IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 10, Issue 2, April - May 2022
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

An Effective Data Security Approach in a Cloud Computing Environment: A Comprehensive Study

Satendra Verma [1], Alex loraay [2],

[1], *Associate Professor,Department of Computer Science And Engineering Thompson Rivers University [TRU]Kamloops, British Columbia*
[2] *Assistant Professor,Department of Computer Science And Engineering Thompson Rivers University [TRU]Kamloops, British Columbia*

Abstract— this paper discusses the data security in cloud computing. It is a study of data in the cloud and aspects related to it concerning security. As we all know Cloud computing is an emerging domain and security of the data must be protected over the network. Cloud computing is used by many of the organizations for storing the huge amount of data on the clouds. Therefore, there is need to secure the data which may in the form of text, audio, video, etc. There are numerous algorithms designed by the researchers for securing the data on the cloud.

The paper will go in to details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats.

Keywords: Data Security, Data-at-rest, Data-in-transit, Data-in-use, Data Encryption.

I. INTRODUCTION

The word Cloud Computing originated recently and is not just used. Of the various definitions available, one of the simplest is "a network solution for providing cheap, reliable, easy and simple access to IT resources." Cloud computing is not considered application-oriented, but service-oriented. This service-oriented nature of cloud computing not only reduces infrastructure overhead and cost of ownership, but also provides flexibility and better end-user performance.

The primary concern of cloud data is security and privacy. Ensuring integrity, privacy and data protection is very important for the cloud service. To this end, many service providers use different policies and mechanisms depending on the nature, type and size of the data.

One of the most important questions when using cloud storage is whether you need to use a third-party cloud service or create an internal organizational cloud. Therefore, the data is more sensitive to be stored in a public cloud, such as defense and national security data or more confidential future product details, and so on. This type of data can be extremely sensitive and the consequences of exposing this data to the public cloud can be serious. Therefore, it is advisable to store data in the internal organizational cloud. This approach facilitates data security by following data usage policies. However, it does not yet guarantee complete data security and privacy,

because many organizations do not have enough skills to access all layers of sensitive data protection. This document continues to improve the data security techniques used to protect and secure data in the cloud. He talks about potential threats to cloud data and their solutions, which use different encryption methods to protect data. In this article we organize four sections.

II. LITERATURE REVIEW

In categorize to understand the basics of cloud computing and storing data securing on the cloud, a number of resources have been consulted. This section provides a review of literature to set a foundation of discussing different data security feature.

PRIYA JAIN, DR. JITENDRA SINGH CHOUHAN[1] there is numerous security issues pertinent to cloud infrastructure of which most critical ones are discussed in this paper. Next cloud computing security considerations

PACHIPALA YELLAMMA , N ARASIMHAM CHALLA AND V SREENIVAS[2]The achievement of the paper has significant meaning to the automation of information and popularization of national economic information network, and has very high reference value to the research of network security technology.

SRINIVAS, VENKATA AND MOIZ[3] provide an excellent insight into the basic concepts of cloud computing. Several key concepts are explored in this paper by providing examples of applications that can be developed using cloud computing and how they can help the developing world in getting benefit from this emerging technology.

TJOA, A.M. AND HUEMER[4]examine the privacy issue by preserving data control to the end user to surge confidence. Several Cloud computing attacks are reviewed and some solutions are proposed to overcome these attacks.

MIRAGE IMAGE MANAGEMENT SYSTEM[5] this system addresses the problems related to safe management of the virtual machine images that summarize each application of the cloud.

KREŠIMIR POPOVIĆ, ŽELJKO HOCENSKI[7] in this paper, security in cloud computing was discussed in a manner that covers security issues and challenges, security principles and security management models.

TAKESHI TAKAHASHI, GREGORY BLANCY, YOUKI KADOBAYASHIY, DOUDOU FALLY, HIROAKI HAZEYAMAY, AND SHIN'ICHIRO MATSUO[8] this paper introduced technical layers and categories, with which it recognized and structured security challenges and approaches of multitenant cloud computing.

