2026 Volume: 02 Issue: 01 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-10

SECURE USER AUTHENTICATION-BASED HEALTHCARE ARCHITECTURE USING OPTIMIZED RSA ALGORITHM

[1]Dr. Ram Krishna Kumar, [2*]Dr. Piyush Raja, [3] Dr. Amit Kumar

[1]Co-Founder, RAM Literature and Research Foundation, Bihar, India.

[2]Professor, Department of Computer Science, Vishun Roy College, Bhagwanpur, Vaishali, Bihar, India

[3]Assistant Professor, Department of Computer Science, Gaya College, Gaya, Bihar, India.

Article Received: 23 November 2025
Article Revised: 13 December 2025
Published on: 02 January 2026

***Corresponding Author: Dr. Piyush Raja**
Professor, Department of Computer Science, Vishun Roy College, Bhagwanpur, Vaishali, Bihar, India.

DOI: https://doi-doi.org/101555/ijrpa.3730

ABSTRACT

The main purpose of the initiative is to set up a new, safe cloud-based system for medical data. The suggested structure changes cloud infrastructures to offer low costs, quick discovery, scalability, security, and the ability to adapt to changing workloads. It also makes me worry about the privacy and safety of patient info. A lot of study has been done on cloud data security, but there are still some problems that could leave data open to theft, changes, and unauthorized access. Using authentication and access control, this study shows a safe way to store healthcare data in cloud-based systems. So, only people who are allowed to can see the info, and it stays the same after being stored. This study suggests a three-step process that puts user ID verification, data privacy, and data accuracy at the top of the list. Putting these protections in place lets healthcare organizations use cloud storage while lowering risks like unauthorized access, data breaches, and abuse. Using the OPTIMI_RSA algorithm to confirm user identities is what this study on protecting cloud-based healthcare systems is all about. Only authorized users will be able to receive healthcare services, which protects the system and patient privacy.

KEYWORDS: Health Care System, Cloud Storage,Data Integrity, Data Encryption, Access control.

INTRODUCTION

The internet effortlessly connects individuals worldwide and constitutes the foundation of the global information communication infrastructure. Throughout the years, technical innovations have significantly transformed the methods of information access and communication. This ongoing transformation is fundamentally modifying the manner in which information is distributed. The advancement of novel tools and technologies is crucial for enabling the seamless flow of knowledge globally across national boundaries. Cloud computing is a significant and intricate advancement, fundamentally transforming data management and utilization. Since its inception, cloud computing has evolved swiftly and continuously to meet the increasing demands of our interconnected digital society.

Due to the fast development of technology, healthcare organizations are utilizing cloud solutions to safeguard patient data and medical information. Due to the critical nature of safeguarding patient records and diagnostic data, more and more healthcare providers are moving their operations to the cloud. In addition to improving security and conforming to healthcare data rules, this improvement makes it easier for authorized experts to communicate and collaborate. A versatile system that emphasizes the protection of patient data while enabling data sharing among medical workers is the outcome of integrating cloud technology into the healthcare system, according to Ermakova et al. (2020). This move away from antiquated practices has led to the processing, storage, and accessibility of sensitive health data in cloud environments. Healthcare providers can better manage sensitive data with the help of cloud technologies, which are versatile and flexible.

Innovation in healthcare is being propelled by cloud technology, which guarantees the security and accessibility of sensitive data during important medical decisions. The use of cloud computing in healthcare has the potential to improve data administration, encourage research collaboration, and, via the secure management of patient data, raise the quality of patient treatment.

The purpose of this research is to analyze healthcare system user ID authentication in the cloud using encryption methods that use the OPTIMI_RSA technique. The administration of patient data, communication, and the quality of care have all been enhanced by digitizing healthcare records. The rising likelihood of illegal access and data breaches has prompted security worries inside the healthcare sector. In 2023, Lee and colleagues reported

This study aims to use user ID authentication to enhance security in healthcare systems while tackling the previously listed problems. The models outlined in this paper are appropriate for deployment in high-security contexts. It allows users with constrained resources to interact with cloud storage efficiently.

