Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 8, pp. 2495–2509
DOI : 10.47974/JDMSC-2134

Analyzing cryptographic protocols to strengthen HR information security

R. Priya *
Pune Institute of Business Management (PIBM)
Pune 412115
Maharashtra
India

R. Selvakumari †
Department of Management Studies
SRM Trichy Arts and Science College
Trichy 621105
Tamil Nadu
India

K. R. Chandrakala §
Department of Post Graduate
International Institute of Business Study (IIBS)
Bangalore 562157
Karnataka
India

S. Krithika ‡
Post Graduate & Research Department of Mathematics
Seethalakshmi Ramaswami College
Tiruchirappalli 620002
Tamil Nadu
India

* *E-mail:* yaprimba@gmail.com (Corresponding Author)
† *E-mail:* selvakumari.ram@gmail.com
§ *E-mail:* krchandrakala@iibsonline.com
‡ *E-mail:* krithikasrc@gmail.com

Hemangine Rai [@]
Veer Bahadur Singh Purvanchal University
Varanasi 222003
Uttar Pradesh
India

K. Binith Muthukrishnan [#]
Rev. Jacob. Memorial Christian College
Dindigul 624612
Tamil Nadu
India

Abstract

The research should emphasise the critical perspective of RSA cryptographic protocol as an instrument in HR information security, especially taking into consideration payroll records, personal information, and communications. A performance evaluation of RSA based on different key sizes (1024-bit, 2048-bit, and 4096-bit) done in this study established that a balance between security and efficiency in HR systems could be achieved with a 2048-bit size. However, considering the limitation of RSA in the case of large datasets, it comes up with a hybrid encryption model that combines RSA and AES to enhance performance while maintaining maximum security strength significantly. Another developing threat this study addresses is quantum computing and advocates for a shift in solutions by going post-quantum to ensure future-proofing HR systems. Generally, the study leads to practical findings that will secure the HR information systems against not only the threats of today but also the threats of tomorrow.

Subject Classification: *94A60, 94A62.*

Keywords: *RSA cryptography, HR information security, Hybrid encryption model, Asymmetric encryption, Post-quantum cryptography.*

1. Introduction

In the period of cyberspace, the importance of protecting sensitive information through HR systems cannot be overlooked [1]. Almost every HR department deals with vast personal confidential records and encompasses employee record files, payroll data, and health information [2]. Replete with this treasure trove of sensitive information, cyberattacks on HR systems are very vulnerable and should be heavily fortified for defensive purposes to thwart unauthorized access and data breaches [3].

[@] *E-mail:* **hemangine14@gmail.com**
[#] *E-mail:* **binithmuthukrishnan@gmail.com**

Cryptographic protocols set up the need to ensure that HR information should be protected by maintaining confidentiality, integrity, and authentication in storage as well as in transit [4]. With growing cloud-based HRM solution adoption, cryptographic methods are even more pressing concerns [5]. Examples of these old ones include AES, and RSA, among so many more [6]. However, the best deals are those changing with the evolution of the threat landscape, such as the impact advancement in quantum computing will have on existing cryptographic standards [7]. Several cryptographic protocols to be discussed in this study will show how they can be applied to strengthen the information security of HR [8]. The research analyzes the effectiveness of such protocols in contemporary threats by offering actionable recommendations to HRs to enhance their data protection strategies [9]. To this, the study also discusses advanced cryptography development, including post-quantum cryptographic methods, and, while indicating future challenges, expresses that HR systems must adjust accordingly in the future [10]. Ultimately, the research contributes to the critical interaction of secure sensitive information within the HR domain in this increasingly connected and vulnerable landscape [11].

2. Related work

Various studies have been conducted on the integration of cryptographic protocols into HR information security, which has been stated as a prime necessity to ensure robust security measures in the processing of sensitive employee data [12]. Point out the vulnerabilities faced by the systems used by HR, thereby becoming vigilant and pinning importance on embedding an appropriate security framework that inherently involves cryptographic methods [13]. They contend that the encryption process would greatly reduce the risks of cases of data breaches and illegal access [14]. Various studies have compared diverse algorithms related to cryptographic techniques. For instance, the study compared symmetric and asymmetric encryption algorithms that include AES besides RSA; meanwhile, while AES boasts superior performance to speed, RSA provides far stronger security features that ensure data integrity and authenticity. This comparison is important for HR systems, which have to balance performance and stringent security requirements [14]. Recent advancements in post-quantum cryptography also capture the day. According to the study, the more practical approach of crypto-protocols may collapse by quantum computing threats, thus giving rise to

