International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Data Secure in Cloud Computing Using Encryption Algorithms

Mrunalini Motilal Shete[1], Pragati Damodar Hipparkar[2]

[1]Department of Computer Engineering, Sahakar Maharshi Shankarrao Mohite-Patil Institute of Technology &Research, Shankarnagar-Akluj, Maharashtra, India.

[2]Department of Computer Engineering, Sahakar Maharshi Shankarrao Mohite-Patil Institute of Technology &Research, Shankarnagar-Akluj,Maharashtra,India

Abstract: ***Cloud computing is the outsourcing of IT communications by the use of the Internet and maintaining own hardware and software environment. Cloud computing facilitates computing assets on demand by the use of a service provider. It is there whenever you need it, as much as you need, and you pay as you go and only for what you use. Security is a prim concern in the use of cloud computing. In this paper, we have presented encryption based security algorithms for cloud computing.***

Keywords: Cloud Compting, AES, DES, RSA

1. Introduction

Cloud computing is the outsourcing of IT communications by the use of the Internet and maintaining own hardware and software environment. Cloud computing facilitates computing assets (processor compute time and data storage) on demand by the use of a service provider. Comparisons of cloud services are made by their nature and utilize services such as gas or electricity. It is there whenever you need it, as much as you need, and you pay as you go and only for what you use. Now a day's Security of data has become a big distress. High levels of data repositioning have off-putting implications for data security and data shield as well as data availability. Thus the main worry regarding security of data residing in the Cloud is: how to make sure the security of data which is at rest. Although, consumers know the dimensions and location of web data high in no data mobility, you can find questions associated with its security and con_dentiality of the USB ports. To be sure the Cloud Computing area happens to be larger to its broad network access and exibility. But reliability regarding a secure and secure environment to the personal data and info on the user is still required.

Cloud computing is a form of information technology which is being used where lesser investment in efficient software is needed. Cloud computing consists of Access to applications and services is enabled over the network and it also require only access to internet connection. Possibly one can get access of the cloud with the use of an ordinary client simply anywhere and any-time and one needs a certain information facility, without any special software. Cloud computing also facilitates the clients for immediate access to pre-set common but valuable information resources (as access to the network, hardware, storage capacities, software, and special information services) that are eagerly available without a wide agreement making process.

2. Security Issue and Challenge of Cloud Computing

Security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven't been fully evaluated with respect to the security. Cloud Computing has several major issues and concerns, such as data security, trust, expectations, regulations, and performances issues. One issue with cloud computing is that the management of the data which might not be fully trustworthy; the risk of malicious insiders in the cloud and the failure of cloud services have received a strong attention by companies.

3. Problem Statement

There are various policies issues and threats in cloud computing technology which include privacy, segregation, storage, reliability, security, capacity and more. But most important among these to concern is security and how service provider assures it to maintain. Generally cloud computing has several customers such as ordinary users, academia and enterprises who have different motivations to move to cloud. If cloud clients are academia, security effect on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises most important problem is also security but with different vision. So, we mainly concentrate on data security of cloud computing using encryption algorithm using particular proposed plan.

4. Proposed Work Plan

We have proposed different security algorithms to eliminate the concerns regarding data loss, segregation and privacy while accessing web application on cloud. Algorithms like: RSA, DES, AES have been used and comparative study among them have also been presented to ensure the security of data on cloud. DES, AES, Blowfish are symmetric key

algorithms, in which a single key is used for both encryption/decryption of messages whereas DES (Data Encryption Standard) was developed in early 1970s by IBM. Blowfish was designed by Bruce Schneier in 1993, expressly for use in performance constrained environments such as embedded system. AES (Advanced Encryption Standard) was designed by NIST in 2001. RSA is a public key algorithm invented by Rivest, Shamir and Adleman in 1978 and also called as Asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. The key sizes of all the algorithms are different from each other. The key length of DES algorithm is 56 bits. The key size of AES algorithm is 128, 192, 256 bits. The key size of Blowfish algorithm is 128-448 bits. The key size of RSA algorithm is 1024 bits. Using Net beans IDE 7.3, and Java Run Time Environment, we have implemented our idea in the form of encryption and decryption algorithms which have discussed above and also we have made comparison between them on the basis of their characteristics.