PROBLEM WITH TRADITIONAL ENCRYPTION ALOGORITH.

Public-key encryption like RSA is a common way for healthcare systems to keep private patient data safe. Still, because it is easy to attack multiple times, people need to be very aware of the risks and use good ways to protect themselves.

Encryption is at risk because of factoring attacks, which use RSA's mathematical traits to figure out prime numbers. Effective factorization stops anyone from decrypting any protected data without permission. Physical or temporal data can be used in side-channel hacks to find hidden keys. Attackers can figure out the key by keeping an eye on the decoding time.

When someone reads and changes protected messages, this is called a man-in-the-middle attack (Suman, Mondal, & Mandal, 2022). Even though it has flaws, RSA is still pretty safe when used correctly. To make things safer, use strong key management techniques, like making keys that are long and hard to guess, to stop factoring attacks.

If someone gets hold of the private key, they could decrypt data, so keeping it secret is very important. To keep the system safe from hackers, it's important to choose a safe version that doesn't have any known flaws.

USER'S ID AUTHENTICATION USING OPTIMI_RSA

The OPTIMI_RSA method was created to make regular RSA algorithms work better while protecting against factoring attacks, side channel attacks, and man-in-the-middle attacks. The Chinese Remainder Theorem with 5 big prime numbers makes RSA work better by breaking modular exponentiation down into smaller, easier-to-handle steps. The main goal of this method is to make the modular exponentiation process better. In Traditional, RSA uses modular exponentiation, which is very hard to compute, to make private keys. This model makes the process better by using CRT traits to cut down on the need for modular exponentiations. This makes decryption work a lot better, which is important for healthcare systems that need to get to patient data quickly.

Because patient information is private, data protection is very important in healthcare. Using this model along with OPTIMI_RSA protects the privacy and security of health data while they are being sent and stored in cloud-based systems. The improvement method speeds up decoding of data and makes the server's job easier. This works great for healthcare systems that don't have a lot of money or staff. If you need to access something quickly, like in e-healthcare systems, OPTIMI_RSA is the way to go. It makes difficult calculations work better for cloud-based healthcare systems, which speeds up the working time.

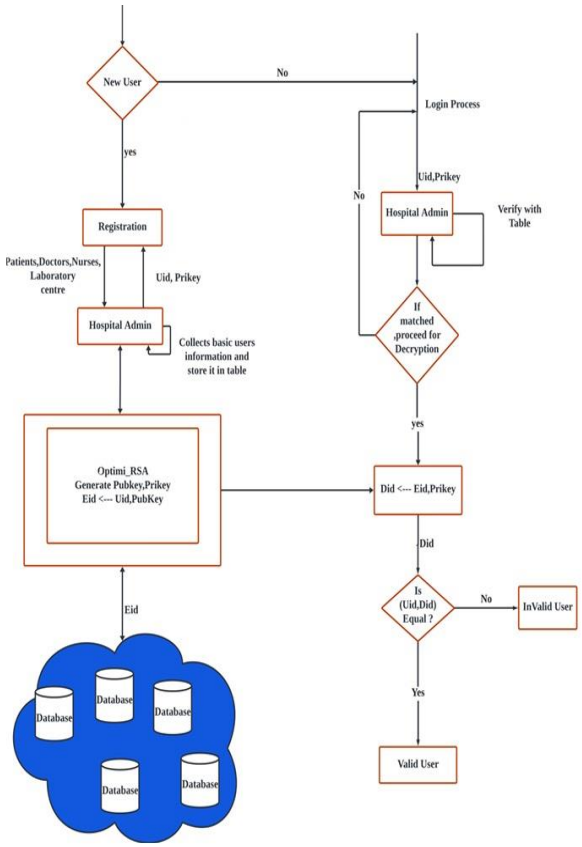

Figure 2: 4-Bit BEC

The Healthcare patient data security design with OPTIMI_RSA is a strong way to protect the privacy of healthcare systems in cloud storage settings. It builds its system on five prime numbers, which are used to make public and private keys for safe contact. The supervisor gives the new user the user's ID and secret key, which makes sure that they can safely register and have a smooth healthcare experience.

