Volume 7, Issue 5, May 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Security Issues of Cloud Computing

[1]Eter Basar*
B.Tech Student, Department of CSE
Assam down Town University,
Assam, India

[2]Ankur Pan Saikia
Asst.Prof, Department of CSE
Assam down Town University,
Assam, India

[3]Dr. L. P. Saikia
Professor, Department of CSE
Assam down Town University,
Assam, India

Abstract*— To avoid the storage efficiency and portability Cloud Computing technique has been introduced which plays an important role in information technology. Cloud Computing is nothing but that technology by which we can handle data over the internet. The Cloud technique helps the users to freely access the data, platform and various applications over the internet. But security is the main problem associated with this technique since the user has no idea what the service provider will do with their data which may be somehow confidential to the user in case of public cloud which has been absolutely free. In this study we will analysis the security issues over the Cloud Computing based on public cloud.

Keywords*— Public Cloud, Encryption, RSA, DES, Blowfish

I. INTRODUCTION

A traditional Cloud in environment data's are moving around internet is known as Cloud Computing. It allows us to share resources information and platform for storing and retrieving data and programming.

1. Services in Cloud:

There are three basic services exist in Cloud Computing:

I. **Infrastructure as a Service (IaaS):** Infrastructure as a service refers to the uses of sharing the network or resources among the users community.
II. **Platform as a Service (PaaS):** Platform as a Service refers to the sharing of application and hardware via Cloud computing.
III. **Software as a Service (SaaS):**Software as a Service refers to the uses of the sharing the software applications and resources among the users.

Types of Cloud:

Three basic types of cloud:

a) Public cloud.
b) Private Cloud.
c) Hybrid Cloud.

a) Public Cloud:

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud is made available to general public by a service provider who host the cloud infrastructure. Generally public cloud providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access over the internet. With this model, customer has no visibility or control over where the infrastructure is located.

It is important to note that all customers on public clouds share the same infrastructure pool with limited configuration, security protections and availability variances.

b) Private cloud:

Private cloud is a cloud infrastructure dedicated to a particular organization. Private clouds allow business to host application in the cloud, while addressing concern regarding data security and control, which is often looking in a public cloud environment. It is shared with other organization, whether managed internally or by a third party and it can be hosted internally or externally.

c) Hybrid Cloud:

Hybrid cloud are composition of two or more clouds(Private, community or public) that remain unique entities but are bound together offering the advantages of multiple deployment models. In a hybrid cloud, you can leverage third party cloud provider in either a full or partial manner, increasing the flexibility of computing.

II. SECURITY IN CLOUD COMPUTING

Since most of the user use Public Cloud for their own benefits since it is free, hence in this study we will look over the security issues regarding with the Public Cloud.

To secure data two technologies has been used bythe users or the service provider

- Data Encryption
- Decryption

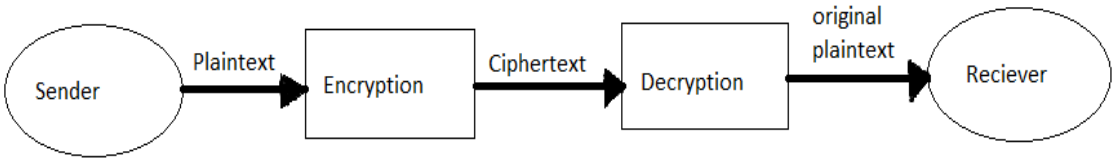

Fig.1: Basic Structure of Encryption and Decryption

Since Cloud is a distributed network, data distributed among the cloud user may be available to all unauthorized people. So to protect the data encryption technologies is used by user or service provider**. Encryption** means the translation of data (Plain text) into a secret code (cipher text). To convert the encrypted data into its original form **Decryption** technique is used. There are two main types of encryption **Asymmetric encryption** also called **public key encryption** and **Symmetric encryption.** Common asymmetric encryption algorithm is **RSA** algorithm**. RSA** is an algorithm used by modern computer to encrypt and decrypt messages, RSA stands for Ron-Rivest, Adi Shamir and Leonard Adleman, who publicly described it in 1978. Some advanced encryption algorithms which have been applied into the cloud computing to increase the protection. Attribute Based Encryption.

