Enhanced I-RSA Technique for Security of Cloud Computing

Gurpreet Singh Matharu

Abstract- **Cloud computing displays a amazing capabilities to present price-potent and extra flexible offerings on-demand to the patrons over the community. It dynamically raises the capabilities of the group without coaching new people, investment in new infrastructure or licensing new software. Cloud computing has grown dramatically in the final few years because of the scalability of assets and appear as a rapid-growing section of the IT enterprise. The dynamic and scalable nature of cloud computing creates security challenges of their management by means of analyzing coverage failure or malicious pastime. This paper propose new technique, I- RSA to increase the security of the cloud computing. Results of the proposed technique is analyzed and compared with the existing technique on the basis of data encryption time and data decryption time.**

Keywords — **Cloud computing, AES, Security, Encryption, Decryption, RSA.**

I. INTRODUCTION

Cloud computing is likely one of the present day tendencies in the IT industry sometimes called on-demand computing. Computing is being transformed into a model consisting of services which can be commoditized and delivered in a way much like utilities corresponding to water, electricity, gasoline, and telephony.

Cloud Computing refers to manipulating, configuring, and having access to the functions online. It presents on-line information storage, infrastructure and application. The term Cloud alludes to a Network or Internet. At the end of the day, we can state that Cloud is something, which is available at remote area. Cloud can give benefits over system, i.e., on open systems or on private systems, i.e., WAN, LAN or VPN. Applications, for example, email, web conferencing, client relationship administration (CRM), all keep running in cloud.

Cloud computing has five fundamental characteristics as follows:

- **On-demand self service:** Distributed computing enables the clients to utilize web administrations and assets on request. One can logon to a site whenever and utilize them.
- **Broad network access:** Since distributed computing is totally electronic, it can be gotten to from anyplace and whenever.
- **Resource pooling:** Distributed computing enables numerous occupants to share a pool of assets. One can share single physical example of equipment, database and fundamental framework.
- **Rapid elasticity:** It is anything but difficult to scale up or down the assets whenever. Assets utilized by the clients or as of now allocated to clients are consequently checked and assets. It makes it conceivable.
- **Measured services:** Resource usage are monitored, measured, and reported (billed) transparently based on utilization. In short, pay for use.

II. BACKGROUND

S.Manjula et al. (2016) proposed work help to accomplish information protection utilizing division of information. In this two algorithms are used- Data Division algorithm and Data Replication Algorithm. To simplify this process we use JAVA and Cloud ME storage. Division of information in the cloud server shields documents from programmers in observing whole record and furthermore even the programmer saw the record put away, he may not see which part of document it is and furthermore he can't recognize what information it contains as it is scrambled. Safe circulation of record will be conceivable with legitimate approval. The encryption of document utilizing unbreakable calculation and split of the record guarantees information protection. [1]

Akshita bhandari et al. (2016) has presented HE-RSA or half and half encryption RSA alongside Advanced Encryption Standard or AES to guarantee productivity, consistency and reliability in cloud servers. The objective of this paper is to utilize different cryptographic idea amid correspondence alongside its applications in distributed computing and to upgrade the security of figure message or scrambled information in the cloud servers alongside limiting the substitution time, cost and memory measure amid encryption and decoding. It has been watched that the distinction between the running time of the first RSA and Improved Algorithm utilizing Hybrid Encryption-RSA and AES is expanding radically as the example measure is expanding. Additionally, utilizing diverse keys amid decoding avoided animal power, scientific and timing assaults. [2]

Mbarek Marwan et al. (2016) has described clients are charged in light of a compensation for every utilization plan of action. Accordingly, it drastically decreases working expenses related with the upkeep of the neighborhood server farm. As of late, database is given as a support of satisfy customers' request. Following this, organizations can depend on a remote database to deal with their information. Thus, associations are increasingly keen on embracing this new innovation as should have been obvious the advantages of doing as such. Despite its numerous points of interest, the move to cloud database emerges a few difficulties: administrative, legitimate and specialized. These calculations are utilized to perform just a single numerical operation, for example, expansion and augmentation. [3]

