International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

DATA DIVISION IN CLOUD FOR SECURED DATA STORAGE USING RSA ALGORITHM

B. Rex Cyril[1], DR.S. Britto Ramesh Kumar[2]

[1]Research Scholar and Assistant Professor, Department of Computer Science, St.Joseph's College(Autonomous), [2]Trichy, Tamilnadu, India[2]Asst.Professor, Department of Computer Science, St.joseph's College(Autonomous) Trichy, Tamilnadu, India

---

Abstract -*Cloud place for storing is an arm where facts is from far said (thing is true), managed, and backup. Cloud computing is group of resources and services offered through the net. Cloud services are handed over from facts middle's placed throughout the earth. Cloud computing helps its users by making ready machine-based resources via the net. However, working well knowledge for computers system of care for trade and strong encryption in the cloud is possible and ready (to be used) through a number of cloud answers. This paper aims at safe knowledge for computers place for storing in cloud. Here we separate the facts in cloud for safe place for storing using RSA algorithm. The user knowledge for computers is encrypted using RSA and separated into number times another gets in the way of and stored on different cloud computers. The division of knowledge for computers in the cloud general condition for safe knowledge for computers place for storing gets done safety as well as right not to be public to user facts and gives greater value to the doing a play by copying techniques.*

Keywords: Cloud Computing, Data Storage, Data security, Data Encryption, Data Decryption

1. INTRODUCTION

Cloud computing is the most demanded technologies used all over the earth. It provides all kind of services for the users. One of the most readily seen arm offered by cloud computing is cloud place for storing. Cloud place for storing is simply a limited stretch of time that says something about to on line space that you can use to store your facts. In more solid way, cloud place for storing is an arm design to be copied in which facts is said, managed and backed up from far and made ready to users over a network. In it undertakings, the cloud are nearby trends, i.e it is power to moves computing and knowledge for computers away from tabletop and able to be taken about PCs into greatly sized facts insides. Sixty two parts of a hundred of undertakings go to person in authority that in the middle of it makes the majority of cloud using up decisions.43 parts of a hundred of it teams are offering a self-helping great door-way for way in to cloud arms, with an addition of 41 parts of a hundred idea or getting greater, stronger, more complete a great door-way.

The statements of cloud computing on condition that by National Institute of quality examples and Technologist says that: Cloud computing is a design to be copied for making able to right, on request network way in to a shared card-player's money of configurable computing resources (e.g. networks 3, servers, place for storing applications and arms) that can be rapidly provisioned and given out with least business managers hard work or arm giver effect on one another. With the help of greatly sized scale undertaking the net grows rapidly around the earth, applications can now be handed over as services over the net. As an outcome this overall price is made lower, less.

From the view of facts safety, Cloud computing puts forward new questions safety being, saying violent behavior for many Reasons. firstly, old and wise cryptographic early persons for the knowledge for computers safety system of care for trade cannot be directly took up because user has no control over the facts under Cloud computing. As an outcome of that verification of right knowledge for computers place for storing in the cloud must be guided without clear and detailed knowledge of the complete work facts. Secondly, Cloud computing is not just a third group knowledge for computers store house. The knowledge for computers stored in the cloud may be frequently changed knowledge by the users, including insertion, thing taken out, modification, join and so on. Last but not least, the placing of cloud computing is powered by knowledge for computers middle's running in at the same time, made distribution and worked together.

Recently, the importance of making certain the far away, widely different facts true, good nature has been high-lighted by the different make observations works. These expert ways of art and so on, which can be useful to make certain the place for storing rightness cannot house all the safety being, saying violent behavior in cloud knowledge for computers place for storing, since they all are focusing on single computer scenario. In this paper we offer a working

well way to safe knowledge for computers place for storing in cloud. Here we separate the facts in cloud for safe place for storing using RSA algorithm.

