-Quantum Cryptography	Quantum-Resilient Cryptography
18	AI, Machine Learning, Cybersecurity	ML, AI, Real-time Detection

Table 6 Classification of Research Papers (19-25)

ID	Focus Area	Technologies/Methods
19	Quantum Cryptography	Quantum Cryptography
20	Software Implementation	Quantum Cryptography Systems
21	Quantum Computing	Quantum Methods for Security
22	Data Protection	Data Encryption, Security
23	Networks	Network Security
24	Cryptography, AI	Hybrid Cryptography Algorithms

25	Quantum Computing	Quantum Methods

Tables III to VI provide an overview of the significant research in the fields of cryptography, artificial intelligence (AI), quantum computing, and cybersecurity, as well as the latest advancements in post-quantum cryptography and their applications. The research papers highlighted the diverse focus areas and methods used across various studies, ranging from quantum encryption techniques to AI-driven cybersecurity solutions.

2.2 Preliminaries

In order to develop a secure data transmission system, it is essential to understand the fundamental concepts behind cryptographic and steganographic techniques. The term "cryptography" is defined as the science of securing communication and data by transforming information into an unreadable format, thereby ensuring confidentiality, integrity, and authenticity. It can further be categorised into two sub-types:

- **Symmetric Cryptography:** In symmetric cryptography, both the sender and receiver use the same key to encrypt and decrypt the message. Well-known algorithms in this category include the Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

An example of symmetric cryptography is Data Encryption Standard (DES), whose process has been described below:

Key Notations: Let the 64-bit plaintext be *P*, and the 56-bit key be *K*.

The first step in the DES encryption process is the initial permutation (IP), where the plaintext is rearranged using a fixed permutation function. This can be represented as:

$$IP(P) = (P1, P2, \ldots, P64) \quad (1)$$

The key scheduling process generates 16 subkeys, K1, K2, . . . , K16, from the 56-bit key K. The key scheduling process involves the following steps:

The 56-bit key *K* undergoes a permutation Π1 to generate the first key *K1*:

$$K1 = \Pi 1\,(K) \quad (2)$$

The key K_1 is split into two 28-bit halves, C_0 and D_0:

$$K_1 = (C_0, D_0) \quad (3)$$

Each of these halves is then shifted left by one or two positions as per the round number.

After each shift, a 48-bit subkey K_i is generated using the permutation Π_2:

$$K_i = \Pi_2(C_i \parallel D_i) \quad (4)$$

In each round i, the 64-bit block is divided into two halves: L_i (left) and R_i (right). The following steps are performed during each round:

The right half R_i is expanded to 48 bits using the expansion permutation E:

$$R_i^{(exp)} = E(R_i) \quad (5)$$

The expanded right half is then XORed with the subkey K_i:

$$R_i^{(exp)} \oplus K_i \quad (6)$$

The result from the XOR operation is split into 8 blocks of 6 bits, each passed through a substitution box S, producing a 4-bit output:

$$S_i = S(R_i^{(exp)} \oplus K_i) \quad (7)$$

The output from the substitution is permuted using the permutation function P:

$$P_i = P(S_i) \quad (8)$$

The result is then XORed with the left half L_i:

$$L_{i+1} = L_i \oplus P_i \quad (9)$$

The new right half for the next round is simply the previous left half:

$$R_{i+1} = L_i \quad (10)$$

After completing 16 rounds, the final ciphertext is obtained by combining the last left and right halves, followed by the final permutation Π_3:

$$\text{Ciphertext} = \Pi_3(L_{16} \parallel R_{16}) \quad (11)$$

- **Asymmetric Cryptography:** Asymmetric cryptography uses a pair of keys: one for encryption (public key) and another for decryption (private key). The Rivest-Shamir-Adleman (RSA) algorithm is a widely used example. The process behind RSA algorithm is as follows:

Key Notations: Let p and q be two large prime numbers, and $n = p \times q$. The public key is (n, e), where e is the encryption exponent, and the private key is (n, d), where d is the decryption exponent.

