International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

A Study of Securing Cloud Data Using Encryption Algorithms

T. A. Mohanaprakash[1], A. Irudayapaulraj Vinod[2], S. Raja[3], Ari Pavan Kalyan[4], C. B. Babu[5], Golla Vivek[6]

Associate Professor, Department of CSE, Panimalar Institute of Technology, Chennai, TamilNadu, India[1]

Assistant Professor, Department of CSE, Panimalar Institute of Technology, Chennai, TamilNadu, India[2]

Student , Department of CSE, Panimalar Institute of Technology, Chennai, TamilNadu, India[3,4,5]

ABSTRACT

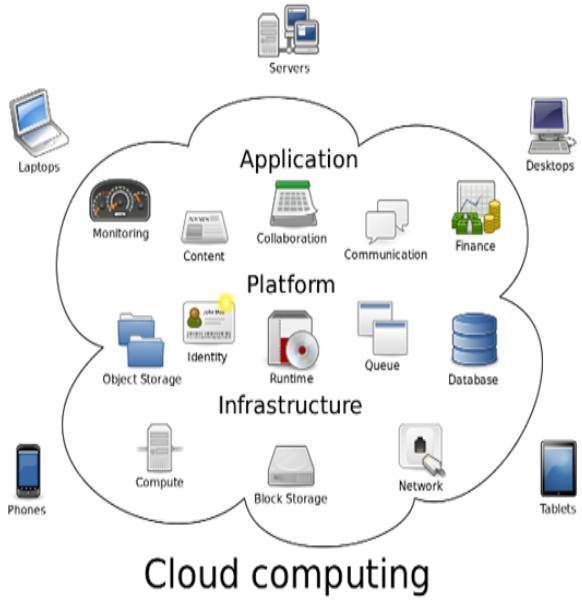
Huge amount of data is energetically updated in today's world. In cloud computing there are a lot of important problems which include issues of privacy, security, secrecy, communications capacity, government surveillance, consistency, and responsibility, among others. Encryption is a popular technique for protecting complex data. This paper proposes a summary of security issues and also examines the possibility of applying encryption procedure for data security and privacy in cloud computing. We also discussed about cloud computing security issues, mechanism, challenges that cloud service provider face during cloud engineering and presented the metaphoric study of various security algorithms.

Keywords : Cloud Computing, Data Security, AES, Blowfish, DES, RSA, Homomorphic Encryption , IDEA

I. INTRODUCTION

Cloud computing introduce new method for computing and related problems likes data privacy, data security in cloud. It offers development environment, allocation and reallocation of assets when needed, storage and interacting facility. The cloud computing is composed of shared computing resources and services that deliver the resources through which users can access the structures, hardware, applications, and services on request which are independent of locations. It contents the on-demand requests of the user. It simplifies the sharable resources "as-a-service" ideal. For the association, the cloud offers data axes to move their data totally. Here comes the assistance of the Cloud Computing i.e. It condenses the total of hardware that could have been used at user completion. As there is no essential for the collection of data at user's end because it is already at some other situation. So as an alternative of buying the complete infrastructure required to run the processes and save bulk of data which you are just renting the assets according to your requirements.

It abolishes the responsibility of local nodes for sustaining their data and also cloud provisions customizable resources on the web. Cloud Service earns keeps computing resources and data repeatedly through software.



II. SECURITY ISSUES AND TESTS OF CLOUD COMPUTING

Security is considered as one of the most critical characteristics in normal computing and it is not dissimilar for cloud computing payable to compassion and importance of data stored on the cloud. Cloud Computing structure uses new skills and services, most of which haven't been completely evaluated with respect to the refuge. Cloud Computing has some major issues and anxieties, such as data security, trust, prospects, procedures, and routine issues.

Solitary topic with cloud computing is that the running of the data which might not be entirely reliable; the hazard of malicious insiders in the cloud and the letdown of cloud services have conventional a strong attention by establishments.

Every time we discussed about security of cloud computing, there are several security issues ascend in route of cloud. Some of the security anxieties and solutions of them are recorded and absorbed below:

III. SECURITY CONCERN

Through the cloud physical refuge is lost because allocation of computing resources with other concerns. No facts or rheostat of where the assets course. Safeguarding the reliability of the data (removal and storage) actually it means changes only in reaction to authorized connections. A common customary to ensure data integrity does not exists.

