DPaaS with Secure Data Forwarding

Sajna.S
Assistant Professor, Dept of CSE,
YCET

***Abstract* — DPaas is an architecture with a suite of security primitives, enforcing data security and privacy which offers evidence of privacy to data owners. Data protection is needed for the data in transit and in rest as well. Cryptography is adopted to ensure data security in this model. Auditing and logging are other two main options in the architecture to ensure integrity and confidentiality of the user's sensitive data. As a part of the good service a service provider should also concern about the response time in data sharing. To improve the response time of the service a re-encryption scheme is adopted here.**

Keywords— Data Protection as a Service, Confidentiality, Integrity, Availability, Cryptography, Re encryption, RSA, AES.

I. INTRODUCTION

Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of computing resources like networks, servers, storage, applications, and services, released with minimal management effort or service provider interaction . It provides an undemanding and non-ineffectual solution for daily computing. The prevalent problem associated with cloud computing is the cloud security and the appropriate implementation of cloud over the network. Confidentially Integrity and Authenticity (CIA) are common security risk for Cloud computing.

Although Cloud computing is having so many promises, it is not chosen by everyone. A recent Microsoft survey[11] found that 58% of the public and 86% of business leaders are excited about the possibilities of cloud computing, but more than 90% of them are worried about security, availability, and privacy of their data as it rests in the cloud.

The cloud is like a big black box, nothing inside the cloud is visible to the clients. Clients have no idea or control over their data. Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity. Computing however suffers from various security issues in the application side and in the hardware components. Infrastructure Security, Data Security and Storage, Identity and Access Management (IAM), Privacy security are some of the main security issues in cloud computing.

Commonly, user data has been encrypted by using different encryption algorithms in order to protect data from intruders. This approach is also used in cloud computing environment. Data security doesn't only engross encrypting the data but also comprises on implementing and enforcing the appropriate policies for data sharing and as well as authenticating the user who required to access the data on cloud.

Security is one of the major problems faced by Cloud environment, this paper deals with providing a security model without compromising the performance of cloud environment. This framework contains different modules to improve the security and trust of key components of cloud. This model also improves the performance by focusing on the response time.

The remainder of this paper is organized as follows: Section 2 presents an overview of unique features of the cloud. Section 3 presents the security framework followed by components of the framework. Finally, Section 5 concludes the paper.

II. OVERVIEW OF CLOUD

Cloud Computing is purely a computing technology which is composed of several Strata of Services[5]. These include services like *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) and *Software as a Service* (SaaS).

A SaaS provider gives subscribers access to both resources and applications. It makes it unnecessary for you to have a physical copy of software to install on your devices. It also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, you have the least control over the cloud. In a PaaS system provider gives subscribers an access to the components that they require to develop and operate applications over the internet. And an IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software, which they need.

Regardless of the service model utilized there are four deployment models for cloud services- Public, Private, Community and Hybrid cloud. A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space and a private cloud is established for a specific group or organization and limits access to just that group. But in a community cloud, it is shared among two or more organizations that have similar cloud requirements. And in case of a hybrid cloud it is a combination of at least two clouds, where the clouds

included are a mixture of public, private, or community.

III. SECURITY IN CLOUD

When making decisions to adopt cloud services, privacy or security has always been a major issue. To deal with these issues, the cloud provider must build up sufficient controls to provide such level of security than the organization would have if the cloud were not used.

In Cloud Computing, service providers will have to provide the storage for data along with services. By focusing on service provider's side security, they must protect their client data by unauthorized access, modification or miss use, denial of services and repudiation.

Due to involvement of many technologies including networks, databases, operating systems, resource scheduling, transaction management, concurrency control and memory management ,various security issues arises in cloud computing. Ensure strong authentication and access controls are implemented in performance with secure transmission.

Cloud Computing however suffers from various security issues in the application side and in the hardware components. Infrastructure Security, Data Security and Storage, Identity and Access Management (IAM), Privacy security are some of the main security issues in cloud computing

Commonly, user data has been encrypted by using different encryption algorithms in order to protect data from intruders. This approach is also used in cloud computing environment. Data security doesn't only engross encrypting the data but also comprises on implementing and enforcing the appropriate policies for data sharing and as well as authenticating the user who required to access the data on cloud.

Cloud security is becoming a key differentiator and competitive edge between cloud providers. Privacy, security, latency, reliability, portability are some of the barriers to the security concerned to the cloud computing. Security issues for cloud computing encompasses data protection, communication, resource management for isolation, virtualization and memory management.

A. Cryptography for Data Security.

Cryptography is the science of securing data. It is using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Cryptography can be strong or weak. Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of strong cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. The security of encrypted data is entirely dependent on two things The strength of the cryptographic algorithm and The secrecy of the key.

Two main classifications of cryptographic algorithms:

- Conventional cryptography - also called secret-key or symmetric-key encryption, in which one key is used both for encryption and decryption.
  Eg: DES, AES, Caesar's cipher etc.
- Public key cryptography - is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption.
  Eg: RSA, DSA(Digital Signature Algorithm) etc.

Proxy re-encryption – A scheme in cryptosystems which allow third-parties (proxies) to alter a ciphertext which has been encrypted for one party, so that it may be decrypted by another.

Re encryption always aid double security in the cloud environment which ensures confidentiality and authenticity.

A cryptographic checksum is a mathematical value (called a checksum) that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously changed. Here checksum is created by performing a complicated series of mathematical operations (known as a cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as a checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum. Cryptographic checksums are used in data transmission and data storage. Cryptographic checksums are also known as message authentication codes, integrity check-values, modification detection codes, or message integrity codes. Check sum ensures the integrity of data.

IV. RELATED WORK

Currently there are many frameworks and security models proposed to ensure the security issues in cloud, among them Data security is having its own importance, since the users are putting their sensitive data into third party storage.

Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. Cryptography is always chosen as the successful remedy for the data security. Some of the existing encryption techniques are:

- Homomorphic Encryption, a method which is able to perform operations of encrypted data without decrypting them.
- Fully Homomorphic Encryption (FHE) and Full Disk Encryption (FDE) is a widely used one, fail to provide a practical solution in a cloud computing setup [1].

DPaaS[1] is an architecture with a suite of security primitives which is proposed as a solution for the existing data security issues and the lack of a technical solution. In this architecture Auditing and key management hold a place next to the cryptography. Auditing of the log details help to ensure the confidentiality.

V. PROPOSED SYSTEM

The proposed system can be classified as two sections- secure data storage and secure data forwarding.

The system concentrates on the security of both the data in transit and in rest.

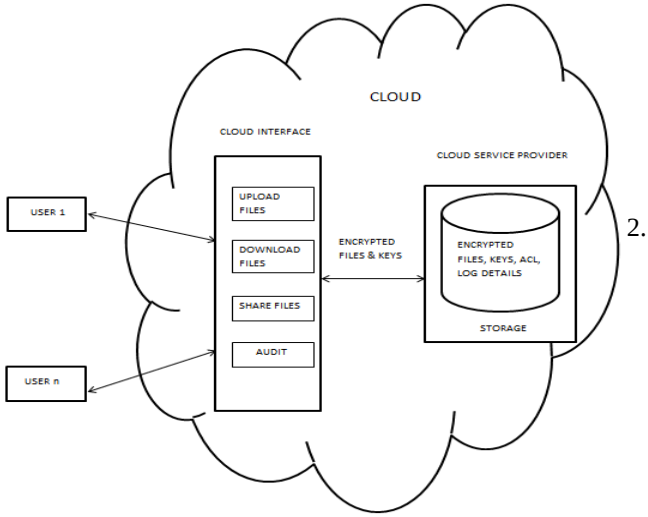

Fig. 1 DPaaS with Secure Data Forwarding Architecture

Here the aopted architecture is Data Protection as a service (DPaaS) which enforces data security and privacy which offers evidence of privacy to data owners. Cryptography is adopted to ensure data security. Auditing and logging are the two other main options in the architecture which is also aopted to ensure integrity and confidentiality.

Data sharing a main application of the cloud; almost all web interactions usually require the exchange of personal and confidential information for a variety of purposes. A key issue affecting these interactions is the lack of trust and control and the response time. Data and key are encrypted before it is taken to cloud and back to user; thereby ensure the data security in transit.

A. Secure Data Storage

Data Storage security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. Confinement of the user data is done by the Authentication and Encryption process. A combination of symmetric and asymmetric encryption algorithms are used in this system. AES and RSA are used for the encryption of data and key respectively. System offering the following actions:

In the system users can

- Upload the data to the cloud: Data uploaded is encrypted by using the AES algorithm with the key provided by the user. The AESkey is then encrypted by the public key algorithm RSA for taking it to the cloud. The cloud provider's public key is used for AESkey encryption and thereby ensure data security in transit and rest.
- Download data from the cloud: Requested data is downloaded by doing a combination of decryption and encryption process before coming to the user node.
- Audit the transactions: Users are allowed to audit the log details related to their data in the cloud thereby ensuring the integrity of data.

Existing system ensures almost all the data security issues.

2.

Encryption makes difficulty in sharing data. The algorithms used are:

A.1. RSA algorithm:

RSA algorithm involves three steps:

- Key generation
- Encryption
- Decryption

Key Generation Algorithm:

1. Choose a and b: two distinct prime numbers.
2. 2. Compute m = a b, Where m is used as the modulus for public and private keys.
3. Compute Φ (m) = (a-1)(b-1), Where Φ is totient function.
4. Choose an integer E such that, 1 < E < Φ (m) and common divisor of (E, Φ (m)) = 1.
5. Determine D = 1/E mod Φ (m).
6. All the above values of public key and private key must be kept secret.

Encryption Algorithm:

1. Sender A transmits her public key (m, E) to recipient B for the process of encryption data.
2. Represent the plaintext message as a positive integer n.
3. Computes the cipher c = nE (mod m).
4. Sends the cipher text c to recipient B.

Decryption Algorithm:

1. Recipient B uses private key (m, D) to compute n = cD (mod m).
2. Decrypt the plaintext from the message representative n.

A.2.AES Algorithm:

AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys Except for the last round in each case, all other rounds are identical.

Each round consists of the following steps.

1. Substitute bytes: called SubBytes for byte-by-byte substitution during the forward process. This step consists of using a 16 × 16 lookup table to find a replacement byte for a given byte in the input state array.
2. Shift rows: for shifting the rows of the state array during the forward process
3. Mix Columns: for mixing up of the bytes in each column separately during the forward process
4. Add Round Key: for adding the round key to the output of the previous step during the forward process.

•The Inverse process of Encryption gives Decryption text.

B. Secure Data Forwarding

Users can share their data in cloud to other users without downloading it and forwarding, thereby reducing the cost and time. This can be done by setting the ACL (Access control list) by the user which is maintained by the cloud.

In data sharing the integrity of the forwarded data is ensured by using the check sum of the message transmitted. When forwarding the data the checksum and the key is send simultaneously by re encrypting the data using the key pairs

IV. EXPERIMENTAL RESULTS

The proposed model is implemented in the real environment which is done after it is simulated in a cloud simulator. A cloud simulator consist of different packages helps to check whether the proposed model can be implemented in an actual cloud environment or not. The implementation proves that the data stored securely and sharing is done cost effectively in a secured path.

V. CONCLUSION

This paper is focused on the security and sharing of user data in cloud. This work helps to ensure the security issues like Confidentiality, Integrity and Authenticity in cloud computing by adopting Encryption and Decryption techniques. Here AES and RSA are used to provide security. Data sharing is also done in a secured path which reduces the cost and time of normal forwarding of data. Faster access to services and better performance of the environment is ensured to some extent. This paper proposed a framework which ensures security of data in transit and rest.

REFERENCES

[1] Cloud Data Protection for the Masses - Dawn Song, Elaine Shi, and Ian Fischer (University of California), Umesh Shankar (Google)[2012].

[2] General Survey on Massive Data Encryption - Mengmeng Wang , Guiliang Zhu (North China University of Water Resources and Electric Power Zhengzhou, China) Xiaoqaing Zhang(State Key Lab of Software Development Environment Beihang University Beijing, China).

[3] Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography - M Sudha and M Monica Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012.

[4] Evaluation and Comparison of Security Issues on Cloud Computing Environment - Priyanka Arora, Arun Singh , Himanshu Tyagi , Raj Kumar Goel World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.

[5] POSTER: A Certificateless Proxy Re-Encryption Scheme for Cloud-based Data Sharing-Xiaoxin Wuy, Lei Xuy, and Xinwen Zhangz CCS'11, October 17–21, 2011, Chicago, Illinois, USA.ACM 978-1-4503-0948-6/11/10.

[6] Security Issues in Cloud Computing: A survey - Rizwana Shaikh , M. Sasikumar International Journal of Computer Applications (0975 – 8887) Volume 44– No19, April 2012.

[7] Advanced encryption standard (AES) Federal Information Processing Standards Publication 197 November 26, 2001. enabled by Trusted Computing Technology, *2010 2ndInternational Conference on Signal Processing Systems (ICSPS).*

[8] Privacy and Security in Cloud Computing Allan A. Friedman and Darrell M. West. Issues in Technology Innovation, Number 3 October 2010.

[9] Qiang Wei, Konstantin Beznosov, "Cooperative Secondary Authorization Recycling", IEEE Transactions On Parallel And Distributed Systems, Vol. 20, No. 2, February 2009

[10] Rodrigo N. Calheiros, Rajiv Ranjan, César A. F. De Rose, and Rajkumar Buyya, "CloudSim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services", GRIDS Laboratory, The University of Melbourne, Australia

[11] C. Dwork, "The Differential Privacy Frontier Extended Abstract," Proc. 6th Theory of Cryptography Conf. (TCC 09), LNCS 5444, Springer, 2009, pp. 496-502.