The Authentication Management Scheme is used to decrypt the user's ID after the ID has been checked. The method uses several stages of encryption to make sure the user is who they say they are. If the decrypted ID doesn't match the user's ID, they can't get in. This

method protects the privacy of patient information and builds a strong base for data protection in the healthcare environment.

The method also has big benefits when it comes to computational performance. It uses the Chinese Remainder Theorem to cut down on computational overhead, which speeds up encryption and decryption. In the cloud, where a lot of user IDs are saved and handled, this is especially important. Overall, the Healthcare patient data security design with OPTIMI_RSA is a complete and strong way to keep patient data safe in the cloud.

MATHEMATICAL MODLE OF OPTIMI_RSA

It involves the following steps

Step 1 : Key Generation

Step 2 : Public key Generation

Step 3 : Private key Generation

Step 4 : Encryption Process

Step 5 : Decryption Process using Chinese Remainder Theorem

Step 6 : Calculations of m values

STEP-1: KEY GENERATION

A: Choose five different prime numbers:

p1,p2,p3,p4,p5.

B: Calculate the public module:

n= p1*p2*p3*p4*p5

C: Calculate.

Ø(n): Ø(n)=(p1-1)*(p2-2)*(p3-3)*(p4-4)*(p5-5).

D: Choose a public exponent e such that

1<e< Ø(n) and gcd(e, Ø(n))=1.

E: Calculate the modular inverses with the primes.

- dp1≡d mod (p1-1).
- dp2≡d mod (p2-1).
- dp3≡d mod (p3-1).
- dp4≡d mod (p4-1).
- dp5≡d mod (p5-1).

Where d is the modular inverse of e mod Ø(n)

Calculate: qInv1, qInv2, qInv3, qInv4, qInv5.

- qInv1=$q1^{-1}$ mod p1

STEP:-2 PUBLIC KEY GENERATION.

Public_key is (e,n)

In public-key cryptography, a public key is represented as a pair of values, often denoted by (e, n).

To summarize, the public key (e, n) is used to encrypt messages. Anyone can encrypt data with this public key, but only the owner of the matched private key should be able to decode it (d, n). Figuring out the number "n" and its prime factors is a difficult math problem that is necessary for the security of the system. This is what the well-known RSA (Rivest-Shamir-Adleman) public-key encryption method is based on.

STEP 3: PRIVATE KEY GENERATION.

Use the modular inverses you collected earlier to figure out the private exponent d. This means that the private key is shown as (d,n).

In mathematical terms, the relationship between 'e', ' d', and Ø(n) is given by:

(e*d) mod Ø(n)=1.

The secrecy of the private key is important for RSA's security because it is hard to factor the number 'n'. With the public key, an attacker can read protected messages if they can factorize "n" or get the private key.

STEP 4: ENCRYPTION PROCESS

- Convert the plaintext message M to an integer m, using the recipient's public key (e, n).
- Calculate the cipher text using the following formula:
  $C=m^e$ mod n.
- To use RSA to encrypt a message, raise the number representation of the plaintext to the power of the public exponent e and split by the modulus n. The ciphertext is made with this method.
- For modular exponentiation m^e mod n, algorithms like square-and-multiply and binary exponentiation work well.

STEP 5: DECRYPTION PROCESS USING CRT.