The Client may be able to sue cloud facility providers if any privacy rights are disrupted and in any situation the cloud facility workers may face damage to their status. Who switches the encryption/decryption keys? Reasonably it should be the client. In instance of Payment Card Industry

Data Security Standard (PCI DSS) data records must be afford to security ampules and controllers.

ENSUE: Secure Data Transfer, Secure Software Interfaces, Data Separation, Secure Stored Data, User Access Control

IV. RELATED WORK

Many research on security in cloud computing has been proposed in recent times. A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture by KawserWazedNafi and others worked on the security of the cloud using more than encryption function to secure the connection and data. Many researcher work on the cloud computing security, the outsider and insider attack still the big concern to transferring form traditional way to cloud computing technique, works on

security on cloud not include the secure of whole system which another problem. Although these models ensures secured communication between users and servers, but they do not encrypt the loaded information. For best security ensuring process , the uploaded information needs to be encrypted so that none can know about the information and its location. Recently some other secured models for cloud computing environment are also being researched. But, these models also fail to ensure all criteria of cloud computing Security issues.

V. SECURITY ALGORITHMS USED IN CLOUD COMPUTING

1. RSA ALGORITHM

The best common Public Key algorithm is RSA, named for its authors Rivest, Shamir, and Adleman (RSA). RSA is mostly an asymmetric encryption /decryption algorithm. It is asymmetric in logic, that there is public key circulated to all through which one can encode the message and private key which is used in decryption is saved secret and is not shared to everybody. It would be a confirmation system of internet encryption. The RSA algorithm is the most usually used encryption. RSA algorithm is used in safeguard the security in cloud computing. While in RSA algorithm we have encrypted a data to afford security. This is the purpose of securing data is only concerned and authorized workers can access it. After encryption data is stored in the cloud. So that when it is required then a request can be placed to cloud provider.

Algorithm :

Key Generation: KeyGen(p, q) Input: Two large primes –p, q Compute m = p. q

$\varphi(n) = (p-1)(q-1)$

Choose e such that $\gcd(e, \varphi(n)) = 1$

Determine d such that $e.d \equiv 1 \bmod \varphi(m)$

Key:

Public key = (e, m) Secret key= (d, m)

2.AES ALGORITHM

Advanced Encryption Standard (AES), also known as Rajinder is used for safeguarding information. AES is a symmetric block cipher has been examined widely and is used usually now-a-days. Now AES works in cloud location symmetric key encryption algorithm is used with key length of 128-bits for this persistence. AnAES is used broadly now-a-days for security of cloud. Execution proposal states that First, User decides cloud services and will travel his data on cloud. The User submits his facilities necessities with Cloud Service Provider (CSP) and selects best specified services offered by worker. After migration of data to the chosen CSP occurs and in future whenever an request uploads any data on cloud, the data will first converted using AES algorithm and then sent towards provider. When encrypted, data is uploaded on cloud, any application to read the data will occur after it is decrypted on the workers end and then plain text facts can be read by worker. The simple text data is written somewhere on cloud. It includes all types of information. This encryption resolution is translucent to the submission and can be combined quickly and easily without any variations to application.

3) DATA ENCRYPTION STANDARD (DES)

It stances for Data Encryption Standard and it was established in 1977 and the first

encryption standard to be mentioned by NIST (National Institute of Standards and Technology). It encrypts the data in blocks of size 64 bits . That is 64 bits of plain text enthusiasms as input to DES, Then produces 64 bits of cipher text. The similar algorithm and the key are used for encryption and decryption, with trivial changes. The length of key of this algorithm is 56 bits; however key is actually input. Thus DES is a symmetric key algorithm

4) BLOWFISH ALGORITHM

Blowfish is a symmetric key algorithm and developed in 1993. It is the most common public algorithm provided by Bruce Schneier. It is a variable length key and 64-bit block cipher. No attack is recognized to be successful compared to this. Several experiments and research exploration proved the dominance of Blowfish algorithm over the other algorithms in relations of the processing time. Blowfish is the improved than any other algorithms in data and power consumption. Fast- Blowfish encryption speed on 32-bit is 26 clock cycles per byte.Simple-Blowfish uses simple operation such as addition, XOR and table consult, making its policy and application simple.

