Data Security In Cloud Computing Using RSA Algorithm

Krishna Biju
Intergated MCA
Amal Jyothi College Of Engineering, Kanjirappally
Kottayam,Kerala
krishnabiju@mca.ajce.in

Dr.Juby Mathew
Assistant Professor
Department of Master of Computer Application
Amal Jyothi College Of Engineering
Kottayam,Kerala
jubymathew@amaljyothi.ac.in

***Abstract*— Now a days knowledge security is a lot of necessary in net world. Today's hottest analysis space is Cloud computing because of its ability to cut back the price that related to computing. it's the foremost attention-grabbing and supply new security challenges that gives varied services to the users over the network. This paper that specializes in the info storage security problems in Cloud atmosphere. though the Cloud Computing is a lot of spectacular and encourage, however their area unit several challenges for knowledge security as there's no district of the info for the Cloud user. to confirm the protection of information, we tend to planned a way by implementing by RSA rule. when corporal punishment RSA rule, we are able to secure {the knowledge the info the information} by encrypting the initial data then decrypting the info that offer by the Cloud supplier. Cloud supplier will solely manifest the user and delivers the info to the user.**

Keywords—Cloud Computing, RSA rule, coding of information, decoding of information, Security of information

I. INTRODUCTION

In several tiny, medium and huge sized organizations has key propulsion is Cloud Computing. And additionally, several cloud users make use of the offerings supplied by using the Cloud Computing. the safety of their information inside the Cloud is that the main difficulty. Securing {the information the info the records} is frequently the significance due to the vital nature of cloud computing and also the large amounts of advanced facts it carries, the requirement is additional vital. Calculate, storage, software package likes these problems and proposes new model for computing by Cloud Computing Cloud Computing affords development environment ，allocation and reallocation of assets as soon as is needed，garage and networking facility nearly. Victimization coding methods, the protection should be obligatory on knowledge to realize secured knowledge storage and access. attributable to incomprehensibility nature of cloud, continues to be having security problems.

The cloud infrastructure is additional dependable and effective than personal computing，however huge selection of inner，outside threats for expertise maintains at the cloud. Enforcing security features cannot be applied directly as a result of the information aren't hold in consumer space. During this work, we have a tendency to implementing RSA rule before storing the sensitive knowledge in cloud as soon as the legal person requests the information for utilization then decrypted and provider to the purchaser the use of RSA rule ，I projected a technique for Cloud{computing system computer system automatic knowledge processing system|ADP system|ADPS|system} by providing data storage and securing Cloud ADP system. Throughout this technique some essential protection services consisting of key generation，encryption and decryption are supplied in Cloud Computing.

II. SECURITY ISSUES OF DATA IN CLOUD

A. Privacy and Confidentiality:

There ought to be some guarantee that access to it information can solely be restricted to the licensed access once the shopper host information to the cloud. via Cloud employees is associate degree other chance which could reason capability hazard to cloud statistics as soon as an inappropriate get admission to patron sensitive information. The consumers，correct practices and privateness regulations ought to be in situ to guarantee the cloud customers of the records protection by way of imparting assurances. facts hosted on the cloud are private that by means of the cloud seeker should be confident.

B. Intergity of Data:

The security of information by providing with, to confirm information integrity ought to be implement mechanisms by cloud suppliers. And ready to be tell what passed off to an precise information set. The consumer tuned in to what precise facts is hosted on the cloud, the starting place and also the integrity mechanisms region in situ for compliance features, it ought to be essential to very own specific records on what facts changed into located I am public cloud, as soon as it happened, what virtual reminiscences ought to be built by cloud supplier.

C. Data Avaliability:

Person statistics normally keep in package deal on absolutely extraordinary servers often living in several locations or in several Clouds. During this case, information availableness become a serious consistent

DOI: 10.5281/zenodo.6223508

issue because the availableness of absolute provision becomes comparatively tough.

D. *Data Location and Relocation:*

High degree of information quality that offered by cloud computing. the placement of user knowledge doesn’t seem to be continuously acknowledged by them. they will additionally would like to specify a most popular location. Make sure the security of systems is the obligation should be taken through the cloud provider. The movement of facts from one location to a distinct is every other problem. Cloud supplier is deciding to the information is at first hold on at AN acceptable location.