NAGARJUNA, C.C KALYAN SRINIVAS, S.SAJIDA,LOKESH[9] In this paper the main issue with multi tenancy is that the clients use the same computer hardware to share and process information and the result is that tenants may share hardware on which their virtual machines or server runs, or they may share database tables.

SABAHI[10] discussed about the security issues, reliability and availability for cloud computing. He also proposed a feasible solution for few security issues

MATHISEN, E[11] discussed about some of the key security issues that cloud computing are bound to be confronted with, as well as current implementations that provide a solutions to these vulnerabilities.

BIN CHEN AND XIAOYI YU[12] discussed a scheme for smart power grid cloud computing, and explains the various benefits with the cloud computing, and the existing security issues and preventive measures.

III. CLOUD SERVICES AND MODELS

Cloud Computing provides common resources and services over the Internet. In recent years, the use of the Internet has increased the cost of infrastructure, hardware and software extremely quickly. This means that a new technology known as cloud computing is used to solve these problems by providing services when an Internet user needs them, and absolutely reduces infrastructure, hardware and software costs. The services offered by cloud computing have various features such as high scalability and reliability. , flexibility and dynamic properties. The cloud uses many similar services and models

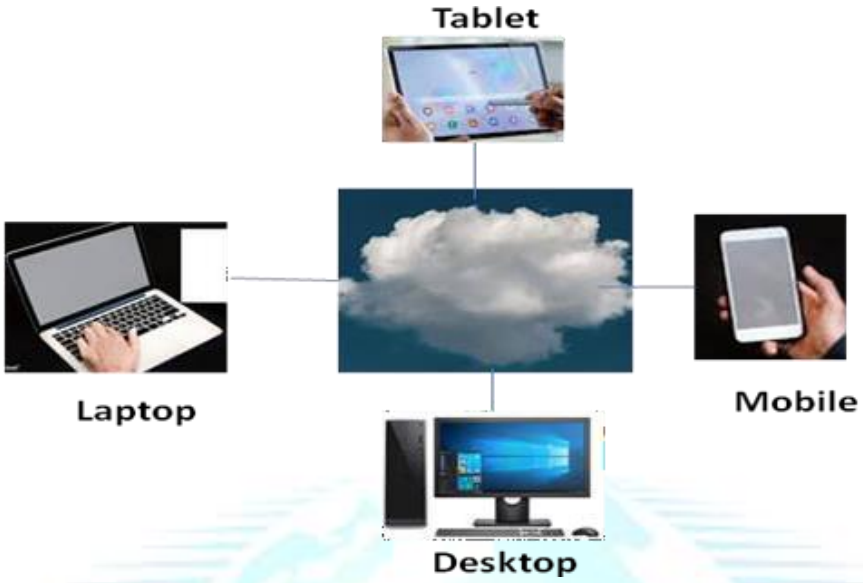


Fig 1 Cloud Computing

SERVICES

Three types of cloud services and user can use any services which are mentioned below:

A. Software as a Service (SaaS)
B. Platform as a service (PaaS)
C. Infrastructure as a service (IaaS)

Essentials	**SaaS**	**PaaS**	**IaaS**
As a service	It is Software as a Service	It is Platform as a service	It is Infrastructure as a service
Features	It is also called a delivery model where the software and the data which is associated with are hosted over the cloud environment by third party.	Web-based tools to develop applications so they run on systems software	provides services to the companies with computing resources including servers, networking, storage, and data centre space on a pay-per-use basis
Examples	Gmail account	Google App Engine	Microsoft Azure

MODELS

There are three Deployment Models and are described below:

A. Public Model
B. Private Model
C. Hybrid Model

Essentials	Public Model	Private Model	Hybrid Model
Infrastructure	This infrastructure is available to the general public.	This infrastructure is available to the private public.	This infrastructure is available to the mixed public.
Resources	Resources are generally available to everyone or anywhere.	Resources are available to individual or selected.	Resources are generally available to everyone or selected.
Services	This kind of a service is accessed by everyone.	This kind of a service is not accessed by everyone.	This kind of a service is accessed by some time yes some time no.

IV. DATA SECURITY IN CLOUD COMPUTING

Cloud computing data security combines more than data encryption. Data security requirements depend on three service models, such as SaaS, PaaS, and IaaS.

