International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 3, ISSN No. 2455-2143, Pages 37-41
Published Online July 2018 in IJEAST (http://www.ijeast.com)

ACHIEVING CLOUD SECURITY USING IMPROVED RSA ENCRYPTION ALGORITHM FOR HEALTHCARE DATABASE

Gurpreet Singh Matharu
Department of CSE
Organization Sviet, Banur, Punjab, India
Computer Science and Engineering
Swami Vivekanand Institute of Engineering and Technology

Abstract- **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. In this sort of model, customers entry services headquartered on their specifications, regardless of where the offerings are hosted. 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.**

Keywords – **Cloud computing, AES, Security, Encryption, Decryption, I- RSA.**

I. INTRODUCTION

.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. In short, cloud computing allows for the sharing and scalable deployment of offerings, as needed, from close to any location, and for which the consumer can also be billed founded on precise usage. It is headquartered on the notion of dynamic provisioning, which is utilized no longer most effective to services but also to compute ability, storage, networking, and expertise science(IT)infra constitution traditionally. Assets are made to be had by way of the internet and furnished on a pay-per-use groundwork from cloud computing vendors.

Cloud Deployment Model

Public cloud: A cloud is to be entitled as open cloud at the point when the organizations (like applications, storing) are being given over framework that are open publically, anyone can get to it. Open cloud's favorable circumstances may be taken as on a pay for each use mode or other getting plans. The National Institute of Standards and Technology characterizes an open Cloud as a Cloud framework that is influenced accessible to the overall population or an expansive industry to gathering. Open Clouds are claimed by the organization(s) offering Cloud administrations. Figure 1.8 beneath gives a fundamental outline of an association utilizing a public Cloud, Public Cloud computing means relying on third parties to provide effective IT services.

Private cloud: A private cloud is a foundation that gives the organizations to a lone affiliation, paying little heed to whether supervised by inside or by a pariah. Cloud which is encouraged remotely is named as "remotely encouraged" private cloud and other encouraged by third social affair are named as "on introduce" private cloud. This organization of appropriated registering is done in disengaged route now here no need of web workplaces in the private cloud show manage and work with untouchable inspector . Private Cloud Computing. On the other hand, Private Cloud figuring reassures the affiliation that their information and methodology are more secure since everything is overseen inside. As indicated by the NIST a private Cloud is a Cloud framework that is worked exclusively for an association. The association or an outsider can oversee it. Private Clouds can exist nearby or off-site Typically private Clouds are utilized when touchy information is included. Figure 2 underneath gives a fundamental representation of an association utilizing a private Cloud.

Hybrid cloud: This is an accumulation of private and in addition open cloud alternatives.) That remaining parts special substances yet is bound together by institutionalized or restrictive innovation. The cross breed cloud is a blend of open and private cloud. Non- essential activities are performed using open cloud while the fundamental activities are performed using private cloud.

Community cloud model: This cloud show enables framework and administrations to be open by collection of relations. It shares the foundation between a few associations

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 3, ISSN No. 2455-2143, Pages 37-41
Published Online July 2018 in IJEAST (http://www.ijeast.com)

from a particular group. It might be overseen by inside or by outsider.

II. LITERATURE REVIEW

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", 2015

Data security is real problem in cloud condition. The information proprietor has not control on the information after it is transferred on cloud. The creator [11] has proposed a plan in this the first information get cut into various cuts. The information in each cut can be encoded by utilizing diverse cryptographic calculations and encryption enter before putting away them in the Cloud. The goal of this strategy is to store information in a legitimate safe way keeping in mind the end goal to stay away from interruptions and information assaults mean while it will lessen the time and cost to store the scrambled information in the Cloud Storage. In this proposed approach the information is splitted into different cuts, at that point connected different distinctive encryption calculations as per security level. The level of multifaceted nature of security shifts agreeing levels and complex encryption calculation will going to pick. This different encryption calculation give more safe than utilizing single encryption calculation to scramble the information**.**

Randeep Kaur and Supriya Kanger, "Analysis of security algorithms in cloud computing", 2015 In this paper the author [12] has explained about the different techniques RSA, DSA, Blowfish, Diffie Hellman etc. that are used to provide security in the field of cloud computing on the basis of different parameters. In this paper the author compare the different algorithm on the basis of different parameters- block size, key length, security and speed.

