Open access Journal International Journal of Emerging Trends in Science and Technology
Impact Factor: 2.838 DOI: http://dx.doi.org/10.18535/ijetst/v3i05.02

Data Confidentiality and Security in Cloud Computing Using KIST Algorithm

Authors
Adesh V. Bhabad[1], Vasant N. Dhatrak[2], Jeevan R. Heda[3], Gaurav P. Shahane[4], Bajirao S. Shirole[5]
[1,2,3,4]Student, Department of Computer Engineering, Sanghavi College of Engg., Nashik
[5]Asst. Prof, Department of Computer Engineering, Sanghavi College of Engg.,Nashik
Email: *bhabadadesh@gmail.com[1],vasantdhatrak06@gmail.com[2],jeevanheda@gmail.com[3] gauravshahane786@gmail.com[4],baji_shirole@yahoo.com[5]*

ABSTRACT

Now days quickly expanded utilization of cloud computing in the numerous association and IT commercial industries and furnishes latest software solution with cost effective. So the cloud computing give us numerous of advantages with minimum cost and of information openness through Internet. The guaranteeing security risk of the cloud computing is the part in the distributed computing environment, the advancing, the evolving quintessence is cloud computing, that is gainful in cost effective parts, such as, ability inflexible computing, down the time period to advertise and in adequate computing power. By utilizing the complete capacity of cloud computing, information are transmitted, prepared and put away on the outside cloud administration suppliers. The truth of the matter is that, the proprietor of the information is feeling to a great degree unconfident to find their information external to their own particular control. Security and Secrecy of information put away in the cloud are key setbacks in the range of of Cloud computing. Security and Secrecy are the key problem for cloud storage. This paper proposes a KIST encryption calculation to focus on the security and Secrecy problem in cloud storage furthermore packed figure content information to ensure the information put away in the cloud.

***Keywords**-Cloud storage, Security, Confidentiality, Cryptography, KIST Algorithm, Encryption, Decryption, Fraud Detection.*

1. INTRODUCTION

Cloud computing is the total term for a gathering of IT propels which in collaboration are changing the scene of how IT organizations are offered, gotten to in addition, paid for. A rate of the supporting advances have as of presently been available for an extended period of time, be that as it may it is the blend of a couple advances which enables a whole better approach for using IT. Cloud computing is a model for enabling profitable, on interest framework access to a normal pool of configurable computing resource (e.g., frameworks, servers, administration, applications, organization). In this paper proposes a KIST calculation with an encryption method for information security and secrecy in the cloud capacity storage. In the framework client can store the information with the assistance of encryption technique on given cloud and gives alert message to approved client in the event of information alteration.

2. CHARACTRISTICE OF CLOUD

Rapid elasticity

The cloud computing resources can rapidly match with the increasing cloud capabilities if the demand increases.

Measured service

It enables the measuring of used resources similar to the utility computing.

Resource pooling

This resource pool helps in enabling the use of physical and virtual resources by multiple users.

Broad network access

Cloud services are available on any kind of network.

On Demand Self-service

Cloud Computing resources can be obtained and disposed of by the consumer without human intervention among cloud service providers.

3. CLOUD SERVICE MODELS

Software-as-a-Service (SaaS)

SaaS is one of the oldest and nature domains of cloud computing. SAAS is nothing but a software distribution model, which is available to customers over a network such as server or internet. SaaS is an interface between cloud applications and customers to offer them on demand network.

Platform-as-a-Service (PaaS)

Platform as a service provides high-level environment to design, build, test, deploy and update online cloud applications. PaaS is a paradigm which mainly deals for delivering operating systems and other services over the internet. Answers for creating and also conveying applications over web such as operating system and virtualized servers.

Infrastructure-as-a-Service (IaaS)

Infrastructure as a service is equipment that used to support hardware, software, storage, servers and mainly used for delivering software application environments. It totally depends on pricing model. IaaS companies provide off line server, stockpiling and systems administration equipment as permanent basis and can be access over the Internet. So it becomes easier to get access to run theirapplications on this hardware anytime without wasting office space.

