ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

Security in Data Storage and Transmission in Cloud Computing

Anupriya Dubey[1], Mr Sourabh Sharma[1]

Gyan Ganga College of Technology, Jabalpur[1]

Abstract: Cloud computing has been envisioned as the next generation architecture of IT Enterprise. In the cloud, the data is transferred among the server and client. High speed is in important issues in networking. Cloud security is the current discussion in the IT world. Secure the data without affecting the network layer and protecting the data from unauthorised into the server. The data is secured in server based on choice of security method so that data is given high secure priority. Cloud computing has been fancied as the next generation architecture of IT enterprise .traditional solution, where the IT service are under proper physical, logical and personal controls cloud computing moves the application software and database to the large data centre, where the manager of the data and services may not be fully trustworthy.

Keywords: Cloud computing, IT Enterprise, Public model, Private model, Hybrid cloud, Community cloud.

I. INTRODUCTION

Cloud computing is a model that enables the development deployment and delivery of products and services to the customer with a pay-as –you –go model . It is a service model that involves the idea of storing and accessing the resource over the internet rather than storing them premise. Basically cloud computing has motivated academia, industry, businesses to take over this technology to host their applications on the cloud so as to cut – off the cost of buying the on premise local server as per Gartner server .

Type Software as a service

1. Software as a service - Software as a service is a software as delivery model that provide the access to software and its function operating on remote cloud infrastructure offered by cloud providers. Salesforce.com offering in the customer relationship management space was the innovator to provide software as service .other example includes online word processing and spreadsheet tools, Gmail, WhatsApp, and SAP.

2. Platform as a service – platform as service provide the framework for deploying and delivering of applications and services. It allows developers to develop new applications without any pressure of buying expensive tools and managing the local server. Examples include Hadoop.

3. Infrastructure as service - infrastructure as a service provides the infrastructure such as a network, memory, storage, processor to the users on demand. Example Amazon EC2.

Various types of deployment model

- Public model – The public cloud refers to sharing of computing infrastructure by many customers and they have no control and visibility over the computing resources where infrastructure is hosted'
- Private model – The private cloud does not share infrastructure with other organizations and dedicate to particular organization. In terms of security and cost, and private cloud exceed public clouds.
- Hybrid cloud – The hybrid cloud make the usage of both of clouds discussed above. Organization may hosts less critical data on the public cloud and confidential data on the private cloud.
- Community cloud - The community cloud is used where several organizations share the similar infrastructure. It may exist on premise or off premise.

II. SECURITY CHALLENGES IN CLOUD COMPUTING

Security is the important aspect for many organizations for cloud adoption .confidentiality, authentication, integrity, non repudiation and availability for clients systems are the general principals of security. Access control is another important factor for security .there is lots of security threats to cloud computing. a single flaw in one client application could allow malicious hacker to acquire access to more then one clients data. This problem is known as a data breach .The data loss is another issues that happens when the unauthorized user may delete or alter the entire records in the cloud if there is vulnerability in cloud provider side. Insecure APIs and weak interfaces are

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

another common security challenges in cloud computing .when confidential data is stored in it, the extreme focus should be given to the security of the cloud the hierarchy of various security in challenges in cloud computing .Three types of deployment model are further classified as public, private, hybrid and the security related to these models have Been discussed. In the same way, the service model is categorized further as IaaS, PaaS, and SaaS stating its security issues in commo

Security challenges in deployment models
To raise the facility of access in the organizations assorted users and departments across the organization allow sharing of assorted resources but alas lead to data breach problem .Cloning leads to the problem of data leakage concealing the machine's authenticity.

Basically the cloning deal with duplicating and replicating the data .Resources pooling refers to the unauthorized access because of sharing through the same network. Furthermore, in a shared multi tenant environment when any user consumers some unequal amount of resources then some resources contention issues might occur. Authentication and identity management is one of the big issues associated with deployment models in closed based systems.

Security challenges in services model
Typically the web browser is used for delivering applications in software as a service to cloud consumer. Since intruders are using the web to do malicious activities. So there is a threat to data because the issues like data leakage, malicious attacks and in the case of disaster backup and storage can lead to unauthorized access of sensitive data. Paas inherit security issues related to third party web services.

In the case of paas , the developer use the platform provided by cloud providers for deployment of the secure application that can be hosted on the cloud and these paas application should be upgraded frequently . This is turns affects security. Privacy and security can also be threatened because data may be stored in different locations with different legal authorities .So the developer must be aware of legal issues related to data to ensure that data is stored apropos location .

Network related security challenges
Cloud computing principally depends on servers the internet and remote computers in managing storing and maintaining data. The security issues associated with the network are of the prime concern .it provides on demand access to the high speed data rate, application, software, and resources to the users. But apart from this network infrastructure also faces various attacks and security challenges.

III. RELATED WORK

L. Tawalbeh, N.S. Darwazeh, R. S. Al-Qassas and F. Al Dosari (2015) [1], proposed an efficient cloud storage model that provides confidentiality and integrity through data classification and minimizes the complexity and processing time needed to encrypt the data by applying TLS, RSA , and SHA security mechanism based on the type of the classified data . They tested the proposed model with assorted encryption algorithms , and their simulation result showed the efficiency and reliability . This paper is established on the idea of manual classification of data and not the automatic classification and other encryption algorithm such as RSA , elliptic curve cryptography , and other asymmetric public key can be used to provide the higher level of security and confidentiality . N .Sengupta and R. Chinnasamy (2015) [2] ,design and encryption algorithm hybrid DESCAST to provide the security to the massive amount of data sent through the internet . through proposed algorithm, they tackled the limitation of both DES and CAST block cipher algorithm and analysed that the computation time and complexity for encryption and decryption is higher then the respective DES and CAST algorithm .In addition to this they concluded that combining 128 bit key and 64 bit key cipher algorithm, the brute force attack and attack via birthday problems were averted and the algorithm is more robust.

S .K .Sood (2013) [9], proposed a security model that keeps the most confidential and critical data on the private cloud and rest on the public cloud and for checking the integrity of the data at the public cloud this model used hash codes. He proposed cloud security model that associates a role to each user and stores the role of the user in the data base for user authorization process and operation can be performed by the user with respect to their roles. Also for security purpose , this model uses dual verification scheme for key authentication on one layer and user authentication on one layer and user authentication by using username and password on another layer . A cryptographic process is proposed for keeping data secure on the cloud . He analysed the model against various model against various types of attacks. This model is compared with various existing cloud security framework and the simulation result showed that this technique is much more robust, efficient and faster than other existing models . Furthermore, this model is efficient in terms of cost because it stores highly sensitive data on the private cloud and less critical data on the public cloud, where storage cost of data is relatively very less.
J .J .Hwang, Taoyuan, Taiwan, Y. C. Hsu and C. H .Wu (2011) [4], has proposed a data security model using encryption and decryption algorithms. The model used such mechanism that the cloud service provider can perform storage and encryption / decryption task. The

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

drawback of this method is that the user or the data owner has no control of data.

J. K Wang and X. Jia (2012) [10], described several method to secure user data such as authentication interface, single encryption, and multi level virtualization. The other main topic of their paper is Authentication inter cloud based on CA and PKI model.

Creighton T .R .Hager, "In personal Digital Assistants energy and performance and efficiency of block cipher ". On various kinds of data comparative analysis has been performed by the author of various encryption algorithms. The best and fast encryption algorithm then others in Blowfish.

Gary C. Kessler, "An overview of cryptography ". It is an old paper based on cryptography by Gary C, Kessler, and since then till date it was continuously updated. It was last updated in 2014. The author suggested again the great source for the cryptography algorithms.

Navita Aggarwal "simultaneously performed compression, steganography and encryption and simultaneously and an efficient pixel - shuffling based approach on images ". The author conducted the research, where it have applied encryption, compression, steganography on the digital image data. Encryption algorithm pixel shuffling based symmetric, compression, algorithm as DCT, for image steganography WinRAR are used to achieve the proposed model in the paper .

IV. CONCLUSION

This paper gives a survey of different threats and solutions in cloud computing environment and with respect to security and privacy of user's sensitive data in the cloud computing. We investigate the problem of data security in cloud data storage and data transmission, which is essentially a distributed storage system. To ensure the correctness of user data in cloud data storage, we proposed an effective and flexible of distributed scheme. In the data transmission of proposed, method transferred data is encrypted in the upper layer on top of the transport layer instead of using IPSec or SSL .THE scheme of for the performance improvement

REFERENCES

[1] L. Tawalbeh , N.S. Darwazeh, R.S. Al-Qassas and F. Al Dosari (2015)[1], proposed an efficient cloud storage model that provides confidentiality and integrity through data classification and minimizes the complexity and processing time needed to encrypt the data by applying TLS, RSA , and SHA security mechanism based on the type of the classified data .

[2] N .Sengupta and R. Chinnasamy (2015) [2], design and encryption algorithm hybrid DESCAST to provide the security to the massive amount of data sent through the internet .

[3] S .K .Sood (2013) [9], proposed a security model that keeps the most confidential and critical data on the private cloud and rest on the public cloud and for checking the integrity of the data at the public cloud this model used hash codes.

[4] J .J .Hwang, Taoyuan, Taiwan, Y . C .Hsu and C . H .Wu (2011)[4], has proposed a data security model using encryption and decryption algorithms. The model used such mechanism that the cloud service provider can perform storage and encryption / decryption task. The drawback of this method is that the user or the data owner has no control of data.

[5] J . K Wang and X . Jia (2012) [10] , described several method to secure user data such as authentication interface , single encryption , and multi level virtualization . The other main topic of their paper is Authentication intercloud based on CA and PKI model.

[6] Creighton T .R .Hager , " In personal Digital Assistants energy and performance and efficiency of block cipher ". On various kinds of data comparative analysis has been performed by the author of various encryption algorithms. The best and fast encryption algorithm then others in Blowfish.

[7] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/ contrib. /supported/IEEEtran/

[8] Gary C. Kessler, "An overview of cryptography ". It is an old paper based on cryptography by Gary C, Kessler, and since then till date it was continuously updated. It was last updated in 2014 . The author suggested again the great source for the cryptography Navita Aggarwal "simultaneously performed compression, steganography and encryption and simultaneously and an efficient pixel -shuffling based approach on images". The author conducted the research, where it have applied encryption, compression , steganography on the digital image data . Encryption algorithm pixel shuffling based symmetric, compression, algorithm as DCT, for image steganography WinRAR are used to achieve the proposed model in the paper .algorithms.