ISSN: 2321-7782 (Online)
Volume 3, Issue 11, November 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Maintaining Data Confidentiality and Security over Cloud: An Overview

Dushyant Balwant Sisode[1]
PG student
Dept of computer science and engineering
Lord Krishna College of Technology Indore, India

Vijay Kumar Verma[2]
Asst. Professor (CSE)
Dept of computer science and engineering
Lord Krishna College of Technology Indore, India

Abstract: ***Cloud computing allows for both large and small organizations to have the opportunity to use internet based services so that they can reduce start-up costs, lower capital expenditures, use services on a pay-as you use basis, access applications only as needed. Cloud Computing is a set of IT based Services provided to a customer over a network and these services are delivered by a third party provider. Cloud services include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Security of data in cloud computing environment is an important challenge. Several Algorithms have been developed for enhancing the security of data in cloud. This paper presents a study of various data security used in cloud.***

Keywords: cloud computing; data Security; data Confidentiality

I. INTRODUCTION

Cloud computing environment is made up with three important elements.

1) Clients

2) Data Center

3) Distributed servers

Clients are typically computers, laptops, tablet computers, mobile phones, or PDA. Datacenter is the collection of servers where the application to which you subscribe is housed [1,2].

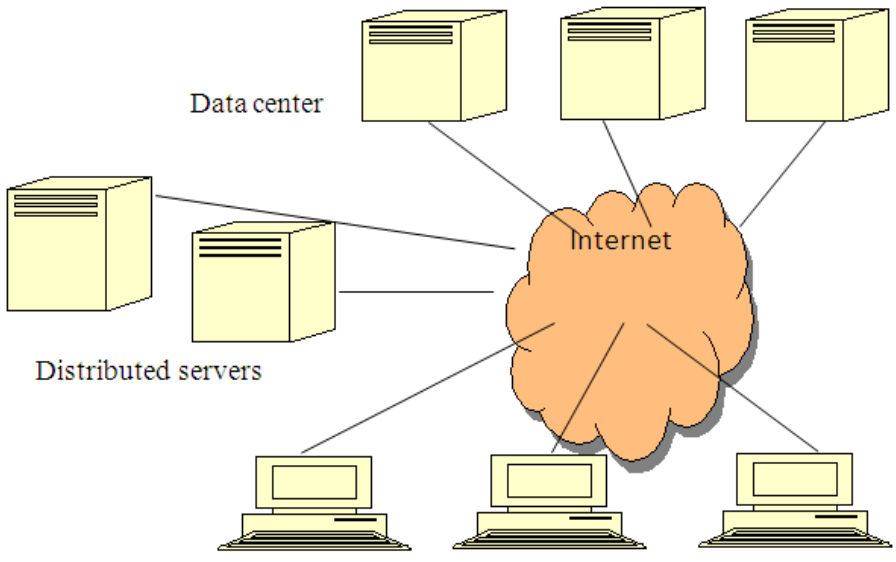

Fig1. Important elements of cloud environment

It could be a large room full of servers on the other side of the world that you access via the Internet. Servers don't all have to be housed in the same location. Servers are in geographically disparate locations. But to you, the cloud subscriber, these servers act as if they're humming away right next to each other. This gives the service provider more flexibility in options and security[3,6,7].

II. Types Services Over Cloud

The cloud computing is a very broad area and it covers about each and every online service. There are usually three models of cloud service under consideration, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

1. Software as a Service (SaaS): Is the model in which an application is hosted as a service to customers who access it via the Internet. When the software is hosted off-site, the customer doesn't have to maintain it or support it. Applications of SaaS include
2. Platform as a Service (PaaS): Is another application delivery model. PaaS supplies all the resources required to build applications and services completely from the Internet, without having to download or install software.
3. Infrastructure as a Service (IaaS): It is comprised of highly automated and scalable compute resources, complemented by cloud storage and network capability which can be self-provisioned, metered, and available on-demand[4,8,9].

Main difference between SaaS, PaaS and IaaS is shown by figure 2.

Fig. 2 Difference between cloud services

III. Standards of Cloud Computing

Large companies require that cloud-computing platforms meet the highest standards of services. To meet these requirements seven standards have been developed for clouding computing these are[12,13].

1. S**ecurity** – Providing world class security using different algorithms and techniques to each and every level of cloud environment.
2. **Belief and transparency** – Providing transparent environment and availability information. Services are delivered on real-time basis with high performance
3. **Accurate multitenancy** – Providing maximum scalability and performance to satisfy the requirement of the customers with a true multitenant architecture.
4. **Confirmed scale** –Providing Support for the millions of users with confirmed scalability.
5. **Great performance** –Providing reliable and high-speed performance globally.
6. **Disaster recovery** – Providing several techniques for protecting data of customer by several data centers. Providing backup, data archive recovery form failover.
7. A**vailability** – Providing excellent infrastructure and equipment for high-availability of the application to the user.