Preeti Garg and Dr.Vineet Sharma, "An efficient and secure data storage in mobile cloud computing through RSA and hash function", 2014 In this paper the author [13] ensured the accuracy of clients' information in the cloud, he proposed a compelling component with striking element of information honesty and secrecy. This paper proposed a system which uses the possibility of RSA estimation, Hash work close by a couple of cryptography instruments to give better security to the data set away on the compact cloud. Here we additionally host a Trusted Third Get-together Auditor (TPA) who is exceptionally very much trusted. TPA checks the respectability of the information put away on versatile cloud for the information proprietor. TPA checks the hash and message to confirm the respectability of the information. The Integrity Verification is given by the TPA which lessens a great deal of work of the versatile client. In this arrangement data proprietor has two keys, one of which is basically known to him called private key and another is open key. Here message/file is encoded twice immediately, by proprietor's private key and open key of TPA. So this gives the secrecy to the information of versatile client. In proposed technique RSA calculation is utilized for performing encryption and decoding which gives message confirmation.

Chaoqun Yu,Lin Yang,Yuan Liu, Xiangyang Luo, "Research on Data Security Issues of Cloud Computing", 2014 The author [15] surveyed conditions of the specialty of the procedures on distributed computing information security issues, for example, information encryption, get to control, trustworthiness validation and different issues. This article concentrated on the essential issue of distributed computing, information security. The exploration advance of issues of information encryption, get to control, honesty confirmation et cetera regarding distributed computing information security is overviewed.

Feng Zhao, Chao Li, Chun Feng Liu, "A cloud computing security solution based on fully homomorphic encryption", 2014 The author [16] proposed a new kind of data security respond in due order regarding the precariousness of the dispersed figuring and the circumstances of this application is later on created. This new security game plan is totally fit for the preparing and recovery of the scrambled information , and adequately prompting the wide pertinent prospect, the security of information transmission and the capacity of the distributed computing. In view of the cloud information security issue confronted, this article displayed the homomorphic encryption framework, proposes a dispersed figuring data security plot. The arrangement ensures the transmission data between the cloud and the customer security. What's more, in the distributed storage their information is as yet protected. It is advantageous for clients and the outsider office to look date to arrange.

Dr. P. Dinadayalan, S. Jegadeeswari, Dr. D. Gnanambigai, "Data Security Issues in Cloud Environment and Solutions", 2014 The author [17] analyzed the fundamental issue of distributed computing and portrayed the information security and protection insurance issues in cloud. Despite the truth that the Cloud providers pitch that the set away information will be secure and set up, there are security ambushes which incite loss of data. To overcome the loss of data, the data security guidelines are executed in different ways to deal with guarantee the data. Data security isn't just particular issues, it in like manner incorporates various alternate points of view, for instance, organization, regulatory approach, laws and bearings, et cetera. With the unrelieved undertakings of entire disseminated registering condition and the consistent difference in critical laws and controls, on executing these game plans in conveyed figuring, it will give secured organizations to customers.

M. Sugumaran , BalaMurugan. B, D. Kamalraj, "An Architecture for Data Security in Cloud Computing", 2014

The author [18] discussed about a segment of the frameworks that were completed to guarantee data and propose designing to secure data in cloud. This building was delivered to store data in cloud in mixed data orchestrate using cryptography framework which relies upon square figure. Cloud security is fundamental in light of the way that it is no doubt the principle inspiration why affiliations fear the cloud. To defeat these dread information security is actualized in various approaches to ensure the information. In distributed figuring, these issues towards data security and those techniques, the proposed building using symmetric cryptography beats these issues and complete the cloud as a capable development for securing the customer's data.

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", 2013 In this paper, the author [19] proposed the method to influence utilization of computerized mark and Diffie Hellman to key trade mixed with AES encryption calculation to secure classification of information put away in cloud. Regardless of whether the key in transmission is hacked, the office of Diffie Hellman key trade render it pointless, since enter in travel is of no utilization without client's private key, which is limited just to the true blue client. This proposed design of three way component makes it intense for programmers to split the security framework, along these lines ensuring information put away in cloud. In our proposed engineering, he utilized three ways security conspire. Right off the bat Diffie Hellman estimation is used to create keys for key exchange step. By then propelled stamp is used for confirmation, from that point AES encryption calculation is used to encode or decode client's information document. This is executed to give trusted registering condition with a specific end goal to dodge information alteration at server. Two distinct servers are kept up, for encryption procedure called figuring stage and another called limit server for securing customer data record. Exactly when a customer needs to exchange an archive to the cloud server, first key are exchanged utilizing Diffie Hellman key exchange at the period of login, by then the client is affirmed using propelled stamp. Customer's data archive is mixed utilizing AES and at precisely that point it is exchanged to another Storage server. By and by when client require same record, it is to be downloaded from cloud server. Thus, when customer login, first encryption keys are exchanged, record to be downloaded is picked, affirmation happens using mechanized mark by then, AES is used to translate the saved archive and client can get to the record.