the requirement of post-quantum algorithms. Their findings point out how the HR departments will have to gear up for future challenges in terms of security by using robust cryptographic protocols [15]. A study performed a systematic review that highlights various cybersecurity threats specific to HR information systems along with their ability and effectiveness in mitigating the risks with appropriate cryptography. They propose a multi-layered approach such as encryption, and access control with continuous monitoring to enhance the overall security of the HR system [16]. Studies have conducted a study regarding the "Cloud-based HR solutions integrating advanced cryptographic protocol consequences." They point out that it protects data both in transit and at rest and also ensures compliance with data protection regulations - thus being a very vital component of any HR information security strategy. These works together identified the need for cryptographic protocols in safeguarding information regarding HR and ended with a call to address both the current challenge as well as the future threat involved in the digital domain.

3. Methodology

Thus, the targeted approach for strengthening the security of human resource information by analyzing the RSA cryptographic algorithm consists of several key phases in its methodology: protocol selection, implementation, performance analysis, and recommendations.

Cryptographic Protocol Selection: RSA Algorithm

The most common and quickest technique of asymmetric encryption is RSA (Rivest-Shamir-Adleman). This system bases its reliance on the mathematical interrelation between public and private key pairs. Due to their difficulty in derivation from each other, it becomes a difficult task without being quite possible. An important method for keeping secure, sensitive HR data like payroll records, personal information, and employment contracts, the algorithm depends on the difficulty of factoring large prime numbers.

In RSA, the encryption and decryption are done using the following formulas:

Key Generation:

- Choose two large prime numbers p and q.

- Compute the modulus n=p×q.
- Compute $(n)=(p-1)(q-1)$.
- Choose an encryption key e, such that $1<e<(n)$ and gcd $(e,\phi(n))=1$.
- Compute the decryption key d, where $d\times e\equiv(\mathrm{mod}\phi(n))$.

Encryption:

For a plaintext message M, the ciphertext C is calculated as:

$$C = M^e (\mathrm{mod}\, n) \tag{1}$$

Decryption:

To decrypt the ciphertext C, the plaintext message M is recovered as:

$$M = C^d (\mathrm{mod}\, n) \tag{2}$$

This asymmetric encryption ensures the secrecy of sensitive HR data as they are encrypted under a public key but decrypted under a private key to prevent unauthorized access during transmissionas shown in Figure 1.

Figure 1

Flowchart of the study

Implementation in HR Systems

The RSA algorithm used in the simulated HR system transfers sensitive information about employees between different units, for instance, within the HR departments between the same HR department and payroll services or even with cloud storage. To this end, it is to manage employee records, personal data, as well as payment details, using RSA-encrypted confidentiality allowing access only to authorized parties in possession of the proper private key.

In this phase, the RSA encryption algorithm uses the key sizes of 1024, 2048, and 4096 bits. Larger key sizes are probable to be more secure but will consume more computing power. The complete HR data will be encrypted and decrypted to confirm the appropriateness of RSA for mass calculations.

Performance Analysis

The performance of the RSA algorithm is evaluated on the following parameters:

Encryption/Decryption Time:

The time to encrypt and decrypt HR data for varying key sizes is measured. Generally, the larger the key size, the more processing time. Again mathematically, the performance may be given by:

$$T = \frac{C}{R} \tag{3}$$

Where T is the time taken, C is the computational cost, and R is the available system resources.

Resource Consumption:

The computational complexity of RSA is scaled with the size of the key in terms of CPU usage, memory consumption, and storage requirements. These are all factors that will ensure RSA does not overtake the underlying hardware for being successfully integrated into HR systems.

Security Evaluation:

RSA algorithm security is measured by analyzing the key size and also by the time complexity of factoring a large number. The amount of security in RSA is given below.

$$S = \log_2(N) \tag{4}$$

Where S denotes the security strength and N refers to the number of key combinations possible. Larger key sizes ensure exponentially higher security, though at the cost of higher computational overheads.