G.PrabuKanna et al. (2016) has proposed a novel personality based half breed encryption (RSA with ECC) to upgrade the security of outsourced information. In this approach sender encodes the delicate information utilizing half breed calculation. At that point the intermediary re encryption is utilized to scramble the catchphrase and personality in institutionalize toward improvement security of information. Our principle method is to utilize a personality based encryption (IBE) to cover the yield of open key encryption. This is accomplished by half and half encryption and intermediary re encryption strategies. In this approach the sender encode their information utilizing the half and half calculation with recipient character (ID) which is then added to the encryption of beneficiary personality and the catchphrase for producing the subsequent figure content Proxy Re Encryption (PRE) is connected to scramble the personality of collector and the watchword. The target of the proposed work is to enhance the security of outsourced information in distributed computing. This plan guarantees the security of client information and result portrays the proficiency of this work. [4]

Punam V Maitri et al. (2016) has discussed about new security mechanism using symmetric key cryptography algorithm and steganography. In this proposed system AES, blowfish, RC6 and BRA algorithms are used to provide block wise security to data. All parts of file are encrypted simultaneously with the help of multithreading technique. Data encryption Keys are inserted into cover image using LSB technique. Stego image is send to valid receiver using email. For file decryption purpose reverse process of encryption is applied. With the help of proposed security mechanism data integrity, high security, low delay, authentication and confidentiality parameters are accomplished. For AES text decryption needs 15% to 17% maximum time as compare to proposed system. In Blowfish for encryption need 12% to 15% maximum time as compare to proposed hybrid algorithm. [5]

N.Jayapandian et al. (2016) has made comparison between the two encryption algorithm- DES and RSA. DSA and RSA are two normal encryption calculations. RSA isn't substantially quicker while creating a key than DSA. in addition, RSA is speedier at encryption than DSA strategy. While unscrambling, DSA demonstrates their quality, basically because of its incredible decoding ability If you require computerized examination technique for marking, DSA is the encryption calculation for the investigation of the procedure of the advanced mark. RSA is the best strategy for the check of information. Since the method for utilizing the level of key for security contrasts as they can utilize the key as where the place it rely upon utilization of private and open as indicated by where they scramble and unscramble. [6]

Vinay Pal Bansal et al. (2015) has presented a hybrid cryptosystem utilizing RSA and Blowfish calculation. Blowfish cryptosystem is one of the quick and solid calculation utilized for cryptography. The unscrambling system is same as the encryption method yet the P-exhibit is utilized as a part of turn around arrange. The encryption and unscrambling forms utilize same kind of Feistel organize. This system likewise gives security from beast constrain moreover. As, two diverse encryption calculations are utilized here, the ideal mix of both keys is important to unscramble the information whicyh is extremely hard to accomplish. In this way, the proposed cross breed system gives security and highlights superior to the past independently utilized strategies. Blowfish and RSA are additionally control effective calculations. [7]

Majda Omer Elbasheer et al. (2015) has purposed implementation by CA by NTRU open key cryptosystem calculation, in term of key age, marking X.509 declarations and check of mark. Execution has been created utilizing java dialect. Moreover, the outcomes have been contrasted and RSA in a similar domain. As consequence of this work, NTRU can create CA all the more effectively contrasting and RSA. In this paper to the creator demonstrated that NTRU calculation is suitable to work with the PKI. The examination are made amongst RSA and NTRU based on key age and process time. As outlines, from the effectiveness perspective, the paper comes about present the NTRU is superior to RSA. In this manner, the utilization of NTRU with the PKI permit to frameworks that have impediment in their condition like cell phones and sensor gadgets to work with the PKI on the off chance that they utilize the NTRU in checking declarations, moreover it upgrade the execution of PKI so it can serve bigger group by most noteworthy effective in correlations with the utilizing of RSA . This paper has been worried about the productivity of CA ingenerating authentications, additionally it show the speed of check of them. [8]