T V Sathyanarayana, Dr. L. Mary Immaculate Sheela, "Data Security in Cloud Computing", 2013 The author [20] presented examination of data safety problems in a cloud space. Examination of these plans could be used to choose the lacunae in the data safety problems. Security of cloud-based applications is key stresses of cloud customers. Secure programming and secure programming life cycle organization are important to the protection of cloud organizations. The information security of cloud structures lay on the customary models of protection, openness, and genuineness, however associated with coursed, virtualized, and dynamic designs.

Ni Zhang, Di Liu, Yun-Yong Zhang, "A Research on Cloud Computing Security", 2013 The author [21] discussed many cutting edge specialized arrangements, e.g., continuation insurance instrument, IDM, information security, and virtualization security to defeat challenges from cloud security. To clear up cloud security, a definition and extent of distributed computing security is introduced. A biological community of cloud security is appeared to outline what every part in industry can do thusly. At that point security effects of cloud security for the two clients and administrators are broke down. At long last, prescribed procedures on point of view of administrator are outlined and a conclusion is directed.

Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev and Shiv Shakti Shrivastva, "Cloud user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment", 2012 In this paper the author [22] proposed a new distributed computing condition where we approach a trusted cloud condition which is controlled by both the customer and the cloud condition administrator. Our approach is for the most part isolated into two sections. Initial segment is controlled by the ordinary client which gets consent by the cloud condition for performing operation and for stacking information. Second part demonstrates a protected put stock in registering for the cloud, if the administrator of the cloud need to peruse and refresh the information then it take consent from the customer condition. This gives an approach to conceal the information and typical client and can shield their information from the cloud supplier. This gives a two way security convention which helps both the cloud and the ordinary client. For the above idea we apply RSA and MD 5 calculation. At the point when the cloud client transfer the information in the cloud condition, the information is transferred in encoded shape utilizing RSA calculation and the cloud administrator can decode utilizing their own particular private key. For refreshing the information in the cloud condition administrator ask for the client for a protected key. Cloud client sends a safe key with a message process tag for refreshing information. On the off chance that any untouchables play out an adjustment in the key, the label bit is additionally changed demonstrating the key isn't secure and remedy.

Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", 2012 The author [23] provided a compact however overall examination on information security and affirmation insurance issues related with appropriated preparing over all times of information life cycle. By then this paper talks about some present approaches. It is amazing that scattered preparing has different potential focal concentrations and different meander applications and information are moving to open or cross breed cloud. Notwithstanding, with respect to some business-basic applications, the affiliations, particularly clearing endeavors, still wouldn't move them to cloud. The market measure the passed on figuring shared is up 'til now a long ways behind the one predicted. From the clients' point of view, coursed preparing security concerns, particularly information security and security affirmation issues, remain the major inhibitor for decision of appropriated enrolling associations. This paper described future research work about data security and privacy protection issues in cloud.

Wenjun Fan and Xudong Chen, "Parallelization of RSA algorithm based on compute unified device architecture", 2010 In this paper the author [24] presents a novel parallelized usage of RSA calculation utilizing JCUDA and Hadoop. Initially the rule of custom RSA calculation is considered. Besides, the parallel RSA calculation is composed and acknowledged in CUDA system. Thirdly, with JCUDA, the RSA parallel calculation actualize work is called by every hub in Hadoop bunch. Our exploratory outcomes exhibit the speed of RSA calculation upgraded drastically contrasted with the first strategy on the CPU as it were. In this paper, we exhibited our experience of porting RSA calculation on to CUDA engineering. We dissected the parallel RSA calculation, depicted our parallelization methods at tow parallel levels, and talked about the outcomes close behind perspectives. The bottleneck for RSA calculation lies in the plaintext measure. This paper plan a strategy to PC the information parcels parallel utilizing the strings separately in light of CUDA. This is with a specific end goal to acknowledge execution enhancements which prompt streamlined outcomes