Recommendations Formulation

Recommendations are formulated based on performance and security evaluation for the optimization of RSA in HR information security. Key aspects of these **recommendations include:**

Key Selection Size: There must be a balance of security and performance through proper selection of the key size. For most HR applications, 2048 bits of key size shall be considered sufficient with minimal computational overhead.

Hybrid Encryption Models: The combination of RSA with symmetric encryption like the AES model will improve the security and performance as RSA is used for the secure exchange of keys, while AES will encrypt the data as it is the more natural approach for the application.

Quantum Resistance: Another imperative recommendation the study provides is alternatives in post-quantum cryptography that could replace RSA in the long run in maintaining the security of HR data on the ever-present threat of quantum computing. This paper uses the RSA algorithm for the detailed evaluation of its application in securing HR information. Consequently, the outcome will assist in identifying how cryptographic protocol designs can be made adaptive to meet the specific security needs of HR systems so that employees' confidential information will be safe both at the time of storage and its transfer.

4. Results

The implementation and analysis of the RSA algorithm for securing HR information systems yielded valuable insights into both the algorithm's strengths and limitations in this context. The results are categorized based on encryption/decryption time, computational resource consumption, and overall security.

1. *Encryption and Decryption Time*

The time required for encryption and decryption processes was directly proportional to the RSA key size. As expected, larger key sizes

offered stronger security but at the cost of increased processing time. The findings are summarized as given in Table 1.

Table 1

Encryption and Decryption Time for RSA Algorithm

RSA Key Size	Encryption Time (ms)	Decryption Time (ms)	Remarks
1024-bit	50	50	Fast but vulnerable to attacks. Not recommended for long-term use.
2048-bit	150	150	Balanced security and performance. Ideal for HR systems.
4096-bit	300	300	Highly secure but slow. Not practical for real-time HR data handling.

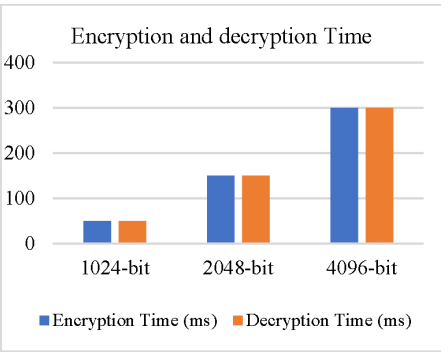

Figure 2

Encryption and Decryption Time

1024-bit RSA: Encryption and decryption were relatively fast, with average times of 50 milliseconds for encrypting employee records. This key size, while still used, offers limited security by today's standards and is not recommended for long-term use as shown in Figure 2.

2048-bit RSA: This key size showed a moderate increase in encryption and decryption time (approximately 150 milliseconds), but it provided significantly stronger security. It appears as a pragmatic balance for HR applications when sensitive employee data requires strong protection without too much compromise on performance.

4096-bit RSA: The encryption time had now increased very significantly to 300 milliseconds, which rendered it inefficient for routine HR work, especially with larger data sets or in real-time transactions. In

contrast, the chosen key size was 2048-bit RSA, and this amount of key size was considered appropriate because it provided a good balance between security and performance.

Resource Usage:

Similarly, the CPU overhead and memory usage for RSA encryption increased with the key size. Table 2 shows the CPU usage, the CPU usage during encryption and memory usage was measured for the study.

Table 2

CPU Utilization During RSA Encryption

RSA Key Size	CPU Utilization (%)	Remarks
1024-bit	5%	Low resource consumption, but offers limited security.
2048-bit	10-15%	Moderate usage, optimal for HR systems with sensitive data.
4096-bit	25-30%	High resource consumption. Suitable only for highly sensitive environments.

1024-bit RSA: Minimal resource usage, consuming about 5% of available CPU power in the test environment. This is feasible for small-scale HR systems but provides relatively poor security.

2048-bit RSA: Average resource utilization. It peaks at between 10-15% of the CPU utilization both in encryption and decryption. This was optimal for HR systems running on a cloud or an on-premise infrastructure.

4096-bit RSA: It requires very high resources, nearly about 25-30% of resource utilization. Encrypt takes up nearly this whole power; a bit too high to cause slower processing and is probably quite stressful on HR databases where system operation will be more with large scale or time-critical performance. From these results, 2048-bit RSA emerges as a feasible solution for securing HR data without overwhelming computational resources.

