Migration Algorithm for Data Security in Cloud Computing

Dhrumil Parikh[1] M. S. Deora[2]

[1,2] Department of Computer Engineering

[1, 2] Gujarat Technological University, Gandhinagar, Gujarat, India.

Abstract— Today's IT infrastructure is converted their all infrastructure in to the cloud based means use on infrastructure through internet resources. And cloud computing is the paradigm which is used in to major to transform infrastructure of company in to use as internet recourse. Still internet is comes then in that cloud data migration or to say transferring the data in to the cloud and also between the two cloud is major reason to apply for the security in data migration and also in data transferring in or off cloud is challengeable in this world. This paper proposed the various cloud computing algorithm which is implemented in to the cloud and also include their issues. Paper also proposed the data migration and also their security approach. Paper proposed the randomized key based approach for data security in cloud computing.

Key words: Randomized Key, Cloud Computing, Data Security, Data Migration, Watermarking, and PRNG.

I. INTRODUCTION

Cloud computing is the emerging field in the modern era. Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. It conveys everything as a service over the internet based on user demand, for instance operating system, network hardware, storage, resources, and software. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed Encryption. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms.

II. LITERATURE REVIEW

There are many security issues which are include in to the cloud computing. Still we need data security. For that different cryptographic algorithm is adoptable in cloud computing paradigm. This algorithm is useful to protect against the unauthorized access data, modification of the data, and also protect against the denial of services attacks. The cryptography provides security in three major manners in cloud is confidentiality, Integrity and Availibity. Cryptography help to the cloud as much security is in that the first security provide by cryptography in to the cloud for the secure storage of the data. Data Security, Backups, Network Traffic, File System, Security of host this all can be solved by the Cryptography. Many algorithms are implemented in to the cloud like in asymmetric based algorithm there are IKE, RSA, Diffie Hellmen key exchange algorithm and RC6 are implemented and in symmetric base algorithm there are DES, Triple DES and also AES algorithms implemented in cloud. It is very important to deliver data on data centers migration efficiently done cost efficiently faced with demands from remote office backup, Outsourcing, and data center moves on cloud computing. There is large number of database in cloud; various methods are there in cloud to divided data migration tasks in the following category: Data Schema migration, Data Migration, Database stored program migration, Application migration, and database administration secure migration. Before migration of the data we need to also one more approach is risk analysis of data. That is done through two methods: Qualitative and Quantative analysis methods of risk.

There are some factors that affect the data migration process in cloud that includes the (I) Commercial relation exists between cloud (II) Transmission of mass data (III) transmission of working done through concurrently. There are various challenges to migrate data in to or off threw cloud is data integrity, data security, portability, data privacy, data accuracy. The one of the best methodology is randomization based cryptography in cloud computing for data secure migration across clouds. Also providing the security in cryptography using the watermarking techniques is also useful in the cloud computing data security.

III. RELATED ISSUES

From Literature survey many security issues are overcome from cloud computing. These all issues are mentioned here as in following manner: Cloud Governance, Cloud Alliances like work according to the cloud laws and important compliances in now a day are storage and migrating data across cloud. There are many attacks possible in data theft like as a malicious insider and session hijacking attacks are possible. Cloud API Security also major issues in cloud

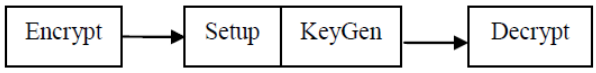
computing. During the migration process in cloud there also many security issues are come like as migrating data over the network, require to migrate data in between two cloud service provider is also so much issues, need more strong encryption in data transfer security and also need security in more from Master private key and shared Key. There is also one of solution in randomization based approach where also need to secure some issues that are: need to cipher text size more than the plaintext every time and also open to see the met In the middle attack for attacker can easily identify the random algorithm and broken it. So we need more security in that randomized key based approach. So basically key management is required for this all issues.

IV. PROPOSED METHODOLOGY

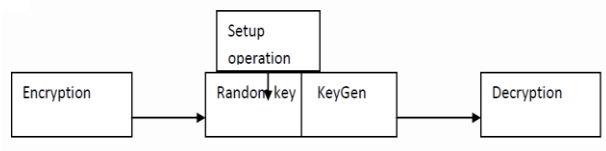
The cloud computing data security have already many solutions are there in which the various encryption based techniques are developed to secure the cloud computing data. In that Identity based encryption and Predicted Based encryption is new technique in cloud to secure in data migration process for cloud.