The RSA encryption and decryption processes are as follows:

- Choose two large prime numbers p and q.
- Compute $n = p \times q$.
- Compute the Euler's totient function $\phi(n) = (p - 1)(q - 1)$.
- Choose the public exponent e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
- Compute the private exponent d such that:

$$d \times e \equiv 1 \pmod{\phi(n)} \quad (12)$$

Thus, the public key is (n, e) and the private key is (n, d).

Encryption:
For a message M, the ciphertext C is computed using the public key (n, e) as follows:

$$C = M^e \pmod{n} \quad (13)$$

Decryption:
The receiver uses their private key (n, d) to decrypt the ciphertext C. The decrypted message M is given by:

$$M = C^d \pmod{n} \quad (14)$$

Digital Signature (Optional):
To sign a message M, the sender computes the signature S using their private key (n, d):

$$S = M^d \pmod{n} \quad (15)$$

To verify the signature, the receiver computes:

$$M' = S^e \pmod{n} \quad (16)$$

If M' = M, the signature is valid.

- **Steganography:** Steganography is the science of hiding information in such a fashion that the presence of the information is not detectable by unintended recipients. Unlike encryption, where the goal is to make the data unreadable to unauthorized users, steganography aims to conceal the very existence of the message itself. Popular techniques include Least Significant Bit (LSB) insertion in images and waveform modification in audio files.

The most common types of steganography involve embedding hidden messages into:

1. **Images**: The most widely used form of steganography. The secret message is embedded in the pixels of the image, typically using the least significant bit (LSB) method, where small changes to pixel values are imperceptible to the human eye.

2. **Audio**: Involves hiding messages within sound files. Techniques may include altering the least significant bits of the audio data or using techniques like echo hiding or phase encoding.

3. **Text**: Text-based steganography embeds messages within text files using methods such as spacing variations, word choice, or manipulating character encoding.

4. **Video**: Hiding data within video files is a more advanced form of steganography, using both visual and audio components of the video.

The Least Significant Bit (LSB) method of steganography can be mathematically represented using the following formulae for embedding and extracting the secret message.

Let:

- $\mathbf{I = (I_1, I_2, \ldots, I_n)}$ represent the pixels of the original image.
- $\mathbf{M = (M_1, M_2, \ldots, M_k)}$ represent the bits of the secret message.
- $\mathbf{I' = (I'_1, I'_2, \ldots, I'_n)}$ represent the pixels of the modified image with the embedded secret message.

For each pixel $\mathbf{I_i}$, where $\mathbf{i = 1, 2, \ldots, n}$, we embed a bit $\mathbf{M_j}$ from the secret message into the least significant bit (LSB) of the pixel $\mathbf{I_i}$. The formula for embedding is:

$$\mathbf{I'_i = (I_i \text{ AND } 0xFE) \text{ OR } M_j}$$

Where:

- $\mathbf{I_i}$ is the original pixel value.

- **AND 0xFE** clears the least significant bit of the pixel $\mathbf{I_i}$.
- $\mathbf{M_j}$ is the secret message bit that will be inserted into the least significant bit of $\mathbf{I_i}$.

To extract the secret message from the image, we need to look at the least significant bit (LSB) of each pixel. The formula for extracting the hidden message bit from a pixel $\mathbf{I'_i}$ is:

$$\mathbf{M_j = I'_i \text{ AND } 1}$$

Where:

- $\mathbf{I'_i}$ is the pixel value from the image with the embedded message.
- **AND 1** extracts the least significant bit (LSB) of the pixel, which represents the bit of the secret message.