4. CLOUD DEPLOYMENT MODELS

Public Cloud

An open cloud can be gotten to by any supporter with a web association and access to the cloud space.

Private Cloud

A private cloud is set up for a particular gathering or association and limits access to only that gathering.

Community Cloud

A group cloud is shared among two or more associations that have comparable cloud necessities.

Hybrid Cloud

A half breed cloud is basically a blend of no less than two mists, where the mists included are a blend of open, private, or group.

5. SYSTEM TASK DIMENSION ABOUT CONFIDENTIALITY

Transfer

Disclosure of sensitive data during transfer from one party to the other is a concern that has been addressed quite extensively with the use of encryption.

Storage

When the data is stored outside the direct control, the data owner can exercise separation of duties, by encrypting the data before storing it externally, while keeping the means of decryption in the owner’s control.

Processing

Processingrefers to any use or transformation of data. When processing needs to take place within the cloud, data cannot be protected by the same means as data at rest and data in transit (e.g. encryption).

6. CHARACTRISTICS

A. An asynchronous key sequence is used which depends on a beginning key and plain content.
B. A Splay tree is used so the substitution is dynamic (progressive).
C. The encryption is brisk and requires small space.
D. Cipher text is compress in most cases.
E. The block size of the plain content and key size is flexible.
F. It is valuable for message integrity.

7. PROPOSED SYSTEM

In proposed system illuminates security challenges for information in the cloud and gives a reliable and simple approach to secure information with the assistance of encryption innovation. In this system, the client will get a proof of integrity of the information that he or she wishes to store in the cloud with absolute minimum expenses and endeavors. Encryption procedure is performed with the assistance of KIST algorithm which will encode the plain information into cipher information and that cipher information is transferred on cloud. At the season of recovery the cipher information is again recovered into plain information which is put away on system. This diminishes the odds of getting discloser inside. In this way, a relationship is built up to cooperation model in the middle of administrator and client gave to the clients furthermore gives redesigning of given information, recovered ready messages from cloud.

Proposed modules describes are as follows.

1. ERP (Enterprise Resource Planning)

The user may be an ERP system or business organizations who use the cloud for data storage.

2. OTP (One Time Password)

OTP is required to authenticate valid user. When OTP is required, we have to send the Message from system only. The OTP will come to Email ID & enter that OTP in the system, then upload data on the cloud.

3. Encryption

In Encryption the plain text data can be converted into cipher text. it is unreadable format.The sytem will acknowledge typical information, then it will encode or scramble the given information, after encryption it will give scrambled information as figure content.

4. Decryption

In Decryption the Cipher text can be converted into plain text it is readable format. Decryption is exactly repeating the procedure as same as encryption.

5. SOAP Protocol

SOAP originally defined as “Simple Object Access Protocol” is a protocol that used in computer networks for trading organized data in the usage of web administrations

6. Searching

In Searching if the user wants to access particular information then searching option can be used for searching particular data.

7. Fraud Detection

In Fraud Detection the System will give alerts to users whenever some other person tries to attack data or unauthorized access to data in cloud storage and alert Message Come On authorized User Mail account.