Vijay Kumar Pant et al. (2015) has described how to secure data and information in cloud environment in time of data sharing or storing by using our proposed cryptography and steganography technique. In first level we use cryptography using RSA algorithm, second level he used steganography technique where he hide the data within the image and third level he accessed the data from image and decrypted data using RSA algorithm. Here he used this method only for image data hiding but this also apply for video, text or audio. [9]

Sakinah Ali Pitchay et al. (2015) has proposed a framework that will utilize Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) blend encryption process utilizing USB gadget. The records might be gotten to in the cloud however every one of the documents will remain encoded till the USB gadget is connected to the PC. The purpose of applying such technique is to completely secure the documents and abstain from utilizing one single secret word. The arbitrarily created passkeys are exceptionally mind boggling blends therefore client won't have the capacity to completely remember them. The proposed framework will identify the USB that contains the private-key utilized for the documents to be downloaded from the cloud. The goal of the security in the cloud computing is to keep the data secure and confidential on the cloud. [10]

III.PROPOSED TECHNIQUE

In the existing system, RSA algorithm is used which involves two keys termed as public and private. The public key is used for encryption process and private key is used for decryption. Both the keys use the same computed 'N' value. The proposed Improved RSA I-RSA algorithm uses two different 'N' values for encryption and decryption. The objectives of the proposed technique are:

- To do the comparative study of existing security algorithms such as RSA and PAILIER algorithms.
- To propose a new technique, I- RSA to increase the security of the cloud computing.
- To more optimize the values of RSA using LCS algorithm.
- To compare the results of proposed technique with the existing techniques on the basis of:
    a. Data Encryption time
    b. Data Decryption time

The algorithm of proposed technique is as follows:

1. Key Generation involves the following steps.
2. Select any two large prime numbers P and Q. Apart from these, choose two more prime numbers PR1 and PR2 using LCS algorithm.
3. Compute the values of N1 and N2 by
4. $N1 = P * Q * PR1 * PR2$
5. $N2 = P * Q$
6. Calculate $\Phi(r) = (P-1) * (Q-1) * (PR1-1) * (PR2-1)$
7. Select the Public Key E, so that $GCD(E, \Phi(r)) = 1$.
8. The Private Key D is calculated from $D * E = 1 * mod(\Phi(r))$.
9. Thus, the Public key component has a pair of E and N1 and Private Key pair as D and N2.
10. Encryption Process The formula for generating a cipher text from the given plain text is $C = ME \bmod (N1)$.
11. Decryption Process The Plain text can be found by using $M = CD \bmod (N2)$.

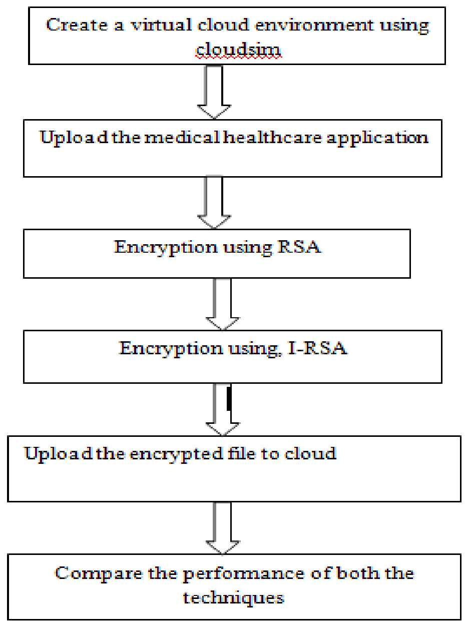
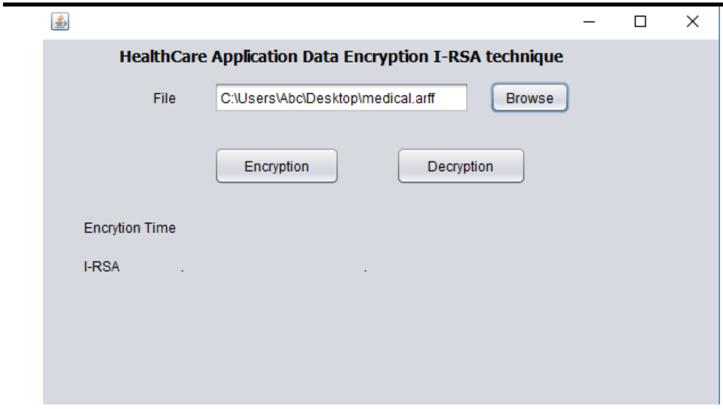