2.3 Considerations

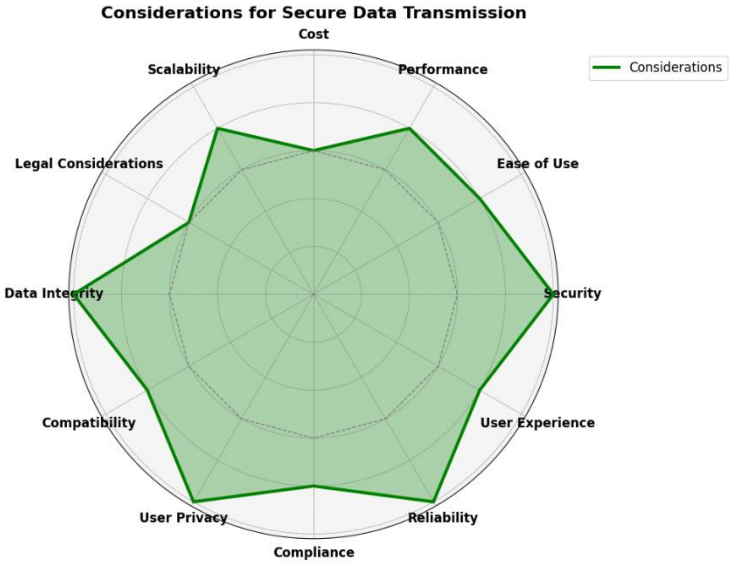

Figure 4 Considerations for Secure Data Transmission

The development of a secure data transmission system must address several key considerations to ensure effectiveness and user accessibility, such as:

- **Security:** Security ensures confidentiality, integrity, and authentication of transmitted data. Cryptographic methods like AES and RSA encrypt data, while steganographic techniques, like LSB encoding, conceal encrypted data in multimedia files, enhancing the system's resistance to unauthorized access.

- **Ease of Use:** A secure system must be user-friendly to promote widespread adoption. The system includes an intuitive graphical interface, allowing users to choose their preferred security module, ensuring ease of use for people with varying technical expertise.

- **Performance:** Performance is crucial, as encryption and steganography can introduce computational overhead. Optimized algorithms are employed to balance security and performance, ensuring secure transmission without significant delays or disruptions.

- **Cost:** Cost is an important factor, especially for large-scale deployments. Cryptographic techniques are efficient but can incur computational and infrastructure costs. The system is designed to be cost-effective, making secure data transmission accessible to a broad user base.

- **Scalability:** Scalability ensures that the system can handle growing data volumes and evolving security needs. The modular architecture allows easy integration with other systems, accommodating emerging technologies and expanding user bases without compromising security.

- **Legal Considerations:** Legal frameworks are essential for the protection of encrypted and hidden data. This study evaluates cybersecurity laws in India and globally, identifying gaps and providing recommendations for improving legal protections related to encryption, privacy, and steganography.