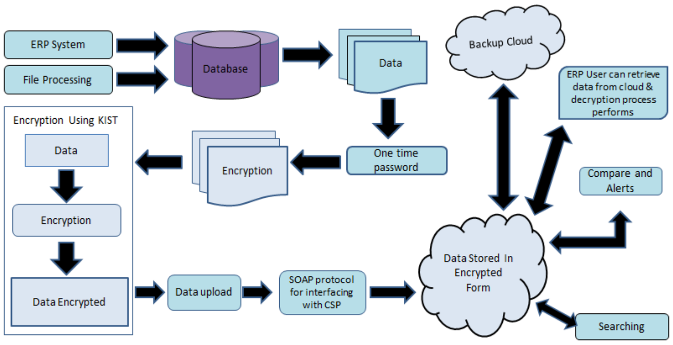

Fig. Proposed System Architecture

8. ALGORITHM

1. Key generation.
2. Encryption Algorithm.
3. Key injection Algorithm.

For effortlessness, The accompanying is an illustration of our encryption. In any case, it is clear to give the general algorithm from our case. Our encryption depends on bytes that empowers it to be executed effortlessly a CPU of 8 bit. We will utilize a binary tree of 256 leaves for the 256 unique bytes. So we require 255 internal hubs in the tree. We utilize three arrays left, right, up over to store the hubs data. Two arrays are of length 255 which records the left and right kids of internal hubs. Other arrays is of length 511 which records the parents of hubs. In this tree, the internal hubs are named 0, 1, 2... 254 and the leaves are named 255, 256... 510. So the file of arrays are the names of the hubs. In the underlying stage, the tree is a finished binary tree. So the estimations of these arrays are instated as takes after: So the values of these arrays are initialized as follows:

left[j] = 2 ∗ j + 1; for j = 0,... , 254.

right[j] = 2 ∗ j + 2; for j = 0,... , 254.

up[j] = (j − 1)/2; for j = 1,... , 510, and up[0] is some special symbol.

- Key injection algorithm

The key injection intended to utilize a key to move about internal hubs. Rather than that, the algorithm is utilized to pack the cipher content. Some tests are done which demonstrates that the arbitrary algorithm may results in failure of compression property. Indeed, in numerous tests, the cipher content is still bigger than the plain content. To take care of that issue just move the inward hubs which are higher than layer O, where O is some parameter. While more recurrent got to bytes are ordinarily at higher layers, this system will remain some compression of the cipher content. The compression of cipher content means little data respects the plain text about some time recently. Be that as it may, expect the estimation of O is high to kill the compression property of the cipher content. After delivering a key, the algorithm will check the layer in light of inward hub. In the event that an inward hub is below layer O, then leave that key. By this strategy, a portion of the keys will be repetitive in irregular. Hence the injection is in vulnerability, which will raise the security of the specific algorithm. The parameter O is utilized as a part of the following algorithm.

In this methodology, switch over the connections between two hubs. So the infusion is cleverer than the splay. The leaving or removing methodology gives a dynamic length of intervals and it is more creative than the run-length encoding concentrated on in .

The algorithm of injection function injection (byte j, integer O) is as follows. In our algorithms, a byte is expressed as an integer between 0 and 255.

Algorithm: Injection (j, O)

Comment j is a byte from input.

```
$k \leftarrow j$
$if\,(j = 0)$
$then\ quit$
$t \leftarrow 1$
$O \leftarrow o$
$while\ (up[k] \neq 0)$
$k \leftarrow up[k], t \leftarrow t + 1$
```

```
                $if\ (t < O)$
         $if\ (k = right[0]$
then     $then\ u \leftarrow left[0]$
         $exchange\ links\ of\ j\ and\ u\ (swap\ up[j] and\ up[u])$
                $else\ quit$
```

Beginning of the encryption first injection function will be called. Same time 16 byte should be injected in the tree then for the encryption of plain content of every byte injection function will be called note that the block of plain content is byte for each block injected a byte a key. Since complete binary tree is nothing but initial tree. For 16 byte injection it we set O> = 7 for the negates of the key in starting. We use threshold O then encryption function some bytes or the keys negate randomly.

- Encryption algorithm

The encryption algorithm incorporates the splay tree algorithm and key infusion algorithm. At first characterize splay function. The splay function splay (byte j) calculation is seen below.

Algorithm: SPLAY (j)

Comment j is a byte from input.

```
$j \leftarrow j + 255$
$k \leftarrow up[j]$
$while (k \neq 0\ and\ up[k] \neq 0)$
    $t \leftarrow up[k]$
    $if\ (k = left[t])$
    $then\ u \leftarrow right[t]$
    $else\ u \leftarrow left[t]$
    $excahnge\ links\ of\ j\ and\ u$
    $j \leftarrow up[j]$
    $k \leftarrow up[j]$
```

Encoding is carried on byte by byte. As encoding is made by consequent way from a leaf to the foundation of the tree, the code bits are delivered in the opposite request from the in which they should be transmitted. Therefore a nearby stack is used as an incidentally stockpiling of the bits. The encode capacity encode (byte j) calculation is seen below.