Iuon-Chang Lin and Hsing-Lei Wang, "An improved digital signature scheme with fault tolerance in RSA", 2010 The integrity and safety of data transmission are very vital problems. In this paper, author [25] had reviewed a computerized signature plot with adaptation to internal failure in light of the RSA cryptosystem. The proposed plan can effectively keep the secrecy of the exchanged message. Besides, the plan can recognize and remedy the blunder happening in the calculation procedures or information transmission procedure. Notwithstanding, Zhang's plan has a genuine weakness that abuses the standards of a protected computerized signature. Subsequently, this paper investigated the powerlessness that disregards the standard of a safe computerized signature in this paper and propose an enhanced plan to conquer the defenselessness. In the end, proposed computerized signature plan can be utilized as a part of distributed computing. A vindictive client can without much of a stretch produce a message by utilizing the legitimate mark of the first message. In any case, the legitimate client can't deny that he/she didn't sign the manufactured message. To take care of the issue, he proposed an enhanced plan in view of the RSA cryptography.

III. PROPOSED WORK

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

IV. 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 utilized to encrypt data and private key is utilized to decrypt data. Both the keys use the same computed 'N' value. The proposed Improved RSA I-RSA algorithm utilizes two distinct 'N' values to encrypt and decrypt. 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.

V. FUTURE SCOPE

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.

VI. REFERENCES

1. Ni Zhang, Di Liu, Yun-Yong Zhang.(2013), "A Research on Cloud Computing Security", IEEE International Conference on Information Technology and Applications, (pp. 370-373).
2. Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev and Shiv Shakti Shrivastva.(2012), "Cloud user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment", *Sixth International Conference,* IEEE *(* pp. 1-8).
3. Deyan Chen, Hong Zhao.(2012), "Data Security and Privacy Protection Issues in Cloud Computing", IEEE International Conference on Computer Science and Electronics Engineering, ,(pp. 647-651).
4. Wenjun Fan and Xudong Chen.(2010), "Parallelization of RSA algorithm based on compute unified device architecture", *9th International Conference.* IEEE, *(* pp. 174-178.).
5. Iuon-Chang Lin and Hsing-Lei Wang.(2010), "An improved digital signature scheme with fault tolerance in RSA", *Sixth International Conference*. IEEE.(pp. 9-12).
6. Chaoqun Yu,Lin Yang,Yuan Liu, Xiangyang Luo.(2014), "RESEARCH ON DATA SECURITY ISSUES OF CLOUD COMPUTING", IEEE, (pp. 1-6).
7. Feng Zhao, Chao Li, Chun Feng Liu.(2014), "A cloud computing security solution based on fully homomorphic encryption", IEEE, ,(pp. 485-488).
8. Dr. P. Dinadayalan, S. Jegadeeswari, Dr. D. Gnanambigai.(2014), "Data Security Issues in Cloud Environment and Solutions", IEEE World Congress on Computing and Communication Technologies,(pp. 88-91).
9. M. Sugumaran, BalaMurugan. B, D. Kamalraj.(2014), "An Architecture for Data Security in Cloud Computing", IEEE World Congress on Computing and Communication Technologies,(pp. 252-255).
10. Mr.Prashant Rewagad and Ms.Yogita Pawar.(2013), "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),* IEEE, (pp. 437-439).
11. T V Sathyanarayana, Dr. L. Mary Immaculate Sheela.(2013), "Data Security in Cloud Computing", IEEE International Conference on Green Computing, Communication and Conservation of Energy, (pp. 822-827).
12. N.Jayapandian, Dr.A.M.J.Md.Zubair Rahman, S.Radhikadevi and M.Koushikaa.(2016), "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),* IEEE, *(*pp. 1-4).
13. Vinay Pal Bansal and Sandeep Singh.(2015), "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),*IEEE,*(* pp.1-5).
14. Majda Omer Elbasheer and Dr.Taring Mohammed.(2015), "Signing and verifying certificates by NTRU and RSA algorithm" *International Conference on Cloud Computing (ICCC),* IEEE,(pp. 1-4).
15. Vijay Kumar Pant, Jyoti Prakash andAmit Asthana.(2015), "Three step data security model for cloud computing based on RSA and Stegnography techniques" *International Conference on Green Computing and Internet of Things (ICGCIoT),* IEEE ,(pp. 490-494).
16. G.PrabuKanna and V.Vasudevan.(2016), "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),* IEEE,(pp. 3688-3693).