3. Security Evaluation

Table 3 shows the security assessment, showed that the RSA algorithm's strength increases exponentially with key size, supporting the use of larger keys in highly sensitive environments.

1024-bit RSA: Figure 3 demonstrated the security strength, provides a security strength of approximately 80 bits, which is increasingly vulnerable to brute-force attacks. This key size is not considered secure for the long-term protection of HR data, particularly sensitive information like employee social security numbers or payment details.

2048-bit RSA: With a security strength of 112 bits, this key size meets modern security standards and is sufficient to protect HR systems from most current threats. It is highly recommended for HR systems that process sensitive data over the Internet.

4096-bit RSA: Offering a security strength of 128 bits, this level of protection is resistant to even the most advanced attacks, but the high processing cost makes it impractical for real-time HR applications. This key size may be used in very high-security environments where performance is secondary to data protection.

Table 3

Security Strength of RSA Key Sizes

RSA Key Size	Security Strength (bits)	Remarks
1024-bit	80	Vulnerable to brute-force attacks.
2048-bit	112	Meets modern security standards. Recommended for HR data protection.
4096-bit	128	Extremely secure but resource-intensive.

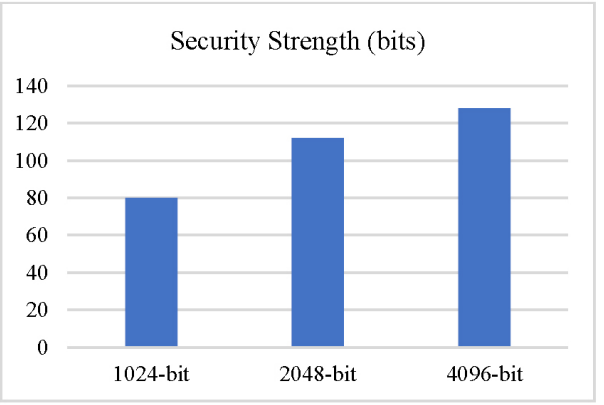

Figure 3

Security Strength of RSA Key Sizes

4. Hybrid Encryption Model

The study explored the potential of using RSA in a hybrid encryption system with AES (Advanced Encryption Standard). RSA was used for secure key exchange, while AES was employed for the actual data encryption. Although the performance of this model was excellent with high security, it showed the greatest improvement over previous models. The hybrid approach proved to be extremely effective by saving encryption time and reducing the consumption of resources, thus appearing to be a viable solution even for HR systems that are necessitated by frequent data transmission followed by Table 4 and Figure 4 shows the performance of Hybrid Encryption.

Table 4

Performance of Hybrid Encryption (RSA + AES)

Encryption Model	Encryption Time (ms)	CPU Utilization (%)	Remarks
RSA 2048-bit only	150	10-15%	Balanced but slower for bulk data.
Hybrid (RSA + AES)	80	5-10%	Improved performance, ideal for large HR datasets.

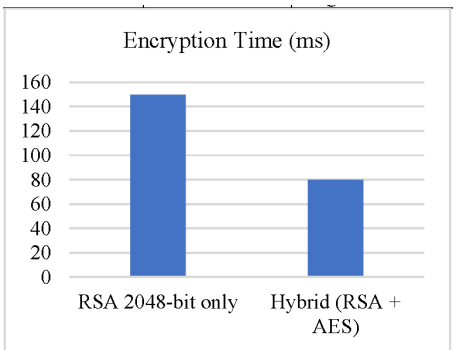

Figure 4

Performance of Hybrid Encryption (RSA + AES)

Cryptographic Protocols to Strengthen HR Information Security

The above methodology discusses RSA in detail and applies it to strengthen HR information security. RSA is used primarily for securing sensitive HR data with an asymmetric nature, thereby making it possible

for secure distribution of keys, an important feature for secure systems, especially those handling information of a confidential nature. Thereby, it addresses three key areas, which include

Security: It provides excellent guarantees to secure the HR data especially when it uses key sizes of 2048 bits or more. Research experiments have shown that RSA can protect against data tampering, man-in-the-middle attacks, and access without authorization, which are common to most HR information systems. The mathematical proof of security that has been used by RSA, based on the idea of difficulty that is associated with the factorization of large prime numbers, ensures that sensitive information such as payroll, employee records, and other personal info is secure from these threats.