Algorithm: ENCODE (j)

Comment j is a byte from input

```
$k \leftarrow j$
$j \leftarrow j + 255$
$while (j \neq 0)$
    $if\ (j = left[up[j]])$
    $then\ push\ bit\ 0\ to\ stack$
    $else\ push\ bit\ 1\ to\ stack$
    $j \leftarrow up[j]$
$\boldsymbol{while} (stack\ is\ not\ empty)\ pop\ a\ bit\ and\ output\ it$
$Splay(k)$
```

The encode function is convert into the byte after access node will be splayed.

For encryption, key generation algorithm generates key sequence is (L1,L2,... ,Lj,...), where 0 ≤ Lj ≤ 255 for each j. The start key is L = (L1,L2,... ,L16)The encryption function algorithm is as follows. Suppose the plain text are bytes

Q = (q1,q2,... ,qn).

Algorithm: ENCRYPTION (Q,L)

Comment: Q is plain text and L is key sequence

```
$for\ j = 1\ to\ 16$
$do\ injection\ (Lj, O)$
$key\ \leftarrow 17$
$for\ k = 1\ to\ n$
do  $encode(Qk)$
    $injection\ (L\ key, O)$
    $key\ \leftarrow key + 1$
```

- **Decryption algorithm**

In decryption algorithm, the same O parameter is utilized as that in encryption calculation. If the Cipher text is a bit string D = (d1, d2. . . dt), the translate is go on a tiny bit at a time alongside the way beginning the root toward a leaf. A bit will be remove from the bit string later than it is gone before. The yield of the capacity is a byte. The algorithm of translate capacity unravel (bit string D) is below.

Algorithm: DECODE(D)

Comment: D is a bit string from input

```
$node \leftarrow 0$
$d \leftarrow frist\ bit\ of\ D$
$while(node \leq 254)$
    $if\ (d = 0)$
    $then\ node \leftarrow left[node]$
    $else\ node \leftarrow right[node]$
    $D = D \backslash \{d\}$
    $d \leftarrow frist\ bit\ of\ D$
$Output\ (node - 255)$
$Splay\ (node - 255)$
```

The calculation of decoding is as per the following. Assume the figure content is a bit string D and key grouping is produced by L. The calculation first injects 16 keys as the encryption. At that point the decode function is called. The key decoding function is every time called in injection function.

Algorithm: DECRYPTION (D, L)

Comment: D is a bit string from and L is key sequence

```
$for\ j = 1\ to\ 16$
$do\ injection(Lj, O)$
$Key \leftarrow 17$
$k \leftarrow 0$
$while(D \neq \emptyset)$
    $decode(D)$
    $k \leftarrow k + 1$
    $injection(Lkey, O)$
    $Key \leftarrow Key + 1$
```

- **Key generation algorithm**

In this algorithm the key succession is created from beginning key and plain content. we assume the symmetric key we utilized is 16 bytes. It is anything but difficult to utilize distinctive lengths of keys in our calculation. We will utilize a "cyclic" array key with length 16 (or the length of the key). Here cyclic implies that key[k] = key[k − 16] for k ≥ 16. These keys are put away in array key. Next, when a byte is scrambled, its guardian is Xored to the present key and after that utilized for infusion.

The key era calculation is as per the following.

Algorithm: Key Generation (Q,L)

Comment: Q is plain text and L is initial key

```
$for\ j = 1\ to\ 16$
$do\ key(j) \leftarrow Kj$
$d \leftarrow 17$
$for\ k = 1\ to\ n$
$do$
    $key\ (d) = key(d) \oplus up[Qk + 255]$
    $output\ (key(d))$
    $d \leftarrow d + 1$
```

The j^{th} key is delivered from the underlying key and Qk, where Qk enclosed with first k bytes of plain content. Watch that because of the splay, the guardian of the Qk is not set and it depends on earlier plain content and the underlying key. As single internal hub possibly contains two leaves called as kids, the change in key is not anticipated by an individual plaintext byte.