These three states of data pose a threat to their security in the cloud; Data and rest, which means that data is stored in the cloud and data transfer, which means moving data inside and data is used, which means that data is used outside the cloud. Data confidentiality and integrity depend on the nature of the data methods, protection mechanisms and processes. It is also in three states.

A. Data at Rest

Data at rest submit to data in cloud, or any data that can be accessed using by Internet. This consists of backup data and also live data. So it is extremely hard for organizations to protect data at rest if they are not maintaining a private cloud since they do not have physical manage over the data. So, this issue can be determined by maintaining a private cloud with carefully controlled access (fig2).

Fig 2 Data in Transit

Data in transit submit to data which is moving in and out of the cloud. This data can be in the form of file/database stored on the cloud and it can be apply for use at selected position. Where, data is uploaded to the cloud, data which uploaded is called data in transit. It is more responsive data like user names and user passwords and can be encrypted at times. So data in unencrypted form is also data in transit.

Data in transit is on event additional which showing to risks than the data at rest because it has to go from one location to another. (Fig2). There are many ways in which intermediary software can watch the data and on occasion have the ability to change the data on its way to the destination. In order to protect data in transit, the major policies are encryption.

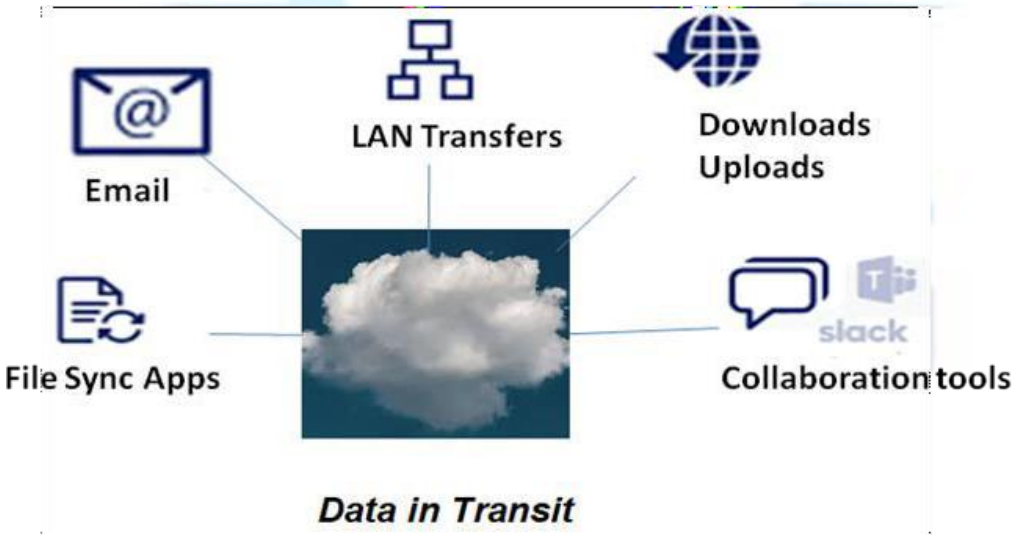


Fig.3

B. Data-in-use

Data in use normally processing like creation or transformation or deletion of data. When processing take place in the Cloud environment, the risks of mistreat increase due to the huge number of users involved in Cloud environment (fig4).

Fig 4

V.MAIN SECURITY CHALLENGES

All we know that it is not simple to protect and guarantee the safety of linked computers because a series of computers and clients are involved this is known as multi-tenancy. The cloud service providers and cloud computing both have to face many challenges, mainly in the area of security issues. So it is very vital to think how these challenges are little and how the security design by models in order to guarantee the security of clients and also establish a safe cloud computing environment. The major challenges involved are:

Require of proper governance

Lock-in

Another problem is unsatisfactory standards of data format, a lack of operating methods and lack of tools which together because compromised portability between the services and applications, still between service providers. So the customer has to be dependent totally and fully on the vendor.

Isolation crash

The distribution of resources owing to multi-tenancy of cloud computing is itself a uncertain characteristic. The lack of divide storage can be deadly to businesses. Other concerns involving guest hopping attacks and their problems are careful to be a huge difficulty in the use and execution of cloud computing applications.