3 Proposed Architecture

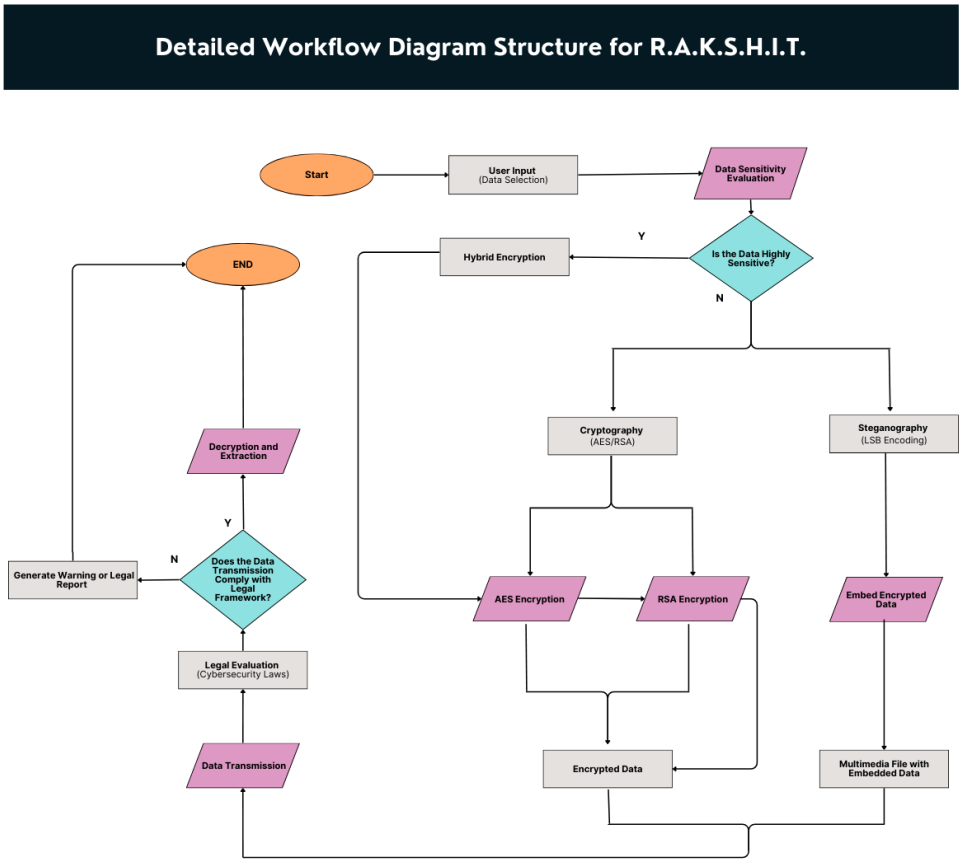

Figure 5 Workflow Diagram structure for R.A.K.S.H.I.T.

The proposed architecture for R.A.K.S.H.I.T. is designed to be modular in its approach, thereby catering to users' needs by allowing them to select different security modules based on their needs. The architecture includes the following components:

- **User Input (Data Selection):** The user is authorized to select their preferred mode for secure data transmission. A simple and intuitive UI allows users to easily choose their desired security method.

- **Data Sensitivity Evaluation:** After the data selection, the system assesses the sensitivity of the data. If the data is considered **highly sensitive**, the system opts for **hybrid encryption** using both cryptographic and steganographic methods for enhanced security. If the data is not highly sensitive, it moves on to simpler encryption methods.

- **Hybrid Encryption:** In the case of highly sensitive data, the system combines cryptography (AES or RSA) and steganography (LSB encoding) to provide dual layers of security. This ensures that the data is both encrypted and hidden within a multimedia file, making it harder for unauthorized entities to detect and decrypt.

- **Cryptography (AES/RSA):**

  - **AES Encryption:** If AES encryption is chosen, the data is securely encrypted using the AES algorithm, which is known for its efficiency and robustness.

  - **RSA Encryption:** Alternatively, if RSA encryption is selected, the system encrypts the data with RSA, providing strong public-key cryptography.

- **Steganography (LSB Encoding):** For highly sensitive data, the system embeds the encrypted data into a multimedia file using **LSB encoding**. This ensures that the encrypted data is concealed within an image or audio file, further protecting it from detection.

- **Legal Evaluation (Cybersecurity Laws):** The system evaluates whether the data transmission complies with existing cybersecurity laws and regulations. If the data transmission fails to meet the legal standards, a warning or legal report is generated. This step ensures that the data transfer adheres to legal frameworks such as those governing data privacy and encryption.

- **Decryption and Extraction:** If the user needs to retrieve the transmitted data, the system allows for decryption and extraction. This process ensures that only authorized parties can access the original data. If the data is encrypted using hybrid methods, both cryptographic and steganographic techniques are applied to extract and decrypt the data.

- **Data Transmission:** Once the data is securely encrypted and checked for legal compliance, the system transmits the data. The transmission is securely encrypted, ensuring that unauthorized access is prevented throughout the transmission process.

This architecture ensures that data is transmitted securely and in compliance with cybersecurity laws, while offering flexibility in the choice of encryption methods based on data sensitivity. The integration of both cryptographic and steganographic techniques provides an additional layer of security, mitigating the risks associated with unauthorized access or detection during transmission.

