ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Data Encryption Oriented in Cloud Computing Security

T. Sivasakthi[1], Dr. S.Latha[2]

Research Scholar, Department of Computer Applications, St.Peter's University, Avadi, Chennai, Tamilnadu, India[1]

Head, Department of computer Application, St.Peter's University, Avadi, Chennai, Tamilnadu, India[2]

ABSTRACT: Cloud computing is the Internet based computing whereby data shared resources, software and information are provided to computers and other devices on demand, like a public utility. It is a remote server to maintain data and applications this cloud computing allowed only and access their personal files. This paper proposed to the efficient encryption and decryption services for cloud computing by splitting a services from a storage service of data to eliminate the particular data of maintain a privacy to enhance one service providers application system, according the case concept for perspective of cloud users or customers.

KEYWORDS: Cloud computing, data privacy, encryption, decryption, blowfish.

I. INTRODUCTION

Cloud computing is a recent field in the computational intelligence techniques which aims surmounting the computational complexity and provide dynamically services. It is a very large scalable and virtualized and resource throw the Internet. Cloud computing is a technology that user the Internet and remote servers to maintain and applications. The cloud computing allows end users to use applications such as data storage,email,word processing, social media etc.this all internet technology allows for much more efficient computing by centralizing various resource such as storage,bandwith,processing and memory.Hence Amazon, Elastic computing (EC2),Google app Engine are public cloud providers. The private is a second type of cloud. A simple example of cloud computing is yahoo, email, gmail of Hotmail etc.all user a would need is just to plug into the internet from anyplace access processing, applications and data services whenever needed.Cloud computing reduce cost and hardware that cloud have been used at end they no need to store data at users end because it is already at some other location. They maintain database and applications for the users at some remote server and provide independence of accessing them from any place through a network. Clouds are of particular commercial interest not only with the growing tendency to outsource and extend existing, limited IT infrastructures.The data center environment allows enterprises to get their applications up and running faster, with easier manageability and less maintains to meet business demands.

Ex:Small phone.This save application and files of its users and it is also seen that main cost for a mobile phone of memory storage.
1. Virsatility. 2. Extremely Inexpensive. 3. On Demand service. 4. High reliability.
1. Virsatility**:**Different application running it at a same time. Its support variety of applications.
2. Extremely Inexpensive:It is a easy to use and lowest cost. It provides secure and dependable data. Its sharing between different equipment.3. On Demand service**:**It's a large resource poul that a user can buy according to they need a information.4. High reliability**:**User data tolerant to ensure the high reliability of the service.

Security threads and goals:

*Interception*Interruption*Modification*Fabrication**.**

- **Interception**:Some authorized party gained access to an asset. The outside party can be person, program and computing system. **Ex:**This type of failure are copying of program or data files or wiretapping to obtain data network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

- **Interruption:**This asset of the system becomes cost, unavailable or unusable. Is malicious destruction of a hardware device, erasure of a program or data file or malfunction of a operating system file manager it cannot find a particular disk file.
- **Modification**:Unauthorized party not only accesses but tampers with an asset,the threat is a modification.**Ex**:Some might change the values in a database, alter a program and it performs an additional computation and data being transmitted electanically.
- **Fabrication:**Un authorized party might create a fabrication of counterfeit objects on system. Additionally can be defected as forgeries but skillfully done and indistinguishable from the real things.
- **Blowfish:**Blowfish is a variable length a new secret-key block ciper.It is a fiestal network, iterating a simple encryption function 16times.The main features are,

Block cipher: 64 bit block.Variable key length: 32 bits to 488 bits.Much faster than IDEA and DES.No license required**.**

Description: This algorithm consists of two parts, they are

1. Key-expansion part 2. Data –expansion part.

1. Key-expansion part:

Key-expansion converts a variable –length key of at most 56byte (448bits) into several sub key arrays totaling 4168 bytes. Data encryption occur Via a 16round Festal network. Each round consists of key dependent permulation,key and data dependent substraction.The additional operations are 4 indexed array data lookups per round.

Blowfish require faster spends should unroll the loop and ensure that all sub keys are stored cache.

Encryption and decryption:

They p-array consists of 18 32-bit sub key.

Background study:

Cloud computing is associated with a new paradigram for the provision of computing infrastructure. Cloud computing provide software provide software, computation, data access and storage resources. Cloud computing is basically broken down into three segments.

1. Application 2. Storage 3. Connectivity.

II.RELATED WORK

Sno	Citation	Paper Name	According this paper
1.	B. A. Caprarescu and D. Petcu	A self-organizing feedback loop for autonomic computing	The Job Tracker thus strives to keep the jobs as close to the data as possible. With a rack-aware file system, if the work cannot be hosted on the actual node where the data resides.
2.	Ranjite Mishra	A privacy presenting repository for securing Data across the colud.	The facilitate data showing and integrating along with data conformations. This has been encrypting technique to data storage**.**
3.	Advanced in cloud security	Recent advance n cloud security**.**	Its present are user secured channel for communication**.**
4.	Gupta Chapin	The MapReduce programming model.	The most expensive in terms of I/O operations. In the last phase the reducer can finally apply the Reduce function and write the output

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

III. CONCLUSION AND FUTURE WORK

In this paper present an identify low efficiency for cloud services and user to identify based on hierarchical model for cloud computing(IBHMCC)and corresponding encryption and signature schemes.This aligned well with the idea of cloud computing to allow the users with an average to outsource their computational tasks to more powerful server. The main goal is to explore and analyse the different threats that virtualization and multi-tenancy combined bring to the Cloud. More specifically, the venues to compromise a hypervisor in a physical machine will be analyzed and recommendations will be given on how to mitigate the risk.The development of cloud computing technology is still at an early stage,we hope our work will provide a better understanding of the design challenges of cloud computing ,and pave the way for further research in this area.

REFERENCES

1.A. Casanova, H. Legrand and M. Quinson, Simgrid: a generic framework for large-scale distributedexperiments, 10th IEEE International Conference on Computer Modeling and Simulation,2012.
2. M. Caeiro-Rodriguez, Z. N´emeth, and T. Priol, A chemical workflow engine to support scientific workflows with dynamicity support, Proceedings of the 3rd Workshop on Workflows in Support of Large-Scale Science, IEEE, November 2008, to appear.
3. Purchasing and RDS Reserved Instance in EU-West by Andrew on August 18, 2010.
4. Cloud Computing: Paradigms and Technologies by Ahmed Shawish and Maria Salama on 2014.
5. Cloud Computing Security Issues and Challenges by Kuyoro S O on 2011.
6.J. Cao, D. P. Spooner, S. A. Jarvis, and G. R. Nudd, Grid load balancing using intelligentagents, Future 135–149. Jenson,Schwenk Bohali,"Security prospects through clud computing".
7."Recent Advanced in cloud security" by jiyiwu Qianlishen Tongwang.
8."A Privacy preserving Repository for Securing Data across the Cloud"by Ranjite mishra.
9.Cloud Computing Implementation, Management and Security by John W Rittinghouse and James F.Ransome on 2010.
10. Cloud Computing Security, Management and Security by John W Rittinghouse and James F.Ransome on 2010.