Malicious attacks from management inside

Occasionally the architecture of cloud computing environments poses danger to the privacy and security of the customers. While it happens infrequently, this risk is very hard to deal with. Like include the administrators and managers of cloud service providers who can occasionally effort as malicious agents and threaten the security of the clients using cloud computing applications.

Insecure or partial data removal

In case where clients request data to be deleted either incompletely or completely, this raises the query of

whether it will be possible to delete the preferred part of their data segment with correctness. This makes it difficult for the clients to subscribe to theservices of the cloud-computing.

VI. PROTECTING DATA USING ENCRYPTION

Encryption techniques for data at rest and data in transit can be different. For examples, encryption keys for data in transit can be short-lived, while for data at rest, keys can be hold for longer periods of time.

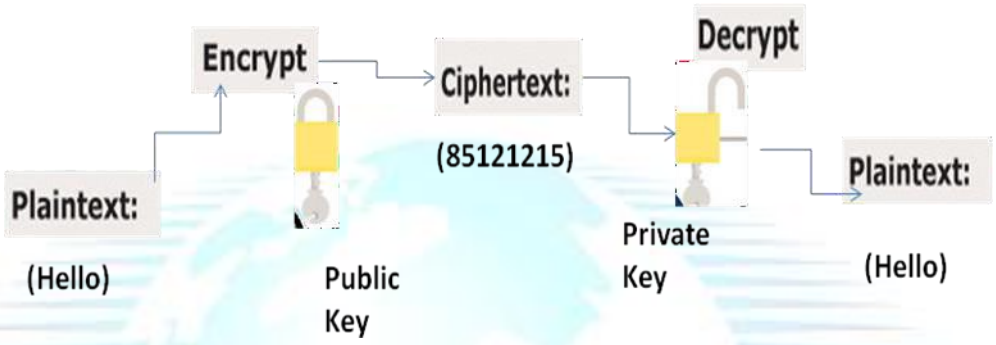


Fig 5: Basic Cryptography Process

Dissimilar cryptographic techniques are used for encrypting the data these days. Cryptography has greater than before the level of data protection for promised content integrity, authentication, and availability. In the basic form of cryptography, plaintext is encrypted into cipher text using an encryption key, and the resulting cipher text is then decrypted using a decryption key as illustrated in Fig 5.
Generally there are three basic uses of cryptography:

As Block Ciphers

A block cipher is an algorithm for encrypting data (to create cipher text) in which a cryptographic key and algorithm are applied to a block of data instead of per bit at a time.

In this technique, it is made certain that similar blocks of text do not get encrypted the same way in a message. Usually, the cipher text from the prior encrypted block is applied to the next block in a series.

As demonstrated in Fig 6, the plain text is divided into blocks of data, regularly 64 bits. These blocks of data are then encrypted using an encryption key to create a cipher text.

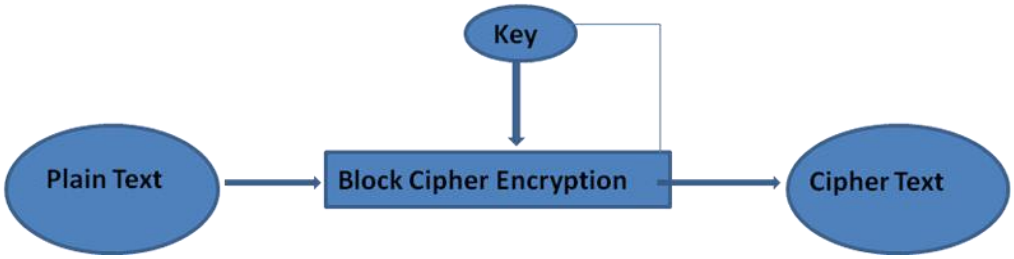
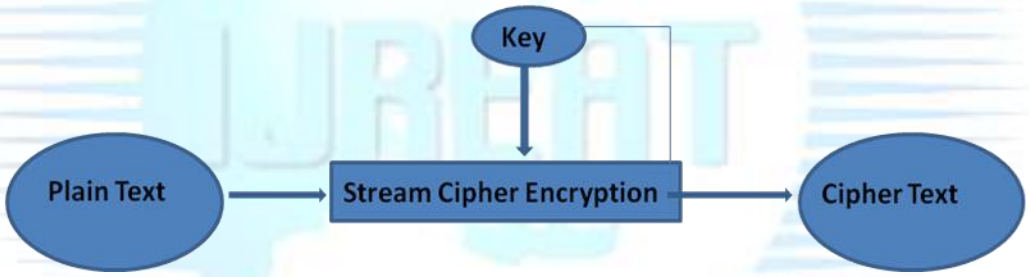