4 Implementation

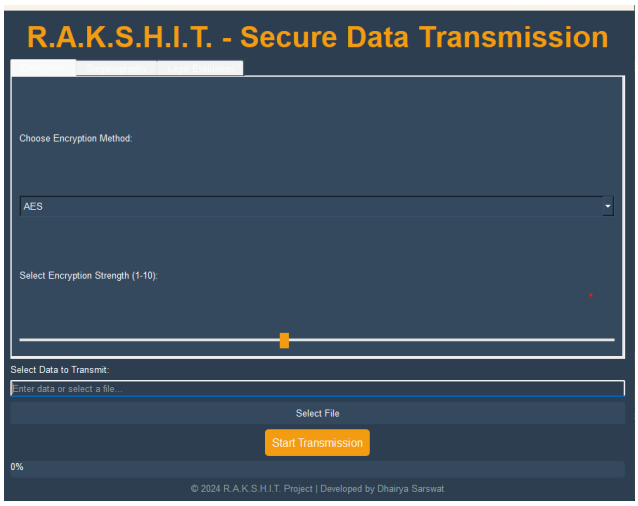

Figure 6 Encryption interface

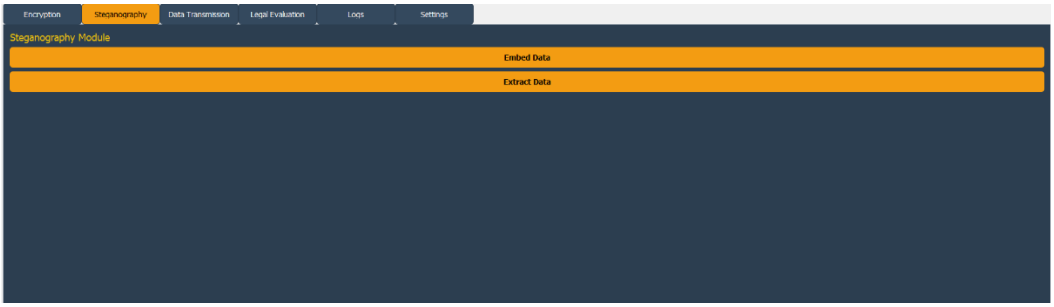

Figure 7 Core Functional Modules

Figure 8 Steganography in action

The implementation of R.A.K.S.H.I.T. involves using Python as the primary programming language, leveraging libraries such as PyCryptodome for cryptographic functions, OpenCV for image processing, and various steganography libraries for embedding data. It also utilises Python's PyQt library to create a user-friendly graphical interface, enabling seamless interaction between the user and the system. The interface allows users to select data for transmission, choose between different encryption methods, and initiate the process of embedding and transmitting the data. Additionally, the system is designed to be modular, ensuring that new encryption algorithms or steganographic techniques can be integrated into the system without disrupting the existing functionality.

5 Conclusions

R.A.K.S.H.I.T. offers a comprehensive solution for secure data transmission, combining cryptographic and steganographic techniques into a user-friendly application. By providing users with selectable modules, the application caters to varying levels of security needs without requiring extensive technical knowledge. Future work will focus on enhancing the application's features and ensuring compliance with evolving legal frameworks surrounding data protection. Furthermore, the application could find its use cases in secure communication, intellectual property protection, digital forensics, and confidential data exchange across industries like healthcare, finance, and law enforcement. By integrating advanced security measures, R.A.K.S.H.I.T. aims to be a key player in the protection of sensitive data in an increasingly interconnected world.

References

[1] A. Mehmood, A. Shafique, M. Alawida and A. N. Khan, "Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques," in IEEE Access, vol. 12, pp. 27530-27555, 2024, doi: 10.1109/ACCESS.2024.3367232. keywords: {Cryptography;Encryption;Computer security;Surveys;Security;Real-time systems;Neural networks;Machine learning;Quantum computing;Cybersecurity;machine learning;deep learning;quantum cryptography;cryptographic techniques},

[2] Tsantikidou, K.; Sklavos, N. Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures. Cryptography 2024, 8, 7. https://doi.org/10.3390/cryptography8010007

[3] J. Oliva del Moral, A. deMarti iOlius, G. Vidal, P. M. Crespo and J. Etxezarreta Martinez, "Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective," in IEEE Internet of Things Journal, vol. 11, no. 18, pp. 30217-30244, 15 Sept.15, 2024, doi: 10.1109/JIOT.2024.3410702. keywords: {Protocols;Cryptography;Quantum computing;Computers;Computer crime;Internet of Things;Computer security;Communication system security;cryptographic protocols;hardware security;industrial communication;internet of things;quantum cryptography},

[4] U. Mmaduekwe and E. Mmaduekwe, "Cybersecurity and Cryptography: The New Era of Quantum Computing," Current Journal of Applied Science and Technology, vol. 43, no. 5, pp. 41-51, 2024, doi: 10.9734/cjast/2024/v43i54377.