Give the ciphertext, c

- Calculate c1= cdp1 mod p1
- c2=cdp2 mod p2

- c3= cdp3 mod p3
- c4= cdp4 mod p4
- c5=cdp5 mod p5

Calculation of 'm' value

- m1=c1*(p2*p3*p4*p5)*(qInv2*qInv3* qInv4* qInv5)
- m2=c2*(p1*p3*p4*p5)*(qInv1*qInv3* qInv4* qInv5)
- m3=c3*(p1*p3*p4*p5)*(qInv1*qInv2* qInv4* qInv5)
- m4=c4*(p1*p2*p3*p5)*(qInv1*qInv2* qInv3* qInv5)
- m5=c5*(p1*p2*p3*p4)*(qInv1*qInv2* qInv3* qInv4)

Reconstruct the decrypted message with

- m=(m1+m2+m3+m4+m5) mod n

When we use OPTIMI_RSA, decoding works faster, especially when n is larger. OPTIMI_RSA makes user identification better by fixing the problem with factoring in traditional RSA and making computers run faster. It makes people more likely to use bigger RSA keys, which indirectly makes things safer. It speeds up the decryption process by breaking it up into smaller steps that are easier to handle. This makes simultaneous work possible and eases the load on computers. This higher level of speed makes it possible to make keys faster, especially for big RSA keys.

MEMORY SPACE COMPARISON OF TRADITION RSA VS. OPTIMI_RSA

The OPTIMI_RSA technique uses less memory than the standard RSA method. Several things, such as smaller key numbers and more efficient data structures, are used to make this happen. The normal RSA method takes up a lot more memory than the OPTIMI_RSA technique. It takes about 16 KB of memory to store a 1024-bit OPTIMI_RSA key, which is half as much as a 1024-bit RSA key. The OPTIMI_RSA method can greatly lower the amount of memory used, which makes it perfect for high-performance or memory-limited programs.

Table: Memory and Execution Time Comparison b/w RSA & OPTIMI_RSA

Algorithm	Memory space(KB)	Execution Time
RSA	33500	0.786
OPTIMI_RSA	33000	0.685

Table shows, how much memory conventional RSA uses and how long it takes to run compared to OPTIMI_RSA. This shows how the improved RSA version makes cryptographic processes faster. For user ID verification, RSA and OPTIMI_RSA use different amounts of memory depending on the key size, how the method is implemented, and the hardware or software being used. In general, though, OPTIMI_RSA uses less memory than RSA. This is because the Chinese Remainder Theorem is used by OPTIMI_RSA to make the program work better and use less memory. In this case, OPTIMI_RSA needs 33000KB of RAM for user ID identification, while RSA needs 33500KB. This shows that it uses about 312 KB less memory than RSA, which means it is a little more memory-efficient.

COMPARATIVE EXECUTION TIME ANALYSIS OF RSA VS. OPTIMI_RSA.

An example of a well-known public-key encryption system that is recognized for its dependability and security is the RSA algorithm. On the other hand, it may be memory-intensive. A significant portion of the memory that is utilized by the RSA method is determined by the size of the key that is utilized. As an illustration, a 2048-bit RSA key requires around 32 KB of random access memory (RAM). All things considered, the OPTIMI_RSA approach is superior than the conventional RSA algorithm in terms of memory use and overall performance. For a healthcare system that requires great speed but has limited memory resources, this is an ideal alternative to consider. The time required for the execution of RSA in the case that has been shown is 0.786 milliseconds (ms), whereas the time required for OPTIMI_ RSA is 0.685 ms. The performance of OPTIMI_RSA is approximately ten percent faster than that of RSA in this scenario. OPTIMI_RSA has the potential to offer significant enhancements in speed, particularly for applications that require real-time encryption or decryption. Examples of such applications include secure communication protocols and file encryption tools.