PBE scheme supports four operations allowing for encryption, decryption and key generation. The precise value for encryption and decryption keys is dependent upon both the construction of the scheme and placement of predicates. A general PBE scheme consists of the four operations:

1) *Setup*: initializes the crypto-scheme and generates a master secret key MSK, used to generate decryption keys, and a set of public parameters MPK. (MSK, MPK):=Setup ()
2) *KeyGen*: generates a decryption key Dec (entity) based upon the master secret key and some entity supplied input. Dec (entity):=KeyGen (MSK, input).
3) *Encrypt*: encrypts a plain-text message M using the public parameters and supplied encryption key for an entity. CT: = Encrypt (M, MPK, Enc (entity)).
4) *Decrypt*: decrypts a cipher-text if and only if the attributes held by the entity can satisfy the access policy. M: = Decrypt (CT, MPK, Dec (entity)).



This is the simplest solution to secure data or data migration in cloud computing. But new approach is comes to as a Randomized key based security in cloud computing is very important. So in that scheme the following is methodology is given:



In this approach randomized key is used in following manner:

Initially start with plaintext P-> Number of cipher text c1, c2, c3…Cn.

And after that randomly create N Cipher text and Map Cipher text any of them with the original plaintext since one who decrypts the text has no knowledge about which are has been picked.

Here the shared key (Public key) is reused but random key is used only for encryption of data. Through this data can be more secure, reliable to outsider to not know what key use for encryption. Still there are many problems occurs in the security related so we go for further research in the cryptography in enhancement for random based cryptography in cloud computing using watermarking technique.

V. IMPLIMENTATION

We have to use the following proposed diagram for securing our migration data. The Above model shows the how the algorithm working on data transferring process in to cloud or from one cloud to another cloud. The algorithms have also capacity to transfer large amount of the data.

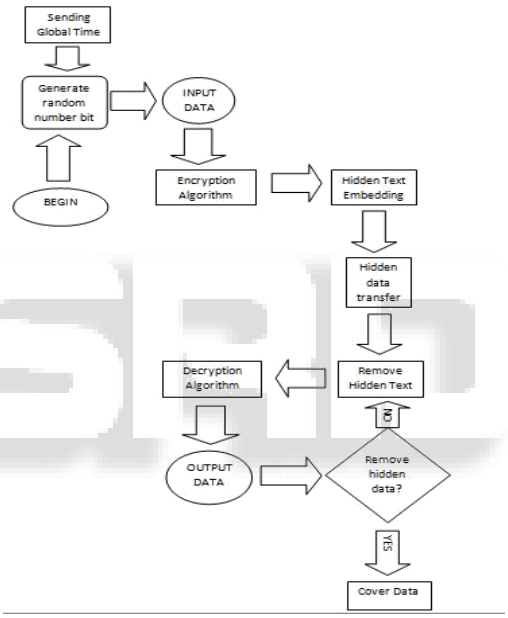


Fig. 1: Key Management

The Steps of the algorithm is given as below:

1) In this step sender get the global time message for sending the data from receivers end. The Sender generate the secret key and then this secret key is generated the random number of bits after the global time message comes.
2) After that the data is encrypted by using the encryption algorithm. This encryption process is done through the blocks of the data adding global timing on the block.
3) Then combined whole encrypted data then using watermarking text based approach for the hidden text in to the encrypted data.
4) After that the data transfer from receiver's end.
5) At receiver end where remove first the hidden text based watermarking and after that doing the decryption of the blocks of the data based on the global time put on the block.
6) Then finally combined all the blocks of the data the original data is received at the receiver's end.

7) Here we use the public key cryptography algorithm in which the Sender generate the two keys in which the Public key and Private Key.
8) Then after that the put the public key in to the watermarking pool which makes an attacker or hacker hard to predict the public key.

For Solution we have try to implement more in Key management problems in that we create the cloud based server for managing the keys of users as well as it also be manage the servers to generate the randomized based key generation where we have to use RSA key generation algorithm.

Flow chart for key management in our algorithm is given as below:

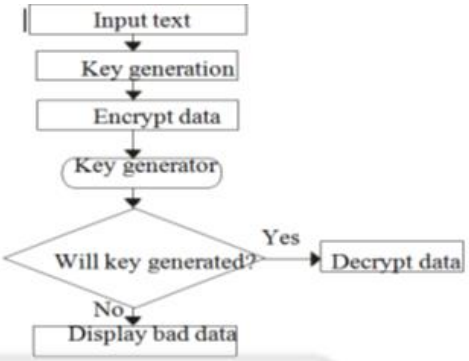


Fig. 2: Execution flow of the entire process

Steps for Proposed algorithm:

1) Step 1: Select two prime numbers.
2) Step 2: Calculate n = p*q.
3) Step 3: Calculate f(n) = (p-1)(q-1)
4) Step 4: Select e such that e is relatively prime to f (n) and less than f (n).
5) Step 5: Determine d such that de congruent modulo 1 (mod f (n)) and d<f (n).
6) Step 6: generate randomized based Public key = {e, n}, Private key = {d, n}
7) Step 7: Generate the text based watermarking
8) Step 8: Cipher text c = message e mod n
9) Step 9: extract watermarking
10) Step 10: Plain text p = cipher text d mod n.