Create a virtual cloud environment using cloudsim
Upload the medical healthcare application
Encryption using RSA
Encryption using I-RSA
Upload the encrypted file to cloud
Compare the performance of both the techniques

Figure 3.1 Proposed Technique

IV.EXPERIMENTAL RESULTS

The proposed system is actualized with the assistance of CloudSim and Net beans IDE 8.0.



HealthCare Application Data Encryption I-RSA technique

File C:\Users\Abc\Desktop\medical.arff

Figure 4.1 Encryption Process

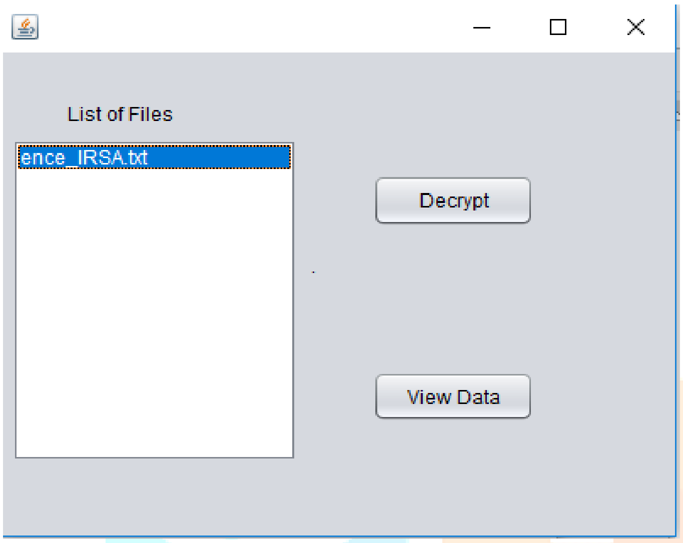


Figure 4.2 Decryption Process

Table 4.1: Encryption time with RSA and Proposed I-RSA

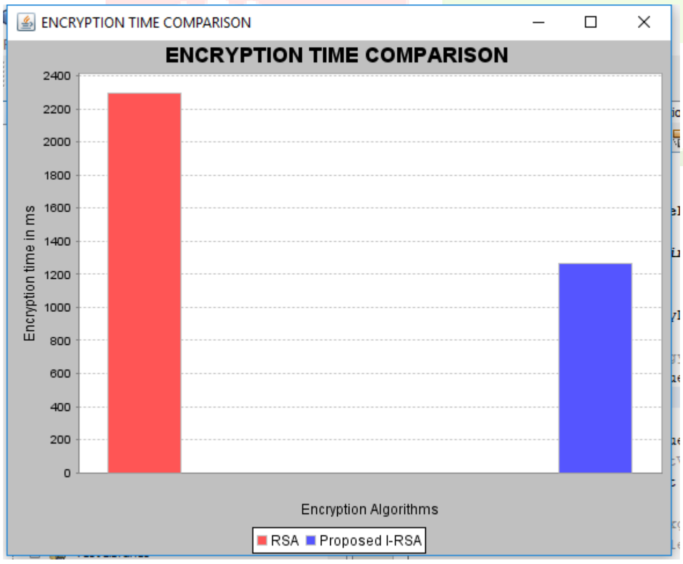


Figure 4.3 Comparison of encryption time of proposed technique with RSA

Table 4.2 Encryption time with Pailier and Proposed I-RSA

Homomorphic base paper technique with Pailier	6499 milliseconds
Proposed Encryption with I-RSA	1266 milliseconds