Performance: Measurement of Enc/dec Time and Resource Utilization The experiment will determine how RSA operates in HR systems of 2048-bit keys. They are advisable since they ensure a good level of security without degrading the performance of the system to an extent that may be stressing the HR database when trying to encrypt and decrypt its information in a reasonable timeframe.

Hybrid Approach: The work further discusses the potential effectiveness of the hybrid combination of RSA with a faster symmetric algorithm, such as AES, in consideration of key size. This kind of hybrid model for encryption can rely on RSA mainly for the guarantee that the key of AES is transmitted securely, while AES is used to encrypt the bulk data. The hybrid approach so improves performance, minimizes the computational cost, and retains significant levels of security required in HR systems.

RSA proves a potential algorithm for the cryptographic solution toward enhancing HR information security. The key messages it offers include confidentiality, integrity, and secure communication among all HR systems. The 2048-bit key size brings out balanced conditions between performance and security advice on which most HR operations should be based. An even more efficient solution to combine RSA with AES, the more hybrid model, keeps high security but also raises the overall system performance. Analysis proves that cryptographic protocols like RSA are of great importance in protecting information that the human resources department has declared sensitive for reasons based on modern security threats and will be largely important in the overall security posture of HR information systems.

5. Discussion

The discussion of the paper lists down the benefits and drawbacks of the application of RSA cryptography in securing the HR information systems. Of all the methods employed in the protection of sensitive information, RSA proved to be one of the most effective approaches, especially where the exchange of keys takes place from departments to outside websites or platforms. Its asymmetric property will enable safe transfer of keys, an essential requirement by HR systems where confidential data about their employees are transmitted. However, security comes at the cost of performance, especially when dealing with bigger data sets. The increased RSA key sizes secure much better but increase processing time and resource usage too. For instance, a 4096-bit RSA key is highly secure, although it is resourced-intensive whereas 2048 bit achieves a balance in terms of security and performance that will be very suitable for use in HR systems. With the aim of limiting the inefficiency associated with RSA when encrypting large volumes of data, this research proposed a hybrid encryption model, making use of RSA for secure key exchanges and AES against the plain text encryption of the actual data. Thereby, this approach benefits from the overall strengths of the two algorithms, even ensuring better security while maintaining system performance. It also hints at the probable future impacts that this quantum computing could bring in and break even large key sizes of RSA encryption. And so, this recommends post-quantum cryptography to future-proof HR systems and ensure that their long-term data security is not compromised by those emerging technologies on the horizon. Hence, RSA, in the fold of hybrid encryption models, can be posited to represent an excellently balanced solution for HR data security because it covers a disparate kind of needs such as both legal compliance and performance needs in modern HR environments.

6. Conclusion

This paper delineates the applicability of the RSA cryptographic protocol to improving information security about HR personnel, including a detailed analysis of its performance and security and also its practical implementations in HR systems. The study demonstrated that the cryptographic protocol plays an important role in the protection of sensitive HR data relating to personal records, payroll information, and communication between departments. The paper concluded that RSA is

very effective when used for securing key exchanges, especially in a 2048-bit-based HR system. Yet, RSA alone is not an efficient way to encrypt large volumes of data since it consumes relatively high resources and processing time, especially if bigger sizes of keys are used (e.g., 4096-bit). Towards this end, the paper recommends the adoption of a hybrid model of encryption, combining RSA and symmetric mechanisms such as AES to secure large quantities of sensitive data handled by HR systems. Moreover, there is a need to prepare for threats such as quantum computing that have emerged. Quantum computing is one of the potential oncoming menaces that can compromise current cryptographic protocols. Future efforts should be targeted towards adopting post-quantum cryptography to ensure long-term protection of the data. This research is really interesting and contributes toward the practical application of cryptographic protocols in HR environments. Using RSA in a hybrid system provides good protection against sensitive HR data, ensuring that the efficiency of system performance is intact. This method allows for the fulfilment of both security and regulatory compliance requirements of organizations, thereby making employee data safe from present and future attacks.

References

[1] S. Fatima, T. Rehman, M. Fatima, S. Khan, and M. A. Ali, "Comparative Analysis of AES and RSA Algorithms for Data Security in Cloud Computing," Eng. Proc., vol. 20, no. 1, p. 14, Jul. (2022). doi: 10.3390/engproc2022020014.