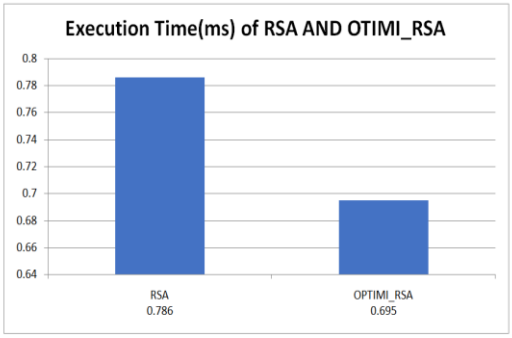

Fig.Comparative Execution Time of RSA vs. OPTIMI_RSA(ms).

In summary, OPTIMI_RSA is a memory-efficient solution for authenticating user IDs, making it a preferable alternative for healthcare systems that prioritize resource use and speed.

CONCLUSION

The OPTIMI_RSA algorithm is a variant of the RSA algorithm specifically engineered for memory efficiency. This is achieved through several methods, including the utilization of smaller key sizes and more efficient data structures. The Optimised RSA technique utilizes significantly less memory compared to the conventional RSA approach. A 1024-bit Optimised RSA key utilizes around 16 KB of RAM, which is half the amount used by a standard 1024-bit RSA key. The Optimised RSA approach can substantially decrease memory consumption, rendering it suitable for high-performance applications with constrained resources. The OPTIMI_RSA algorithm facilitates secure communication in embedded devices, such as smart cards and medical apparatus. The improved RSA algorithm offers several benefits compared to the standard RSA approach, including reduced memory consumption. Optimized RSA offers significant benefits compared to standard RSA, including improved performance and reduced power consumption. Its rapid execution speed renders it an efficient choice for several applications, while its little power consumption renders it optimal for battery-operated devices.

The implementation of OPTIMI_RSA enhances decryption efficiency, particularly for larger n values. This invention enhances user authentication by resolving the factorization problem in traditional RSA and augmenting computational efficiency. The method advocates for the utilization of larger RSA keys to enhance security. Moreover, it accelerates the decryption process by subdividing it into smaller, more manageable tasks. This facilitates parallel processing and decreases computational load. This enhanced efficiency significantly expedites essential generating, particularly.

REFERENCES

1. Alharbe, N, Aljohani, A, Rakrouki, MA & Khayyat, M 2023, ‘An Access Control Model Based on System Security Risk for Dynamic Sensitive Data Storage in the Cloud’, Applied Sciences, vol. 13, no. 5, pp. 3187-3203
2. Alsyouf, A, Lutfi, A, Alsubahi, N, Alhazmi, FN, Al-Mugheed, K, Anshasi, RJ et al. 2023, ‘The use of a Technology Acceptance Model (TAM) to predict patients usage of a

personal health record system: The role of security, privacy, and usability',International Journal of Environmental Research and Public Health, vol. 20, no. 2, p. 1347

3. Abdul Jabbar, MD & Aldeen, YAAS 2023, 'State-of-the-Art in Data Integrity and Privacy-Preserving in Cloud Computing', Journal of Engineering, vol. 29, no. 1, pp.42-60.
4. Anuradha, M, Jayasankar, T, Prakash, NB, Sikkandar, MY, Hemalakshmi, GR, Bharatiraja, C et al. 2021, 'IoT enabled cancer prediction system to enhance the authentication and security using cloud computing', Microprocessors and Microsystems, vol. 80,
5. Boomija, MD & Raja, SK 2023, 'Securing medical data by role-based user policy with partially homomorphic encryption in AWS cloud', Soft Computing, vol. 27, no. 1, pp. 559-568
6. Cao, S, Yan, J, Fang, Z & Wang, C 2023, 'A Searchable Encryption with Forward/Backward Security and Constant Storage', Applied Sciences (Switzerland), vol. 13, no. 4, p. 2181,
7. Chinnasamy, P & Deepalakshmi, P 2022, 'HCAC-EHR: Hybrid Cryptographic Access Control for secure EHR retrieval in healthcare cloud', Journal of Ambient Intelligence and Humanized Computing, vol. 13, pp. 1001-1019.