VI. CONCLUSION

The cloud computing is emerging technology in recent industry in information technology. Many IT infrastructure transfer their infrastructure in to the cloud and that is why the cloud computing is very important factor to communication between two infrastructure. For that the transfer data done through using the cloud. But recent years many cybercrimes are increase so we have to much require to security over the internet in cloud and also between clouds where transfer the data migration process. Many papers are published on data security in cloud and also in data migration process over the various clouds. But the recent survey of above all the paper I conclude that the cryptography is very useful in to the data migration and also in data security in the cloud computing. So for the reading above all cryptographic paper in cloud there are many cryptography algorithm is already implemented in to the cloud. Still there require the strong cryptographic techniques. And finally the recent paper on randomized key based cryptography for the data migration process provides the solution based on the data migration and data security. But still there is some limitation in time delay, Easily detectable random key by cryptanalysis and so for I proposed the basic solution in enhancement of text based watermarking techniques using PRNG algorithm for cryptography in cloud computing data security and data migration process across the clouds.

VII. FUTURE WORK

In Future we have try to implement more our proposed system over the cloud using the eucalyptus enterprise cloud and we then check the performance of the our algorithm based to send simple file migration over the cloud and check that migration process based upon security and time factors include.

REFERENCES

[1] "Cloud Computing and Security –A Natural Match", published by Trusted computing group in April 2010.
[2] "HP Secures data migration in the cloud"- whitepaper published by Lisa Yarbrough, HP in June 2013.
[3] "A Survey of Cryptographic Algorithms for Cloud Computing"- Published By Rashmi Nigoti1, Manoj Jhuria2 Dr. Shailendra Singh3 Member IEEE Computer Engineering & Applications National Institute of Technical Teachers Training and Research Bhopal Madhya Pradesh, India in May 2013.
[4] "Creation on secure cloud environment using RC6 algorithm"- Narendra Chandel, M. Tech Student, Dept. of Information Tech., Technocats Inst. of Tech., Bhopal,narendrachn@gmail.com Sanjay Gupta, Neetesh Gupta, Amit Sinhal Dept. of Information Tech., Technocats Inst. of technology, Bhopal. Published IEEE in 2013
[5] "Data Migration across the Clouds" – Prashant Pant and Sanjeev Thakur published in May 2013.
[6] "Security approach for data migration in cloud computing" – Virendra Singh Kushwah and Aradhana Saxena published in May 2013.
[7] "Improving security for data migration in cloud computing using randomized encryption technique" – Rashmi Rao and Pawan Prakash published in June 2013.
[8] "Design and Implementation of Text based Watermarking combined with Pseudo-Random Number Generator (PRNG) for Cryptography Application"- by Chee Hon Lew and Chaw Seng Woo Faculty of Computer Science and Information Technology University of Malaya, Malaysia published in 2012.
[9] "Strengthening Private Cloud Security using Hierarchical Key-based Cryptography for Enhanced Manageability Facets"- by Amit Joshi and* D. K. Sharma Pacific Institute of Engineering, Pacific University, Jaipur Rajasthan in March 2013.
[10] "Randomized Approach for Cryptography" - published by Amit joshi and Bhavesh joshi for enhanced cryptographic solution in cloud at advent institute of Management studies Jaipur Rajasthan in 2013.

[11] Jiezhao Peng, Qi Wu, "Research and Implementation of RSA Algorithm in Java", International Conference on Management of e-Commerce and e-Government, published in IEEE 2009.
[12] "http://en.kioskea.net/contents/crypto/cleprivee.php3" dated 15 March 2011.
[13] Bellare, Mihir; Rogaway, Phillip, "Introduction". "Introduction for modern Cryptography." (21 September 2005).
[14] "http://en.wikipedia.org/wiki/Eucalyptus_ (computing) #Eucalyptus_Software_architecture" accessed on 12 June 2012.
[15] Joshi. An "A Global Time Based Approach towards Communication", International Journal for Electro Computational World knowledge Interface 1(1): 44 – 48, ISSN Number: 2249 - 541X (Print), 2249 – 5428 (Online) published in. (September 2011).