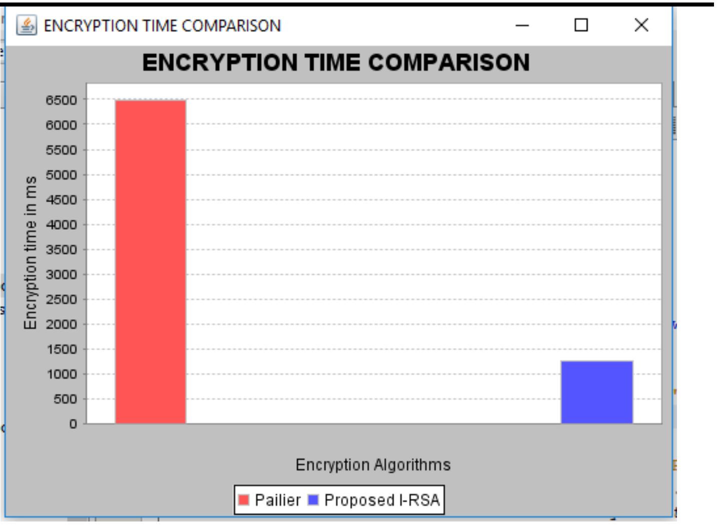


Figure 4.4 comparison of encryption time of proposed technique with Pailier

Table 4.3 Decryption time with RSA and Proposed I-RSA

Homomorphic base paper technique with RSA	2298 milliseconds
Proposed Encryption with I-RSA	1266 milliseconds

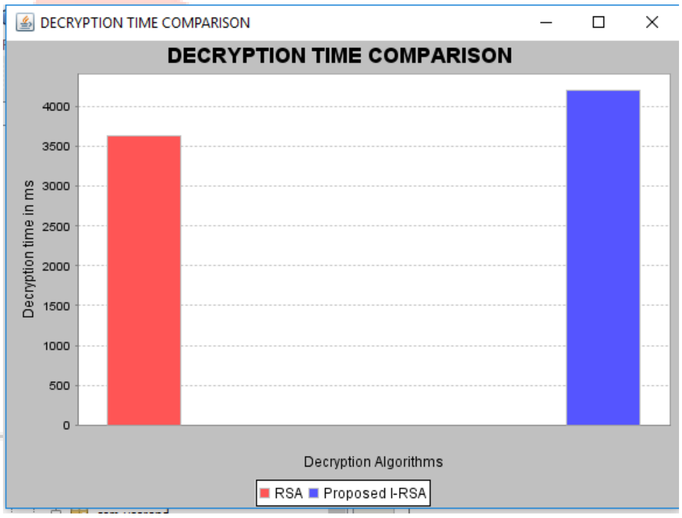


Figure 4.5 Representing comparison of decryption time of proposed technique with RSA

V. CONCLUSION

In this research work, a new technique is proposed named I- RSA to increase the security of the cloud computing. This work optimizes the values of RSA using LCS algorithm. In the existing system, RSA algorithm is used which involves two keys termed as public and private. The public key is used for encryption process and private key is used for decryption. Both the keys use the same computed 'N' value. The proposed Improved RSA I-RSA algorithm uses two different 'N' values for encryption and decryption. The proposed methodology is implemented with the help of CloudSim and Net beans IDE 8.0. Results are evaluated by comparing the proposed technique with the existing technique by using data encryption time and data decryption time. Proposed technique take 1266 milliseconds for encryption and 4199 milliseconds for decryption process. Proposed technique takes more time for decryption process as it is more secure than the existing technique. In this research, improvement in RSA is implemented. In future, we can enhance the security of the algorithm by adding security at authentication level using biometric devices. Further decryption time of the algorithm should be reduced. Also we can make encryption process more optimized by using some AI techniques.