5. HOMOMORPHIC ENCRYPTION

Homomorphic encryption uses unequal key algorithm in which different two keys are applied for encryption and decryption i.e. public key and private key . Homomorphic means conversion of one data set to another, without losing its relation between them. In homomorpic complex functions are applied to encode the data and related but reverse function to decode the data.

6. IDEA

International Data Encryption Algorithm was suggested by James Massey and Xuejia Lai in

1991 and considered as popular symmetric key algorithm. It accepts 64 bits plain text and key size is 128 bits. In IDEA the 64 bits of data is divided into 4 blocks each having size 16 bits. Now basic operations modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied on sub blocks. There are eight and half rounds in IDEA each round consist of different sub keys. Total number of keys used for performing different rounds is 52. In round 1 the K1 to K6 sub keys are generated, the sub key K1 has the first 16 bits of the original key and K2 has the next 16 bits similarly for K3, K4, K5 and K6. Therefore for round 1 (16*6=96) 96 bits of original cipher key is used. What is the sequence of operations performed in each round? Let I1, I2 …I6 be the inputs to [5] round 1, functions in round 1 are:-

(i) Multiply I1 and

K1. (ii) Add I2 and

K2.

(iii) Add I3 and K3.

(iv) Multiply I4 and K4.

(v) Now, step 1 is EXOR with step

3. (vi) Step 2 EXOR with step 4.

(vii) Multiply step 5 with K5.

Similar operations are performed in other rounds

VI.CHARACTERISTICS AND COMPARISON OF ALGORITHMS

CHARACTERISTICS	AES	RSA	BLOWFISH	DES	HOMOMORPHIC	IDEA
Platform	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing
Scalability	Scalable	Not Scalable	Scalable	Scalable	Scalable	Not Scalable

Security	Secure for both provider and user.	Secure for user only	Secure for both providers and user/client side	Security applied to both providers and user	Secure for both provider and user	Secure for user only
Data Encryption Capacity	used for encryption of huge amount of data	used for encryption of less data	Less than AES	Less than AES	Less than AES	Can be used for encryption of small data
Authentication Type	Best authenticity provider	Robust authentic implementation	Comparable to AES	Less authentic than AES.	Less authentic than AES	Less authentic
Memory Usage	Low RAM needed	Highest memory usage algorithm	Can execute in less than 5 kb	More than AES	More than AES	Highest memory usage algorithm
Execution Time	Faster than others	Requires maximum time	Lesser time to execute	Equals to AES	Requires maximum time	Requires maximum time

VI. CONCLUSION AND FUTURE WORK

In this paper encryption algorithms have been offered to make cloud data secure, susceptible and provided to disquiet the security problems, contests and also evaluations have been made between RSA, AES, DES, Blowfish, Holomorphic Encryption, IDEA algorithms to find the best one security algorithm. It has used in cloud computing to making cloud data to secure and not to be slashed by invaders.

VII. REFERENCES

[1]. Auditing and Resisting Key Exposure on Cloud Storage Akshata M. Bhand, D. A. Meshram Student, ME (IT) , RMD Sinhgad School of Engineering,Pune, Assistant Professor, ME (IT), RMD Sinhgad School of Engineering, Pune,2017

[2]. Strong Key-Exposure Resilient Auditing for Secure Cloud Storage Jia Yu, and Huaqun Wang - IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. , NO., 2016

[3]. M.TECH, Dept. of CSE TKREC, JNTUH T.S, 2016

[4]. Enabling Cloud Storage Auditing with Key-Exposure Resistance Jia Yu, Kui Ren, Senior Member, IEEE, Cong Wang, Member, IEEE and Vijay Varadharajan, Senior Member, IEEE , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL XX NO1. , 2015

[5]. A Survey Paper on Cloud Storage Auditing with Key Exposure Resistance - Sneha Singha , S. D. Satav - International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611,2014

[6]. C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, Vol. 62, No. 2, pp. 362- 375, 2013.

[7]. Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Trans. on Services Computing, vol. 6, no. 2, pp. 409-428, 2013.

[8]. K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," World Wide Web, vol. 15, no.4, pp. 409-428, 2012.

[9]. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[10]. Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S.

[11]. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conference on Computer and Communications Security, pp. 756-758, 2010.

[12]. C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[13]. F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1-6, 2008.