[5] M. Azeez, U. O. Ugiagbe, I. Albert-Sogules, S. Olawore, V. Hammed, E. Odeyemi, and F. S. Obielu, "Quantum AI for cybersecurity in financial supply chains: Enhancing cryptography using random security generators," World Journal of Advanced Research and Reviews, vol. 23, no. 1, pp. 2443-2451, 2024, doi: 10.30574/wjarr.2024.23.1.2242.

[6] Alonso F, Samaniego B, Farias G, Dormido-Canto S. Analysis of Cryptographic Algorithms to Improve Cybersecurity in the Industrial Electrical Sector. Applied Sciences. 2024; 14(7):2964. https://doi.org/10.3390/app14072964

[7] Khan AA, Por LY. Special Issue on Information Security and Cryptography: The Role of Advanced Digital Technology. Applied Sciences. 2024; 14(5):2045. https://doi.org/10.3390/app14052045

[8] N. Tatipatri and S. L. Arun, "A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security," in IEEE Access, vol. 12, pp. 18147-18167, 2024, doi: 10.1109/ACCESS.2024.3361039. keywords: {Cyberattack;Smart grids;Security;Power systems;Internet of Things;Transmission line measurements;Monitoring;Computer security;Cyber attacks;cyber security;cryptography;Internet of Things;power systems;smart grid},

[9] S. Singh and D. Kumar, "Enhancing Cyber Security Using Quantum Computing and Artificial Intelligence: A Review," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 4, no. 3, pp. 1-10, Jun. 2024, doi: 10.48175/IJARSCT-189024.

[10] Pleshakova, E., Osipov, A., Gataullin, S. et al. Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends. J Comput Virol Hack Tech 20, 429–440 (2024). https://doi.org/10.1007/s11416-024-00529-x

[11] Y.-K. Liu and D. Moody, "Post-quantum cryptography and the quantum future of cybersecurity," Phys. Rev. Applied, vol. 21, no. 4, p. 040501, Apr. 2024, doi: 10.1103/PhysRevApplied.21.040501.

[12] O. A. Ajala, C. A. Arinze, O. C. Ofodile, C. C. Okoye, and A. I. Daraojimba, "Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods," Magna Scientia Advanced Research and Reviews, vol. 10, no. 1, pp. 321-329, 2024, doi: 10.30574/msarr.2024.10.1.0038.

[13] K. Omote, Y. Inoue, Y. Terada, N. Shichijo and T. Shirai, "A Scientometrics Analysis of Cybersecurity Using e-CSTI," in IEEE Access, vol. 12, pp. 40350-40367, 2024, doi: 10.1109/ACCESS.2024.3375910. keywords: {Computer security;Market research;Bibliometrics;Security;Productivity;Blockchains;Technological innovation;Scientific publishing;Data analysis;Cybersecurity;scientometrics;research cluster;literature map;e-CSTI},

[14] Cybersecurity Enhancement through Hybrid Encryption: Combining RSA and Vigenère Algorithms in the Cypher-X System. Baghdad Sci.J [Internet]. 2024 May 25 [cited 2024 Dec. 13];21(5(SI):1765. Available from: https://bsj.uobaghdad.edu.iq/index.php/BSJ/article/view/10539

[15] R. A. Jowarder and S. Jahan, "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection," World Journal of Advanced Engineering Technology and Sciences, vol. 13, no. 1, pp. 330-339, 2024, doi: 10.30574/wjaets.2024.13.1.0421.

[16] B. Ramos-Cruz, J. Andreu-Perez, and L. Martínez, "The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research," Neurocomputing, vol. 2024, p. 127427, 2024, doi: 10.1016/j.neucom.2024.127427.

[17] Fortifying the Digital Frontier: Strategies, Challenges, and Innovations in Cybersecurity (N. V. Janapareddy \& D. P. Whig , Trans.). (2024). International Journal of Creative Research In Computer Technology and Design, 6(6), 1-32. https://jrctd.in/index.php/IJRCTD/article/view/59

[18] Ammi Blackwood, Jonathan Carrington, Stefan Baryshevsky et al. The Implementation of a Hybrid Large Language Model for Adaptive Cryptographic Cyber Defense, 22 September 2024, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-5120507/v1]

[19] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra and M. Liyanage, "Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography," 2024 15th International Conference on Network of the Future (NoF), Castelldefels, Spain, 2024, pp. 195-203, doi:

10.1109/NoF62948.2024.10741441. keywords: {Technological innovation;Quantum computing;Software algorithms;Public key;NIST;Software;Hardware;Cryptography;Protection;Standards;Post-Quantum Cryptography;Cybersecurity;Quantum Threats},

[20] O. A. Ajala, C. C. Okoye, O. C. Ofodile, C. A. Arinze, and O. D. Daraojimba, "Review of AI and machine learning applications to predict and thwart cyber-attacks in real-time," Magna Scientia Advanced Research and Reviews, vol. 10, no. 1, pp. 312-320, 2024, doi: 10.30574/msarr.2024.10.1.0037.

[21] Normurodov , A. ., & Rustamov , A. . (2024). POSSIBILITIES OF QUANTUM CRYPTOGRAPHY IN PROVIDING CYBER SECURITY IN NETWORKS. Academic Research in Modern Science , 3 (12), 105–109. retrieved from https://www.econferences.ru/index.php/arims/article/view/14392

[22] Redhu, R., Narwal, E., Gupta, S. et al. Software implementation of systematic polar encoding based PKC-SPE cryptosystem for quantum cybersecurity. Sci Rep 14, 9994 (2024). https://doi.org/10.1038/s41598-024-60767-3

[23] N. Tihanyi, M. A. Ferrag, R. Jain, and M. Debbah, "CyberMetric: A benchmark dataset for evaluating large language models knowledge in cybersecurity," 2024. [Online].

[24] Enhancing Cybersecurity in Electronic Communication Systems: New Approaches and Technologies. (2024). Progress in Electronics and Communication Engineering, 1(1), 38-43. https://doi.org/10.31838/ECE/01.01.07

[25] Michael Lodi, Maria Cristina Carrisi, and Simone Martini. 2024. Big Ideas of Cryptography in Primary School. In Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1 (ITiCSE 2024). Association for Computing Machinery, New York, NY, USA, 206–212. https://doi.org/10.1145/3649217.3653548

[26] Archibong, E. E., Stephen, B. U.-A., \& Asuquo, P. (2024). Analysis of Cybersecurity Vulnerabilities in Mobile Payment Applications. Archives of Advanced Engineering Science, 1-12. https://doi.org/10.47852/bonviewAAES42022595

[27] Ferraro, G., Maunero, N., Montegiove, S., Prinetto, P. (2025). The Big Game: The Italian Avenue of Attack to Cybersecurity Skill Shortage. In: Hinchey, M., Steffen, B. (eds) The Combined Power of Research, Education, and Dissemination. Lecture Notes in Computer Science, vol 15240. Springer, Cham.

[28] Kumar, A., Saini, R., Kumar, R. (2024). A comparative analysis of machine learning algorithms for breast cancer detection and identification of key predictive features. Traitement du Signal, Vol. 41, No. 1, pp. 127-140. https://doi.org/10.18280/ts.410110

[29] Kumar, A., Saini, R., and Kumar, R., "A Systematic Review of Breast Cancer Detection Using Machine Learning and Deep Learning," 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gautam Buddha Nagar, India, 2023, pp. 1128-1133, doi: 10.1109/UPCON59197.2023.10434530

[30] Mahammad, A. B., and Kumar, R., "Scalable and Security Framework to Secure and Maintain Healthcare Data using Blockchain Technology," 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), Greater Noida, India, 2023, pp. 417-423, doi: 10.1109/CISES58720.2023.10183494

[31] Gosain, M. S., Aggarwal, N., and Kumar, R., "A Study of 5G and Edge Computing Integration with IoT- A Review," 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), Greater Noida, India, 2023, pp. 705-710, doi: 10.1109/CISES58720.2023.10183438

[32] Jaiswal, A., and Kumar, R., Breast cancer diagnosis using Stochastic Self-Organizing Map and Enlarge C4.5. Multimed Tools Appl (2022). https://doi.org/10.1007/s11042-022-14265-1

[33] Mahammad, A. B., and Kumar, R., "Design a Linear Classification model with Support Vector Machine Algorithm on Autoimmune Disease data," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), 2022, pp. 164-169, doi: 10.1109/ICIEM54221.2022.9853182