Homomorphic base paper technique with Pailier	3638 milliseconds
Proposed Encryption with I-RSA	4199 milliseconds

REFERENCES

1. S.Manjula, Dr.M.Indra Devi, and R.Swathiya, “Division of data in cloud environment for secure data storage”, *International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE)*, pp. 1-5, IEEE. 2016.
2. Akshita bhandari, Ashutosh Gupta, and Debasis Das, “Secure algorithm for cloud computing and its application”, *6th International Conference on Cloud System and Big Data Engineering (Confluence)*, pp. 188-192, IEEE. 2016.
3. Mbarek Marwan, Ali kartit, and Hassan Ouahmane, “Applying homomorphic encryption for securing cloud database” *4th IEEE International Colloquium on Information Science and Technology (CiSt)*, pp. 658-664. IEEE. 2016.
4. G.PrabuKanna and V.Vasudevan, “Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud” *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 3688-3693, IEEE.2016.
5. Punam V Maitri and Aruna Verma, “Secure file storage in cloud computing using hybrid cryptography algorithm” *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 1635-1638 IEEE.2016.
6. N.Jayapandian, Dr.A.M.J.Md.Zubair Rahman, S.Radhikadevi and M.Koushikaa, “Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption” *World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, pp. 1-4. IEEE. 2016.
7. Vinay Pal Bansal and Sandeep Singh, “A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs” *2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS)*,. pp.1-5. IEEE.2015.
8. Majda Omer Elbasheer and Dr.Taring Mohammed, “Signing and verifying certificates by NTRU and RSA algorithm” *International Conference on Cloud Computing (ICCC)*, pp. 1-4. IEEE.2015.
9. Vijay Kumar Pant, Jyoti Prakash andAmit Asthana, “Three step data security model for cloud computing based on RSA and Stegnography techniques” *International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 490-494. IEEE. 2015.
10. Sakinah Ali Pitchay, Wail Abdo Ali Alhiangem, Farida Ridzuan and Madihah Mohd Saudi, “A proposed system concept on enhancing the encryption and decryption method for cloud computing”*17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim)*, pp. 201-205. IEEE. 2015 IEEE.
11. Mr.Rupesh R Bobde, Prof.Amit Khaparde and Prof.Dr.M.M.Raghuwanshi, “An approach for securing data on cloud using data slicing and cryptography” *9th International Conference on Intelligent Systems and Control (ISCO)*, (pp. 1-5). IEEE. 2015.
12. Randeep Kaur and Supriya Kanger, “Analysis of security algorithms in cloud computing” *International Journal of Application or Innovation in Engineering and Management*.vol 3, issue 3, pp. 171-6 2015.
13. Preeti Garg and Dr.Vineet Sharma, “An efficient and secure data storage in mobile cloud computing through RSA and hash function”, *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp. 334-339. IEEE. 2014.
14. Vishwanath S Mahalle and Aniket K Shahade, “Enhancing the data security in cloud by implementing hybrid(RSA & AES) encryption algorithm”, *International Conference on Power, Automation and Communication (INPAC)*, pp. 146-149. IEEE. 2014.
15. Chaoqun Yu,Lin Yang,Yuan Liu, Xiangyang Luo, “RESEARCH ON DATA SECURITY ISSUES OF CLOUD COMPUTING”, IEEE, 2014, pp. 1-6.
16. Feng Zhao, Chao Li, Chun Feng Liu, “A cloud computing security solution based on fully homomorphic encryption”, IEEE, 2014, pp. 485-488.
17. Dr. P. Dinadayalan, S. Jegadeeswari, Dr. D. Gnanambigai, “Data Security Issues in Cloud Environment and Solutions”, IEEE World Congress on Computing and Communication Technologies, 2014, pp. 88-91.
18. M. Sugumaran , BalaMurugan. B, D. Kamalraj, “An Architecture for Data Security in Cloud Computing”, IEEE World Congress on Computing and Communication Technologies, 2014, pp. 252-255.
19. Mr.Prashant Rewagad and Ms.Yogita Pawar, “Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance security in cloud computing” *International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 437-439. IEEE.2013.
20. T V Sathyanarayana, Dr. L. Mary Immaculate Sheela, “Data Security in Cloud Computing”, IEEE International Conference on Green Computing, Communication and Conservation of Energy, 2013, pp. 822-827.