- **CONCLUSIONS**

The system is intended for securing the database of ERP what's more, other delicate information on cloud with the assistance of encryption algorithm and SAOP convention APIs design. It has turned out to be anything but difficult to scramble and additionally transfer information all the while on cloud on a single tick just that is booking. The information which are noticeable to the client on CSP is in Encoded structure. So here the programmer couldn't get it what precisely the data is or which record it is. On covering the information, the system will give unique information and as well as CSV document is created implies an entire record of database is seen as comma separated values. Log record describes the signed in points of interest of, client or some other individual who is attempting to get to the record. Look at catch which gives the ready sending message (Email) from the Email Server on Email Id. It depicts which information has been updated by programmers. However, the best part is just information which is invisible to programmer on the cloud is redesigned, the first information is most certainly not redesigned. So when client will get a ready client can once more transfer information on cloud and the first information is secure and shielded from programmer.

ACKNOWLEDGEMENT

We are thankful to IJETST for giving us opportunity to present the paper in their journal. We are also thankful to the Prof. Puspendu Biswas. (HOD of Comp. Engg. Dept.) for proper guidance and valuable suggestions. We are also greatly thankful Prof.Akshay Jain to other faculty members for giving us an opportunity to learn and do this paper. If not for the above mentioned people, our paper would never have been completed in such a successfully manner. We once again extend our sincere thanks to all of them.

REFERENCES

1. A. Mercy Gnana Rani, Dr. A. Marimuthu , “KeyInsertion and Splay Tree Encryption Algorithm forSecure DataOutsourcing in Cloud ” ,in Proc. Of IEEEComputing and Communication Technologies(WCCCT), 2014 World Congress, ISBN: 978-1 -4799-2876-7.
2. R. Wei and Z. Zeng, “KIST: A new encryptionalgorithm based on splay”, IACR Cryptology ePrintArchive, 2010s
3. Abhinandan P Shirahatti, P S Khanagoudar, “Preserving Integrity of Data and Public Auditing for Data Storage Security in Cloud Computing”, in IMACST of NCACC-12 and NCETCT-2012, VOLUME 3 NUMBER 3 JUNE 2012, pages:161 -171.
4. Li, H.; Yang, Y.; Luan, T.; Liang, X.; Zhou, L.; Shen,X., “Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over EncryptedCloud Data” ,in Proc. Of IEEE Dependable and SecureComputing, IEEE Transactions on (Volume:PP ,Issue: 99), ISSN : 1545-5971 , DOI:10.1109/TDSC.2015.2406704 ,Date of Publication :24 February 2015.
5. Ning Cao, Cong Wang, Ming Li, Kui Ren, andWenjing Lou. “Privacy-Preserving Multi-keywordRanked Search over Encrypted Cloud Data”.
6. Mohit Marwaha, Rajeev Bedi “Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing” in IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 ISSN (Print): 1694-0784, ISSN (Online): 1694-0814.
7. Rashmi Nigoti, Manoj Jhuria, Dr.Shailendra Singh, “A Survey of Cryptographic Algorithms for Cloud Computing” in IJETCAS ISSN (print):2279-0047, ISSN (online) :2279-0055.
8. Neha Tirthani, Ganesan R. “Data Security in CloudArchitecture Based on DiffieHellman and EllipticalCurve Cryptography.”
9. Dr. L. Arockiam, S. Monikandan “Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm” in IJARCCE ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021.
10. Dr. Chander Kant, Yogesh Sharma “Enhanced Security Architecture for Cloud Data Security” in IJARCSSE Volume 3, Issue 5, May 2013 ISSN: 2277 128X.
11. Shirole Bajirao Subhash, Dr Sanjay Thakur. “Data Confidentiality in Cloud Computing with Blowfish Algorithm” in IJETST- Volume 01, Issue 01, Pages01 - 06, March 2014. ISSN: 2348-9480.