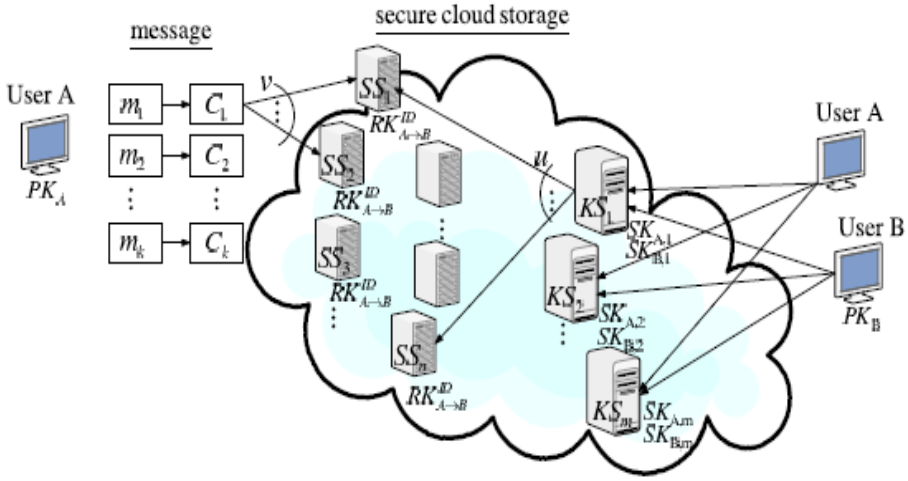

Fig.2: Cloud Computing Architecture

- **Cipher text-policy CP-ABE:**

In the CP-ABE, each user's private key (decryption key) is tied to a set of attributes representing that user's permission**.** When a cipher text is encrypted a set of attributes is designated for the encryption and only users are able to decrypt the cipher text if his attributes satisfy the policy of respective cipher texts

- **Key Policy ABE:**

In the KP-ABE, attribute sets are used to explain the encrypted texts and the private keys with the specified encrypted texts that users will have the left to decrypt.

- **Fully Homomorphic Encryption FHE:**

Fully Homomorphic encryption allows straightforward computations on encrypted information, and also allows computing sum and product for the encrypted data without decryption. To give the security users basically take the concept of public key and private key. **A public key** is known to everyone and a **private or secret key** known only to the recipient of the message. An important element to the public key system is that the public and private key are related in such a way that only the public key can be used encrypt message and only the corresponding private key can be used to decrypt them.

III. LITERATURE REVIEW

Many researchers proposed the equivalent system model and security model to work on security issue. Latest work was proposed by **Wang H. (2015)** which was an ID based RDPC approach for multi cloud storage.

In **2007**, provable data possession (PDP) paradigm was proposed by **Ateniese** et al. , where the verifier can check remote data integrity with a high probability. Based on the RSA technique, they provided two provably secure PDP schemes.

As a continuation, **Ateniese et al**. proposed dynamic PDP model and concrete scheme which failed in providing a support for insert operations. Taking this limitation in consideration, in **2009**, Erway et al. proposed a full-dynamic PDP scheme based on the authenticated flip table.F. Seb´e et al. did the similar work in . The central idea of PDP is it allows a verifier to verify the remote data integrity even with no retrieving or downloading the complete data. It is based on robabilistic proof of possession by sampling random set of blocks from the server, which reduces I/O costs considerably.

In some scenarios, the client can delegate the remote data integrity checking job to the third party which is commonly referred as the third party auditing in cloud computing .One of the profits of cloud storage is to enable global access to

data with location liberty. We have obtained the comparison on currently available PDP systems in along with rewards and Drawbacks of the schemes.