III. Security 0f Data Storage

the safety in their information inside the Cloud is that the primary challenge. Once quality {of information of knowledge of information} is at high level then the risks and problems increase several folds particularly once data is transferred totally different} country with different regulative framework. Negative implications for information security are to be high levels {of information of knowledge of information} relocation and data protection still as handiness of knowledge although the most concern with guarantee to security of knowledge residing within the cloud is a way to guarantee security of knowledge that's at rest. Albeit cloud user is aware of the placement of knowledge and there's no quality of knowledge, there square measure queries about its security and confidentiality of it. little question the cloud computing space has become target thanks to its broad network access and adaptability. User store their information within the cloud and now not possess the domestically of knowledge within the Cloud ADP system. Our main goal during this planned work to confirm the information storage security within the cloud computing. The user continues to be needed in terms of a secure and secure setting for the non-public information.

IV. Assumed Work

RSA algorithmic rule become introduced in 1977 by West Chadic Rivest, Adi Shamir and Len Adleman. RSA is wide used for secure knowledge transmission. One in all the primary practical public key cryptosystems. during this projected work, we have a tendency to area unit mistreatment RSA algorithmic rule to cypher the information to produce security so solely the involved user will access it. at the same time as now not allowing unauthorized get right of entry to thereto via securing the information. Initial encrypting the cloud user knowledge then it's hold on within the cloud.

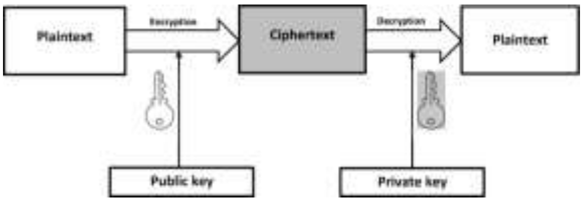

Fig 1: Public Key Cryptosystem

User placed the request for the information to the cloud provider and additionally the cloud provider alone access the documented the cloud user and delivered the information. A Block cipher is RSA， all through that every message is mapped to partner integer. RSA consists of keys are personal key and public key. In atmosphere of cloud, public secret's celebrated to all or any or any, but private secrets alone celebrated to the user administrative unit owns the information in originally. secret writing is completed by the Cloud service provider and additionally the secret writing is completed by the cloud user. Already the information is encrypted with the final public key then it's decrypted with the private key on my own.

RSA algorithmic rule consists of 3 steps:
1. Key Generation
2. Encryption
3. Decryption
secret writing and decoding used standard exponential that provided by RSA. 2 exponents are utilized by RSA are e and d. wherever e is public key and d is personal key then allow the obvious text is M and C is cipher textual content. Secret writing n may be a terribly sizable amount and created throughout the key generation method.

Key Generation
Key generation ought to be done before the information is encrypted. This approach is finished with the aid of among the cloud service supplier and cloud person.

Steps:

1. choose any 2 distinct prime numbers letter and r. For the needs of security, the integers letter and r ought to be hand-picked every which way and will be in same bit length.
2. Calculate n=q*r.
3. Calculate Euler’s Totient function,
$$\emptyset(n) = (q-1)*(r-1)$$
4. Select an integer e, such that 1<e<$\emptyset(n)$ and gcd (greatest common divisor) of e. $\emptyset(n)$is 1. Now e is obtained as public key exponent,
5. Now determine d as follows:

   d=e $^{-1}$(mod $\emptyset(n)$), where d is multiplicate inverse of e mod$\emptyset(n)$.
6. d is kept as Private key exponent.
   So that d*e=1 mod $\emptyset(n)$.
7. Then the general public key consists of modulus n and the general public exponent therefore, we get
   [e, n]
8. Then the personal key includes of modulus n and the personal exponent d， it needs to be kept secret therefore we get
   [d, n]

Encryption:

The technique of changing precise simple textual content into cipher text is called encryption.

Steps:

1) Cloud provider issuer must be transmitting the public key to the user who need to shop the facts with him/her.
2) Cloud man or woman statistics is now mapped to an integer through the use of an agreed upon reversible protocol known as padding scheme.
3) Facts is encrypted and the ensuing cipher text C is $C=m^e$ (mod n)
4) This cipher text is now saved in the cloud provider enterprise.