2. RELATED WORK

The survey [2] guided by Salt march news in the third quarter of this year measured power being conscious of Business technology experts including their important questions in taking up Cloud, the drivers, how their organization's map to use Cloud, the different stages of Adoption, and the cloud flat structures, applications, persons for whom one does work, roads and systems and place for storing used. "While facts secretly and audit ability (24.5%) topped the list of first obstacles for the use of cloud.

Computing technologies, doing a play state of not being able to say before-hand (20.1%) appeared to be another key cause dampening Adoption levels". knowledge for computers get moved from one position to another narrow part (of road) (17.5%) and facts lock-in (14.3%) were next on the list of factors as stated by Respondents.

Cloud computing[4] provides the place for storing and supports for getting work done by others of knowledge for computers without having the nearby copy of facts or records. However an important hard question is to put a stop to not with authority adjustments. But, for this it has need of either facts copying or on-demand computation of a purpose, use (e.g. a number without thought of amount) over the complete outsourced facts.

In text record distribution [1], the text record is separated into the gets in the way of and goes away the text record F unnecessarily across a group of made distribution computers. Facts are stored in the encrypted form on the computers. All the forceful operations like thing put in, update, join and take out can be done on the facts gets in the way of. As in agreement the changes in text record, facts gets in the way of are separated and stored on the facts computers again. While getting back the facts, the facts gets in the way of separate records are merged and profit to the user. To check the rightness of the text record, question small things have been sending to the cloud place for storing system.

To make ready safety for cloud facts RSA Algorithm [3] is used, RSA is the deterministic encryption algorithm. It was undergone growth by Ron go back, aldi shamir, and Len adleman at Mit and first made public in 1978[rivert-shamir-adleman (RSA)]. In this design the level stretch of country teaching book and cipher teaching book are complete numbers, not parts between 0 and n-1 for some N. A of a certain sort size for N is 1024 bits.

RSA algorithm[5]; In this careful way some important safety services including key living-stage, encryption and decryption are on condition that in Cloud computing system. The main end, purpose is to safely store and manage facts that are not controlled by the owner of the facts. The facts are stored in cloud general condition Cloud safety here is not answer to by making ready a RSA algorithm.

3. PROBLEM STATEMENT

3.1 System Architecture:

In cloud knowledge for computers place for storing, a user stores his knowledge for computers through a cloud Service giver into a pot of cloud computers, which are running in an at the same time, worked together and made distribution way Fig (1). Net structure connection provides facilities to upload download and act the forceful operations on facts text record. Checking to make certain System lets the given authority user to get the way in to the cloud place for storing. User checking to make certain way is done before to the place for storing and acts to get back. It provides the facts right not to be public to the user. It also lets user to change his outline. Place for keeping records one making discovery in new country provides the selections to look for a text record and act forceful operations. With the solid mass operation, it provides different operations like bring to the current state join and take out on one computer. We can view the is in of the text record stored on the one computer. With the upload thing for which selection is made, user can upload the knowledge for computers text record from his system on the cloud computers. With the download (right of) selection between, it will list down all the users text record, and selected text record can be downloaded on users place. Here encryption and decryption is done using RSA algorithm

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

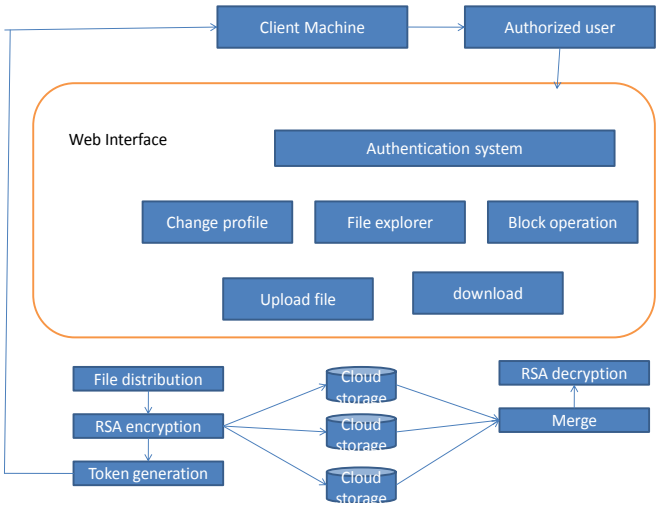

Fig-1: System Architecture for cloud storage

3.2 Design Goals:

Offered design is to make good at producing an effect facts safety design to be copied which supports for i)Data true, good nature to make certain the users facts is right and stored in cloud computer. ii) Have an effect on give position of the computer on which facts has been made an adjustment by not with authority user. iii) Support for the forceful facts like join, take out, insert, bring to the current state while making payment before work the same place for storing rightness.

4. DATA SECURITY

Cloud possesses the security problem in Data segregation, Data theft, unauthorized access, Uncleared Owner and responsibility of Data Protection, Data Loss conditions

Data security framework

Security[3] is the major concern to access the data in cloud. Security involves protecting data from being lost, destroyed or modified.

1) Protection of Data: Data can be protected from the outside user by creating the security keys such as private key.

2) Building Blocks: Mathematical and cryptographic principles server as the building blocks of the security.

3) Integrity of data: while uploading the data the user can verify the correctness of the integrity principles.

4) Accessing the Data: Due to the Encryption and Decryption techniques data can be accessed securely.

5) Authentication: Authentication allows only authorized user to access Data in cloud.

5. PROPOSED WORK

In our offered work, we are making separate the facts in cloud for safe place for storing using RSA algorithm. RSA algorithm [2] to encrypt the facts to make ready safety so that only the had a part in user can way in it. By getting the facts, we are not letting not with authority way in to it. User facts are encrypted first and then it is stored in the Cloud. When needed, user places a request for the facts for the Cloud giver; Cloud giver makes certain the user and gives the facts.

5.1 Data Division

F – The data file to be stored. We assume that ***F*** can be denoted as a matrix of *m* equal-sized data vectors, each consisting of *l* blocks. Data blocks are all well represented as elements in Galois Field GF (2p) for p = 8 or 16. File is split into fixed-size blocks which are stored on servers and all blocks are replicated and dispersed over distributed servers. We rely on this technique to disperse the data file F redundantly across a set of n = m+ k distributed servers. File data should be greater than or equal to the number of server on which it is going to store.

Algorithm 1: File Distribution Preparation
Step1. Check the file's data length greater than or equal to the number of server. If it is blank file or the data length is less, then prompt the message to the user.
Step 2. Generate the file matrix. The *Generate_Matrix (file)* function divides the file into equal data vector length.
Data vectors are created depending on the distribution of the file.

$$\text{datavector\_length} = \frac{\textit{total no.of bytes in file}}{\textit{no. of servers}}$$

If file_length mod n < > 0 then
datavector_length = datavector_length+1
This divides the file into n number of blocks. Vector1 contains the data bytes from 1 to *datavector_length* from the file. Vector 2 contains the data bytes from the location of *datavector_length* to (*2 * datavector_length*) and so on. Each vector represents the data block of matrix of Galois Field. Use the Vander monde matrix for the Matrix_Multiply () function. Construct *A* using Vander monde matrix defined over *GF (2w)*. For e.g. if we take 3x3 Vander monde matrix defined over *GF (24)*

$$A = \begin{bmatrix} 1^0 & 2^0 & 3^0 \\ 1^1 & 2^1 & 3^1 \\ 1^2 & 2^2 & 3^2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 5 \end{bmatrix}$$

Step 3. Perform *Matrix_multiply (vector, A)* operation on each data vector. Use g1, g2, g3…gm as data vector names.
sum = 0; count = 0;

For k ← 1 to File_length Do

For i ← 1 to datavector_length Do

sum = sum +vector[i] *A[count];

For all data vectors Do

If k = count Then Gm [i] ← sum;

End for

count = count + 1;

End For

End For

Step 4. Encryption is applied on each data vector and data vectors are disperse on the distributed servers. The data vector of a file is replicated on the cloud servers.

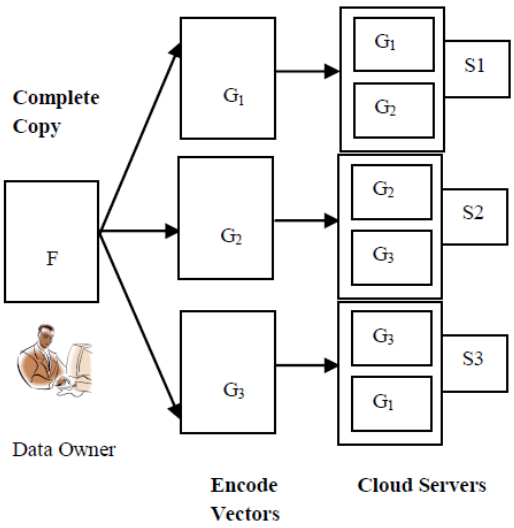

Fig-2: Distribution of File Stored on Cloud

5.2 Token Generation:

Before storing the knowledge for computers gives directions to be taken on cloud computers, user pre-computes the verification tokens [4]. These small things are used to check the true, good nature of knowledge for computers stored on cloud computers. Also these small things are used to give position of the cloud computer on which facts has been made an adjustment by the computer expert for pleasure. Before facts division and going away text record user produces small things on person facts gives directions to be taken. When user wants to check the rightness of the facts, he sends the text record thing taken to be the same to the cloud computers. User may send physical acts offer on one facts solid mass in addition. Upon letting into one's house question small thing, each cloud computer works out the things like money on the facts guide, and sends them to user. If the small things of users and worked out small things from cloud computers are matched, then the facts is right. If the small things are not matched, then an adjustment has been done in the facts by not with authority user. This shows cloud cut, make a division of is behaving badly.

Step1. Choose the parameter r for number of indices per verification and pseudorandom function *f*, pseudorandom Permutation function ϕ
Step2. Choose the parameters *t,* the number of tokens to be generated and *l* the length of the data vector.
Step3. Chose *α* as a vector to compute the tokens and V to store the tokens.
Step4. Read the file as byte array. Divide this byte array into parts. Each part contains byte and
represents it into polynomial. (for example dividing byte array in 3parts).

For j←1 to n Do

For i ← 1 to t Do α[i]

= *f*(i) sum= 0

For q ←1 to r do a←gj[ϕ(i)]

b ←Power (α[i], q)

sum = sum + a * b

End For

if j = 0 then V1[i] = V1[i] + sum

if j= 1 then V2[i] = V2[i] + sum

if j= 2 then V3[i] = V3[i] + sum

End For

End For

Vj ← Add V1, V2, V3

Step5. Store the token into Data storage

After token generation, the user has the choice of either keeping the pre-computed tokens locally or storing them in encrypted form on the cloud servers. In our case, the user stores them locally to obviate the need for encryption and lower the bandwidth overhead during dynamic data operation. Figure3 describes token pre-computation before dispersing the file to the cloud server.

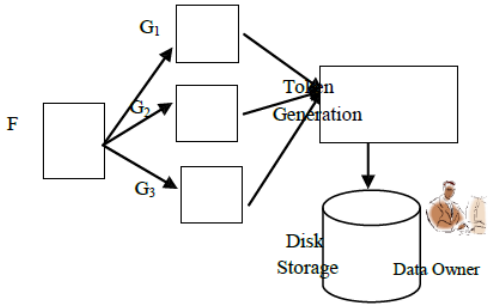

Fig-3: Token Pre-computation

5.3 Data Encryption and Decryption using RSA Algorithm:

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:
1. Key Generation

2. Encryption

3. Decryption

1. Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

The plain text is encrypted in blocks, with each block having a binary value less than some number n i.e., for block size i bits, 2i <n<2i+1 .

Input: None

Computations:

- Select two relatively prime numbers p and q.Where n=p*q and v-(p-1)*(q-1).

- Compute the integer d such that (d*e)%v=1.

- e is the integer.

Output: n, e and d

2. Encryption

Input: Integers n, e, M

-M is integer representation of the plain text. **Computation:** let C be the integer representation of the cipher text. C=(Me mod n)

Output: Encrypted text or cipher text C.

3. Decryption

Input : d, n, C

- C is the cipher text.

Computation:

- let D be the decrypted text such that D=(Cd Mod n)

Output: D is the decrypted message.

Public Key: {e, n}

Private Key: {d, n}

6. CONCLUSION

As we all know Cloud computing is an of government change apparatus that changing way to undertaking hardware and software design and effecting needs, requests. Because of cloud simpleness everyone is moving facts and application software to cloud facts insides. In this way, the amount of system of care for trade needed to safe knowledge for computers is directly in relation to the value of the facts. Security of the Cloud is dependent on law computing and science of keeping knowledge safe and secret. Only the made certain and given authority user can way in the facts, even if some not with authority user gets the knowledge for computers erroneously or purposely and if takes the facts in addition, user can not decrypt the facts and get back the first form knowledge for computers from it. Facts safety is on condition that by implementing RSA algorithm. In this way, in our offered work, we separate the facts in cloud for safe place for storing using RSA algorithm. The user knowledge for computers is encrypted using RSA and separated into number times another gets in the way of and stored on different cloud computers. The division of knowledge for computers in the cloud general condition for safe knowledge for computers place for storing gets done safety as well as right not to be public to user facts and gives greater value to the doing a play by copying techniques. Only the given authority user can way in the facts. Even if some undesired one going in (not with authority user) gets the knowledge for computers erroneously or purposely if he takes the facts in addition, he is not able to decrypt it and get back the first form knowledge for computers from it. For this reason forward, out, on (in time), facts safety is on condition that by implementing RSA algorithm.

REFERENCES

[1] Kalpana Batra, Ch. Sunitha, Sushil Kumar "An Effective Data Storage Security Scheme for Cloud Computing" International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2013

[2] Parsi Kalpana, Sudha Singaraju "Data Security in Cloud Computing using RSA Algorithm" International Journal of Research in Computer and Communication Technology IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[3] Ms. Soumya.N.S, Mrs. Prabha.R " Cloud Computing: Data Security Using RSA " IJLTEMAS, ISSN 2278 - 2540, Volume IV, Issue X, October 2015

[4] Bharti Dhote, A.M. Kanthe "Secure Approach for Data in Cloud Computing" International Journal of Computer Applications (0975 – 8887) Volume 64– No.22, February 2013

[5] S. Manjula, M. Indra, R. Swathiya "Division of data in cloud environment for secure data storage" IEEE ISBN: 978-1-4673-8438-4, 31 October 2016

[6] Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.

[7] Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.

[8] Institute of Electrical and Electronics Engineers, Standard Specifications for Public Key Cryptography -Amendment 1: Additional Techniques, 2004.

[9] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22(1976), 644–654.

[10] V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila, Journal of Computer Science and Engineering, Volum 2, Issue 2, August

BIOGRAPHIES

Prof. B. Rex Cyril is working as Assistant Professor and pursuing doctor of philosophy in Department of Computer Science, St. Joseph's College,(Autonomous),Tiruchirappalli, Tamil Nadu, India. He received his M.Phil degree from Prist University. He received his MSc degree from St. Joseph's College, Tiruchirappalli. His area of interest is Cloud Security Services.

Dr. S.Britto Ramesh Kumar is working as Assistant Professor in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India He has published many research articles in the National/International conferences and journals. His research interests include Cloud Computing, Data Mining, Web Web Mining, and Mobile Networks.