A brief description of various ciphers and modes of operations used by existing cryptographic file systems has been provided along with a detailed description of XEX-based Tweaked codebook mode with cipher text Stealing(XTS) **[IEEE (2008), Dworkin (2009)]** that can be used by cryptographic file systems for better performance. Then, existing cryptographic file systems at the block device level and at file system level in user-space and in kernel space are presented with their advantages and limitations. [**BlowFish**]

R.Biddle, S. Chiasson (2012) presents three type of graphical password. Recognition based Graphical password, cued recall graphical password, and recall based graphical password. In recall based graphical password user need to recall password without any cue, in recognition based graphical password user need to recognize password from the set of image, in cued recall graphical password some cue is provided to identify password from the image.[Graphical Password]

IV. CHALLENGES OF CLOUD COMPUTING

The cloud acts as a big black box, nothing inside the cloud is visible to the clients. Clients have no idea or control over what happens inside a cloud. Even if the cloud provider is honest, it can have malicious system admin's who can tamper with the VMs and violate confidentiality and integrity. Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks.

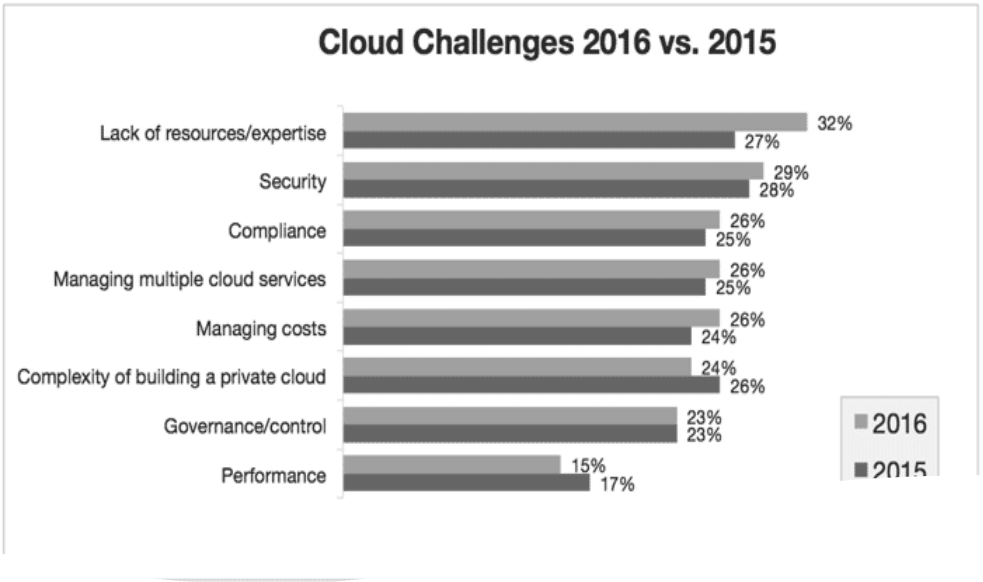

Fig3: Cloud challenges in 2016 vs 2015

Cause of the problem associated with Cloud Computing:

Most security problems stem from:

- Loss of control
- Lack of trust (mechanisms)
- Multi-tenancy

These problems exist mainly in 3rd party management models

- Self-managed clouds still have security issues, but not related to above

Password is the Most commonly used form of user authentication. It is used to prove identity or access approval to gain access to a resource. Two conflicting requirements of alphanumeric passwords-

- Easy to remember
- Hard to guess

Many people tend to ignore second requirement, which lead to weak passwords. So many solutions have been proposed one of them is graphical passwords.

Recall Based Techniques:

Pass points: user click on any place on the image to create password. In order to be authenticated user must click within the tolerances in correct sequence.