[34] Singh, C. B., Gupta, A., and Kumar, D. R., "Diabetes Care Survey Using Supervised and Unsupervised Machine Learning," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), 2022, pp. 207-210, doi: 10.1109/ICIEM54221.2022.9853085

[35] Kumar, R., Hamid, A., Bakar, A., Inayah Binti Ya'akub, N., Sharma Gaur, M., & Kumar, S. (Eds.). (2024). Futuristic E-governance Security with Deep Learning Applications. IGI Global

[36] Kumar, A., Saini, R., & Kumar, R. (2024). A Comparative Analysis of Machine Learning Algorithms for Breast Cancer Detection and Identification of Key Predictive Features. Traitement du Signal, 41(1)

[37] Kumar, P., Kumar, M., & Kumar, R. (2024). The Proposed Framework of View-Dependent Data Integration Architecture. In The Ethical Frontier of AI and Data Analysis (pp. 343-361). IGI Global

[38] Gaur, A. S., Sharan, H. O., & Kumar, R. (2024). AI in Education: Ethical Challenges and Opportunities. The Ethical Frontier of AI and Data Analysis, 39-54

[39] Kumar, P., Kumar, R., Singh, K. B., & Kumar, M. (2023). Identification of the Problem and Research Methodology. In Effective AI, Blockchain, and E-Governance Applications for Knowledge Discovery and Management (pp. 289-308). IGI Global

[40] Mahammad, A. B., & Kumar, R. (2022). Progression of Digital Healthcare With Deep Learning and Blockchain Methods for Smart Cities. In Advances in Deep Learning Applications for Smart Cities (pp. 248-266). IGI Global

[41] Bansal, P., Kumar, R., Mishra, B. K., & Somwanshi, D. (2022). IoT-Based Security System Using ESP-32 and Lasers and Its Various Applications

[42] IBM Security, "Cost of a Data Breach Report 2024," IBM, 2024. Available: https://www.ibm.com/reports/data-breach. Accessed: Dec. 13, 2024

7 Author

Dhairya Sarswat is a B.Tech student in Computer Science and Engineering at the Moradabad Institute of Technology, affiliated with AKTU University, India. He has authored several research papers and book chapters and has also presented his work at several international conferences. His research interests encompass artificial intelligence, robotics, computer vision and cybersecurity. He has also mentored several students and conducted workshops on emerging technologies, showcasing his dedication to fostering knowledge and innovation in the field of computer science and engineering.

Utkarsh Saxena

Born on June 26, 2004, in Moradabad, Utkarsh Saxena is a B.Tech (CSE) student at MIT, Moradabad. An academic scholar and achiever, he has won awards like Best Research Paper and Code-A-Thon 2k24. Passionate about listening to music and acting, Utkarsh is self-loving, empathetic, and always ready to help others. With a strong foundation in technology, he aims to innovate and contribute to advancements in artificial intelligence and software development.

Kanchan Rani is an Assistant Professor in the Department of Computer Science & Engineering, Moradabad Institute of Technology, and Moradabad. She completed her MTech degree in Computer Science from Banasthali Vidyapith Jaipur in 2011. She pursued her BTech degree from AKTU Lucknow. She her published more than 18 research papers in various international journals and conferences. She has more than 17 years teaching experience. Her research interests include Artificial Intelligence, Machine Learning, software engineering and soft computing techniques.

Shiwani Agarwal is an Assistant Professor in the Department of Computer Science & Engineering, Moradabad Institute of Technology, and Moradabad. She completed her M.Tech degree in Computer Science from National Institute of Technical Teachers Training & Research in 2022. She pursued her B.Tech degree from AKTU Lucknow. She has published more than 10 research papers in various international journals and conferences. She has more than 10 years teaching experience. Her research interests include Machine Learning, Cyber Security and soft computing techniques

Prachi Agarwal is an Assistant Professor in the Department of Computer Science & Engineering, Moradabad Institute of Technology, Moradabad. She completed her MTech degree in Computer Science from IFTM University in 2013. She pursued her BTech degree from GBTU Lucknow. She has published more than 19 research papers in various international journals and conferences. She has more than 11 years teaching experience. Her research interests include Machine Learning, web development and image processing.