Fig 6: Block Cipher Mechanism

As Stream Ciphers

This technique of encrypting data is also called state cipher since it depends upon the present state of cipher. In this technique, every bit is encrypted instead of blocks of data. An encryption key and an algorithm are applied to every bit, one at a time.
Presentation of Stream ciphers is usually faster than block ciphers because of their low hardware complexity. But, this technique can be vulnerable to severe security problems if not used properly as fig 6.



As demonstrated in Fig 7, stream cipher uses an encryption key to encrypt every bit instead of block of text.

Fig 7: Stream Cipher Mechanism

The resultant cipher text is a stream of encrypted bits that can be soon decrypted using decryption key to produce to new plain text.

As Hash Functions

In this technique, a mathematical function called a hash function is used to change an input text into an alphanumeric string. Usually the produced alphanumeric string is permanent in size. This technique makes sure that no two strings can have similar alphanumeric string as an output. Still if the input strings are slightly dissimilar from each other, there is a possibility of great differentiation between the outputs strings produced through them.

This hash function can be an extremely simple mathematical function as the one shown in equation (1) or extremely complex (fig 8).

Fig 8: Cryptographic Hash Function Mechanism

All these on top of mentioned methods and techniques are extensively used in encrypting the data in the cloud to make sure data security. Use of these techniques varies from one scenario to another. Whichever technique is used, it is well suggested to ensure the security of data in both private and also public clouds.

VII. CONCLUSION

Improved use of cloud computing for storage contributes to the style of improving cloud storage methods. Data presented in the cloud can be dangerous if it is not legally protected. This document, "An Effective Approach to Data Security with Cloud Computing: A Comprehensive Study," discusses the risks and threats to cloud data security and provides an overview of three types of security issues. One of the main issues of this article is data security and its threats and implications for cloud computing. Data in various states is discussed along with effective data encryption techniques in cloud computing. The study provides a summary of block ciphers, stream ciphers, and hash functions used to encrypt data in the cloud, whether at rest, during transmission, or in use.

VIII. REFFERENCES

[1] www.engpaper.com › cloud-computing-security-2019 cloud computing security 2019 IEEE PAPERS.

[2] J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secur., vol. 1, no. September 2011, pp. 3–22, 2014.

[3] D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, "Retaining data control to the client in infrastructure clouds," Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE. pp. pp. 9–16, 2009.

[4] Zhang and H. Chen, "Security-Preserving Live Migration of Virtual Machines in the Cloud," J. Netw. Syst. Manag., pp. 562–587, 2012.

[5] J. Hu and A. Klein, "A benchmark of transparent data encryption for migration of web applications in the cloud," 8th IEEE Int. Symp. Dependable, Auton. Secur. Comput. DASC 2009, pp. 735–740, 2009.

[6] Krešimir Popović, Željko Hocenski,"Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia.

[7] Takeshi Takahashi, Gregory Blancy, Youki Kadobayashiy, Doudou Fally, Hiroaki Hazeyamay, Shin'ichiro Matsuo,"Enabling Secure Multitenancy in Cloud Computing: Challenges and Approaches".

[8] Nagarjuna,C.C kalyan srinivas,S.Sajida,Lokesh" SECURITY TECHNIQUES FOR MULTITENANCY APPLICATIONS IN CLOUD", C.C. Kalyan Srinivas et al, International Journal of Computer Science and Mobile Computing Vol.2 Issue. 8, August-2013, pg. 248-251.