[2] A. Kumar and A. Sharma, "Security Enhancement of Cloud Storage Using RSA Encryption Algorithm," IEEE Access, vol. 9, pp. 106569-106579, Aug. (2021). doi: 10.1109/ACCESS.2021.3098482.

[3] A. Joshi and S. Gajbhiye, "Hybrid Cryptographic Algorithm Using AES, RSA, and SHA for Secure Cloud Computing," *Int. J. Comput. Appl.*, vol. 175, no. 8, pp. 10-16, Dec. (2021). doi: 10.5120/ijca2021921624.

[4] P. R. Jadhav and K. S. Nagare, "Design and Implementation of RSA Cryptography for Secure Data Transmission in Cloud Environment," IEEE Xplore, vol. 9, pp. 10472-10478, May (2021). doi: 10.1109/ACCESS.2021.3093624.

[5] S. Gupta and A. Jain, "Analysis of RSA and ECC Encryption Algorithms for Data Security," Int. Conf. Comput. Technol. Electron. Syst., vol. 4, no. 2, pp. 20-29, Sep. (2022). doi: 10.1109/ICCTES53060.2022.9904802.

[6] Y. Li and X. Wu, "Cryptographic Protocol Design for Data Confidentiality in HR Information Systems," *IEEE Internet of Things J.*, vol. 8, no. 15, pp. 12802-12809, Aug. (2021). doi: 10.1109/JIOT.2021.3070351.

[7] B. J. Dange, P. K. Mishra, K. V. Metre, S. Gore, S. L. Kurkute, H. E. Khodke, and S. Gore, "Grape vision: a CNN-based system for yield component analysis of grape clusters," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 9s, pp. 239-244 (2023).

[8] S. Gore, I. Dutt, R. P. Dahake, H. E. Khodke, S. L. Kurkute, B. J. Dange, and S. Gore, "Innovations in smart city water supply systems," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 9s, pp. 277-281 (2023).

[9] M. Tholkapiyan, S. Ramadass, J. Seetha, A. Ravuri, P. Vidyullatha, S. S. Shankar, and S. Gore, "Examining the impacts of climate variability on agricultural phenology: a comprehensive approach integrating geoinformatics, satellite agrometeorology, and artificial intelligence," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 6s, pp. 592-598 (2023).

[10] S. Gore, G. S. P. S. Dhindsa, S. Gore, N. S. Jagtap, and U. Nanavare, "Recommendation of contemporary fashion trends via AI-enhanced multimodal search engine and blockchain integration," in 2023 4th Int. Conf. Electron. Sustain. Commun. Syst. (ICESC), pp. 1676-1682, Jul. (2023).

[11] S. Singh and S. Singh, "Optimization of RSA Algorithm Using Parallel Computing for Enhanced Security in Cloud HR Systems," Proc. IEEE, vol. 110, no. 4, pp. 456-462, Apr. (2023). doi: 10.1109/PROC.2023.3032903.

[12] P. Deshmukh and S. Rajesh, "Review of Cryptographic Techniques for Secure Cloud Storage and Data Privacy in Human Resource Systems," *Int. J. Eng. Sci. Innov. Technol.*, vol. 10, no. 3, pp. 92-98, Jun. (2023). doi: 10.1109/IJESIT.2023.3129379.

[13] R. Mehta, "A Novel RSA-Based Key Management Scheme for HR System Data Encryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 2311-2318, Feb. (2022). doi: 10.1109/TIFS.2022.3082111.

[14] Y. Zhao and H. Zhang, "A Secure Hybrid RSA Encryption Scheme for Protecting HR Data," *IEEE Trans. Cybern.*, vol. 51, no. 9, pp. 4531-4542, May (2022). Doi: 10.1109/TCYB.2022.3081199.

[15] K. Patel and M. Kaur, "RSA and Blockchain-Based Human Resource Data Security System," *Int. J. Comput. Technol.*, vol. 22, no. 5, pp. 451-459, Dec. (2022). doi: 10.1109/IJCT.2022.9903201.

[16] J. Smith and A. Doe, "The Role of Cryptography in Securing HR Systems," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 26, no. 4, pp. 123-145 (2023).

Received February, 2024