IV. Information Security In Cloud

There are three important parameter are considered for security of information over cloud. They are

1. **Confidentiality**:- Ensure that only authorized users have access to data.
2. **Integrity**: Ensure that unauthorized changes to data are not allowed.
3. **Availability** :ensure that authorized user have reliable and timely access to data Information security frameworks have five important layers

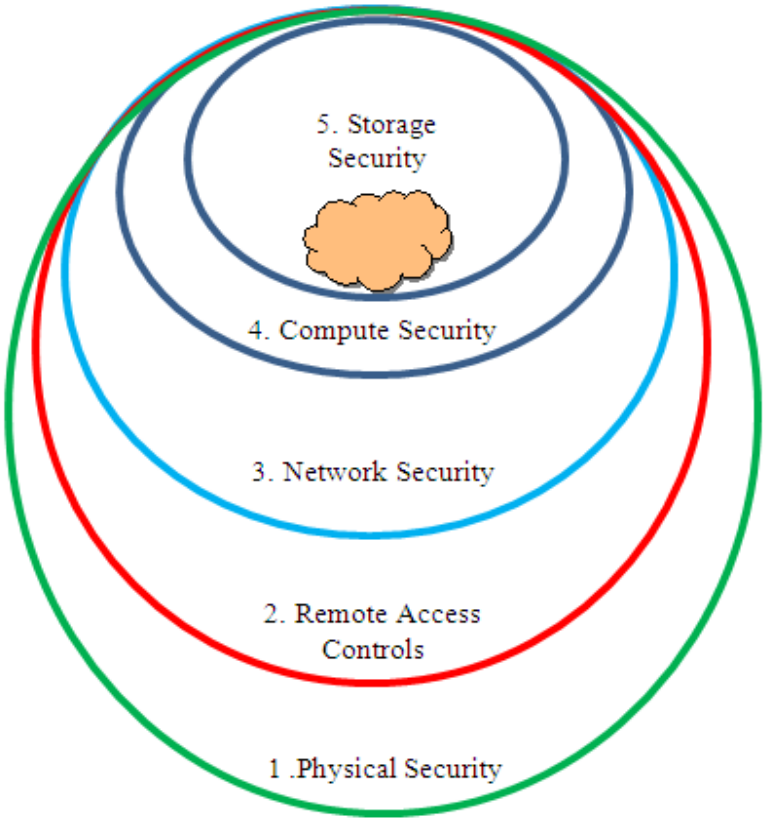

Fig. 3 data Information security frameworks

1. Perimeter Security (Physical security)
2. Remote Access Controls (Authentication)
3. Network Security (Firewall)
4. Compute Security (Hardening, Antivirus)
5. Storage Security(Encryption)

V. Encryption Based Security

In cloud computing services are provided over the Internet and that was typically in the form (IaaS), (PaaS), (SaaS). Data security is an important challenges and issue in cloud computing.

Modern data communications uses cryptography an effective, efficient and essential techniques for secure transmission of information in cloud environment. Cryptography can be classified as Symmetric key algorithm and Asymmetric key algorithm[10,11]

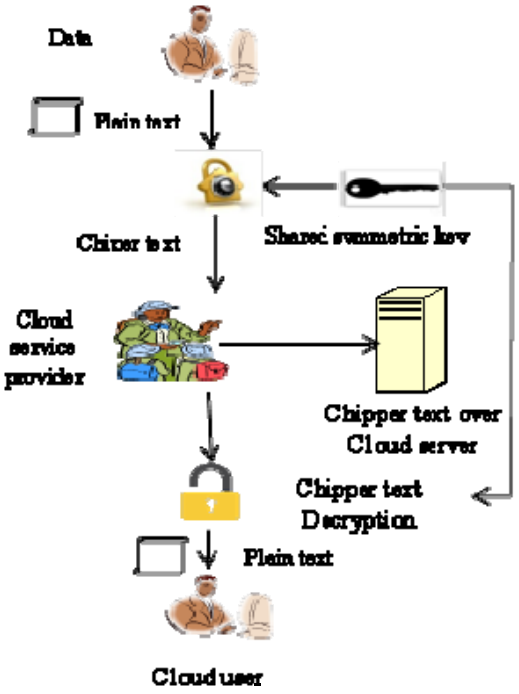

Fig. 4 Data Encryption and Decryption over Cloud

VI. LITERATURE REVIEW

Several methods have been developed for securing data over cloud using different encryption techniques. In 2012 Neha Jain and Gurpreet Kaur " Implementing DES Algorithm in Cloud for Data Security". They proposed a chipper Block Chaining system to secure for clients and server. They design a security architecture using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data[7,8].