Password space: N^K

N= the number of pixels,

K= number of points to be clicked on

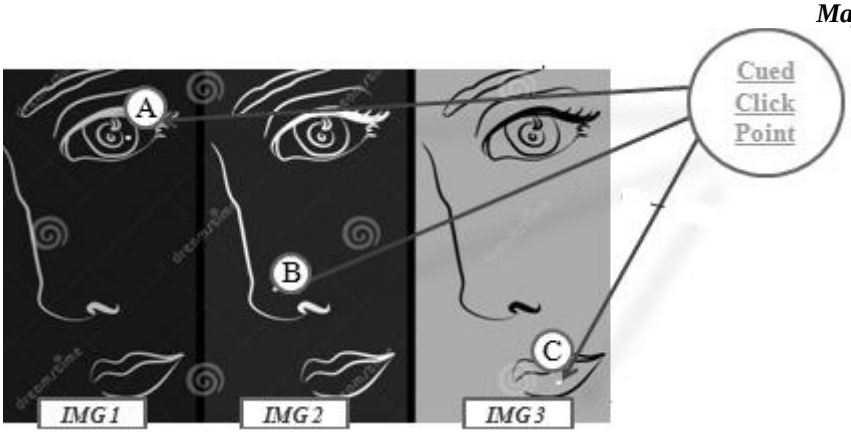

Fig.4: Cued Click Point Example

Cued Click point:

- User can select their images only to extent that their click point determines the next image, as it consist of different images, so it prevent guessing attacks.
- Remembering the order of click points is no longer the requirement of user.

Cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages.
Data integrity is the maintenance of, and the assurance of the accuracy and consistency of, data over its entire life-cycle and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

Blowfish Algorithm:

- Blowfish was designed in 1993 by Bruce Scheier as a fast, alternative to existing encryption algorithms.
- Blowfish is a symmetric block encryption algorithm designed in consideration with
  - Fast :it encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte
  - Compact: it can run in less than 5K of memory
  - Simple: it uses addition, XOR, lookup table with 32-bit operands
  - Secure: the key length is variable ,it can be in the range of 32~448 bits: default 128 bits key length
  - It is suitable for applications where the key does not change often, like communication link or an automatic file encryptor.
  - Unpatented and royalty-free.

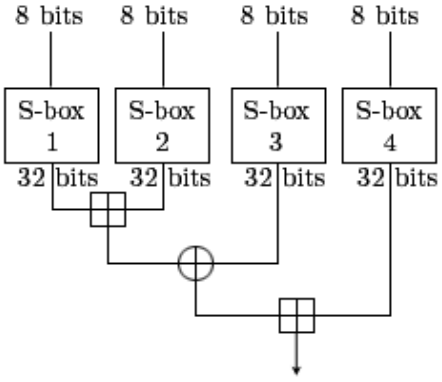

Fig.5: Function of Blowfish Algorithm

Functional and Non-functional Requirements for Cloud System:
Functional Requirement:

- Encryption
- Re-encryption
- Storage
- Decryption

Non Functional Requirement:

- Privacy
- Reliability
- Scalability
- Performance
- Security

V. CONCLUSION

Integrated a newly proposed threshold proxy re-encryption scheme and erasure codes over exponents. The threshold proxy Re-encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way. By using the threshold proxy re-encryption scheme, we present a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure. Key servers act as access nodes for providing a front-end layer such as a traditional file system interface.

REFERENCES

[1] M. Armbrust, *et al.*, "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems LaboratoryFebruary 10 2013.
[2] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing, ver. 2.1," 2014.
[3] M. Jensen, *et al.*, "On Technical Security Issues in Cloud Computing," presented at the 2009 IEEE International Conference on Cloud Computing, Bangalore, India 2009.
[4] P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm," ed: National Institute of Standards and Technology, Information Technology Laboratory, 2014.
[5] N. Santos, *et al.*, "Towards Trusted Cloud Computing," in *Usenix 09 Hot Cloud Workshop*, San Diego, CA, 2015.
[6] R. G. Lennon, *et al.*, "Best practices in cloud computing: designing for the cloud," presented at the Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications, Orlando, Florida, USA, 2009.
[7] P. Mell and T. Grance, "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology LaboratoryOctober 7 2009.
[8] C. Cachin, *et al.*, "Trusting the cloud," *SIGACT News*, vol. 40, pp. 81-86, 2015
[9] J. Heiser and M. Nicolett, "Assessing the Security Risks of Cloud Computing," Gartner 2016.
[10] A. Joch. (2009, June 18) Cloud Computing: Is It Secure Enough? *Federal Computer Week*.
[11] AWS Amazon EC2: http://aws.amazon.com/ec2/
[12] Amazon CloudWatch: http://aws.amazon.com/cloudwatch/
[13] Iperf: http://iperf.sourceforge.net/