5. Security Algorithm using Cloud Computing

5.1 RSA Algorithm

The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). RSA is basically an asymmetric encryption and decryption algorithm. It is asymmetric in the sense, that here public key distributed to all through which one can encrypt the message and private key which is used for decryption is kept secret and is not shared to everyone.

How RSA is going to work in cloud environment is explained as: RSA algorithm is used to ensure the security of data in cloud computing. In RSA algorithm we have encrypted our data to provide security. The purpose of securing data is that only concerned and authorized users 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. Cloud provider authenticates the user and delivers the data to user. As RSA is a Block Cipher in which every message is mapped to an integer. In the proposed cloud environment, Public key is known to all, whereas Private Key known only to user who originally owns the data. Thusencryption 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 will be decrypted using the corresponding Private Key only.

5.2 AES Algorithm

Advanced Encryption Standard (AES), also known as Rijindael is used for securing information. AES is a symmetric block cipher that has been analyzed extensively and is used widely now-a-days. How AES works in cloud environment? AES, symmetric key encryption algorithm is used with key length of 128-bits for this purpose. As AES is used widely now-a-days for security of cloud. Implementation proposal states that First, User decides to use cloud services and will migrate his data on cloud. Then User submits his services requirements with Cloud Service Provider (CSP) and chooses best specified services offered by provider. When migration of data to the chosen CSP happens and in future whenever an application uploads any data on cloud, the data will first encrypted using AES algorithm and then sent to provider. Once encrypted, data is uploaded on the cloud, any request to read the data will occur after it is decrypted on the users end and then plain text data can be read by user. The plain text data is never written anywhere on cloud. This includes all types of data. This encryption solution is transparent to the application and can be integrated quickly and easily without any changes to application. The key is never stored next to the encrypted data, since it may compromise the key also. To store the keys, a physical key management server can be installed in the user's premises. This encryption protects data and keys and guarantees that they remain under user's control and will never be exposed in storage or in transit. AES has replaced the DES as approved standard for a wide range of applications.

5.3 DES Algorithm

The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. DES is therefore a symmetric key algorithm.

6. Conclusion

In this paper encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges and also comparisons have been made between AES, DES and RSA algorithms to find the best one security algorithm, which has to be used in cloud computing for making cloud data secure and not to be hacked by attackers.
Encryption algorithms play an important role in data security on cloud and by comparison of different parameters used in algorithms, it has been found that AES algorithm uses least time to execute cloud data. DES algorithm consumes least encrypt-ion time. RSA consumes longest memory size and encryption time. By doing implementation for all algorithms in IDE tool and JDK 1.7, the desired output for the data on cloud computing has been achieved. In today's era demand of cloud is increasing so the security of the cloud and user is on top concern. Hence, proposed algorithms are helpful for today's requirement. In future several comparisons with different approaches and results to show effectiveness of proposed framework can be provided.

Reference

[1] Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , Cloud Computing System Based on Trusted Computing Platform, International Conference on Intelligent Computation Technology and Automation, Volume 1, May 2010, On page(s): 942-945.
[2] Pearson, S., Benameur, A., Privacy, Security and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference 2010, On page(s): 693-702.

[3] Rohit Bhadauria and Sugata Sanyal, A Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, Volume 47- Number 18, June 2012, On page(s): 47-66.
[4] Mohammed, E.M, Ambelkadar, H.S, Enhanced Data Security Model on Cloud Computing, 8th International Conference on IEEE publication 2012, On page(s): cc-12-cc-17
[5] Sang Ho. Na, Jun-Young Park, Eui- Nam Huh, Personal Cloud Computing Security Framework, Service Computing Conference (APSSC), Dec 2010 IEEE, On page(s): 671-675.
[6] Wang, J.K.; Xinpei Jia, Data Security and Authentication in hybrid cloud computing model, Global High Tech Congress on Electronics (GHTCE), 2012 IEEE, On page(s): 117-120.

Author Profile

Mrunalini Motilal Sheteis pursuing her Diploma in Computer Engineering from Sahakar Maharshi Shankarrao Mohite-Patil Institute of Technology &Research, currently she is studying in the last year of the course.

PragatiDamodar Hipparkaris pursuing her Diploma in Computer Engineering from Sahakar Maharshi Shankarrao Mohite-Patil Institute of Technology &Research, currently she is studying in the last year of the course.