In 2012 Nilesh N. Kumbhar and Virendrasingh V. Chaudhari proposed "The Comprehensive Approach for Data Security in Cloud Computing: A Survey". This paper gives descriptive knowledge regarding cloud computing by encryption and decryption services. They show that if a cloud system is performing a task of storage of data and encryption and decryption of data on the same cloud then there are much more chances of getting access to the confidential data without authorization[6].

In 2013 Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti "An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding". They implemented security for image. They have used an image, read its pixels and convert it into pixels matrix of order as height and width of the image. Replace that pixels into some fixed numbers, generate the key using random generation technique and applied Huffman coding on that array[9].

In 2013 Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem proposed "Efficiency of Modern Encryption Algorithms in Cloud Computing". They give introduction of various encryption algorithms (symmetric, asymmetric). They discuss various issue involved in using cloud services such as the performance of encryption algorithms on a cloud environment for different input block data size, how the change in the size of the files after encryption is complete[3].

In 2014 Ashwini R. Tonde, Akshay P. Dhande prposed "FPGA based implementation of Advanced Encryption Standard (AES) Algorithm". They proposed FPGA-based Advanced Encryption Standard algorithm. The design has been coded by Very high speed integrated circuit Hardware Descriptive Language. The design uses an iterative looping approach with block and key size of 128 bits, lookup table implementation of S-box[9,10].

In 2014 Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona proposed "Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features". They provides a comparative study using symmetric key cryptographic ciphers (RC4, AES, Blowfish, RC2, DES, Skipjack, and Triple DES) on the basis of encryption time with the

variation of various file features. They use different file features like different data types, data size, data density and key sizes[14,15].

VII. Advantage And Disadvantage

Advantages & Disadvantages of Symmetric Key Encryption

Advantage	Disadvantage
Symmetric key encryption can be extremely secure	Sharing the Key
Symmetric key encryption Relatively Fast	More Damage if Compromised

Table 1 Advantages & Disadvantages of Symmetric Key Encryption

Advantages & Disadvantages of Asymmetric Key Encryption

Advantage	Disadvantage
cryptography there is no need for exchanging keys	comparatively complex
public-key cryptography is increased security	asymmetric encryption to encode a symmetric key and transfer it to the other party

Table 2 Advantages & Disadvantages of Asymmetric Key Encryption

VIII. Conclusion

In this paper we have presented a study over types cloud service and cloud standards. Data security over cloud is an important issue. We also present a model which show how encryption based techniques used to store data over cloud We also introduce the advantage and disadvantage of various encryption techniques.

References

1. Sruthi B. Asok, P. Karthigaikumar, Sandhya R3, Naveen Jarold K4, Siva Mangai "IRIS Based Cryptography" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2013
2. Obaida Mohammad Awad Al-Hazaimeh "A New Approach For Complex Encrypting And Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.
3. Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti, "An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding" IJCTA | Nov-Dec 2013 .
4. Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem. "Efficiency of Modern Encryption Algorithms inCloud Computing" Web Site: www.ijettcs.org Email:editor@ijettcs.org, Volume 2, Issue 6, November – December 2013.
5. Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona" Analysis And Comparison Of Symmetric Key Cryptographic Algorithms Based On Various File Features" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014.
6. Neha Jain and Gurpreet Kaur "Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 (4), 2012
7. Mandeep Kaur and Manish Mahajan "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Vol. 2 No. 10 October 2012
8. Amir Mohamed Talib" Security Framework of Cloud Data Storage Based on Multi Agent System Architecture: Semantic Literature Review" Computer and Information Science Vol. 3, No. 4; November 2010
9. Rachna Arora and Anshu Parashar " Secure User Data in Cloud Computing Using Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926
10. B. Ravi Kumar, Dr.P.R.K.Murti" Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology" B. Ravi Kumar et al. / International Journal on Computer Science and Engineering (IJCSE) Vol. 3 No. 7 July 2011.
11. Anthony T. Velte Toby J. Velte, Ph.D. Robert Elsenpeter Cloud Computing: A Practical Approach Copyright © 2010 by The McGraw-Hill Companies
12. Matthew J. Harmon Cloud Security (ISC)2 Twin Cities Area Chapter 2013 Annual Meeting 18 June 2013
13. K Nava Jyothi Practical Approach to Cloud Centre for Development of Advanced Computing, Hyderabad 8/9/2010
14. Tobias Kurze_, Markus Klemsy, David Bermbachy, Alexander Lenkz, Stefan Taiy and Marcel Kunze Cloud Federation Karlsruhe Institute of Technology (KIT), Kaiserstrasse 12, 76131 Karlsruhe, Germany