Decryption:

The technique of changing cipher text into simple text is referred to as decryption.

Steps:

1) The Cloud person requests the Cloud carrier company for the facts.
2) Cloud provider affirm the authenticity of the cloud man or woman and offers the encrypted information C.
3) The Cloud individual then decrypts the information by way of calculating,
   $m=C^d$ (mod n)
4) as quickly as m is passed off the cloud customer can get lower back the original facts thru reversing the padding scheme.

   its safety comes from the procedure trouble of factorization large numbers. To be relaxed, terribly massive numbers must be used for letter and r -one hundred decimal digits

V. EXPERIENTAL RESULT

A simple example work: Key generation

1. Create massive top numbers p and q to make the instance easy to comply with I'm going to use small numbers, however this isn't relaxed. To locate random primes, we start at a random variety and cross up ascending ordinary numbers till we find a high. permit recall:
   q=7 and r=11
2. Calculate n=q*r
   n=7*11
   =77
3. Calculate
   $$\emptyset(n) = (q-1)*(r-1)$$
   $$= 6*10$$
   $$= 60$$
4. choose a small variety, e is co-top to ∅n, means that the biggest number can precisely divide the both e and ∅n.
   gcd (e, $\emptyset(n)$)
   gcd (e,60)
   e=13
5. Find d,
   d=e $^{-1}$(mod $\emptyset(n)$)
   d*e mod $\emptyset(n)$ =1
   d*13mod 60
   d=37
6. Public key — Secret key

Public key	Secret key
n=77	n=77
e=13	d=37

Encryption:

1) the general public key (thirteen,77) is given by the cloud provider issuer to the person who wish to shop the facts.
2) Let us considered the user mapped information to an integer m = nine.
3) statistics is encrypted now through the cloud provider company via the usage of the public key that is shared with the aid of both the cloud provider and the consumer.
   $C=9^{13}$ mod 77
   =58
4) This encrypted statistics cipher text is now save by means of the cloud carrier company.

Decryption:

1. whilst the cloud person requests for the records cloud carrier issuer will authenticate the consumer and offers the encrypted information if simplest get admission to by means of the user is valid.
2. The cloud person then decrypts the records through calculating,
   $m=C^d$ (mod n)
   $=58^{37}$ mod 77
   =9
3. And that matches the plain text we put in at the initialing, so we worked these successfully.

CONCLUSION

Clouds providing on demand access to computing utilities. Installation and access their personal files at any system with web access with none applications. The RSA affords the excessive safety in excessive potential encryption. comprehensive solution of cloud computing that provides IT as a service. Wherever shared resources square measure provided on the premise of internet-based computing. The perform of the allocation of resources on demand for Associate in internet-based computing answer. wherever the cloud computing is thought to be on demand service and still a brand new and evolving paradigm. Once the corporate takes the choice to maneuver to the cloud then loses management over the information. Therefore， the amount of protection required to secure understanding is immediately proportional to the well worth of the information. Computing and cryptography square measure sure that depends for the safety of the cloud consequently， the quantity of protection required to cozy information is without delay proportional to the worth of the data. Despite the fact that some unauthorized cloud user gets the information accidently if he picks up the information conjointly, he can’t decipher it and find back the initial knowledge from it. Here when knowledge security is provided by victimization RSA rule.

REFERENCES

[1] https://www.researchgate.net/publication/271557328_Data_security_in_cloud_using_RSA.

[2] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.454.9950&rep=rep1&type=pdf .

[3] http://ijiset.com/vol6/v6s4/IJISET_V6_I4_09.pdf.

[4] https://www.ijarcce.com/upload/2016/august-16/IJARCCE%203.pdf

[5] https://www.semanticscholar.org/paper/Enhancing-Data-Security-in-Cloud-Computing-Using-Lenka-Nayak/08c02c78d94e771c3383a91b76b33212690873f2.

[6] https://www.researchgate.net/publication/343834275_CLOUD_COMPUTING

DOI: 10.5281/zenodo.6223508
ISBN: 978-93-5607-317-3 @2022 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam