SURVEY ON CONFIDENTIALITY IN CLOUD COMPUTING

Dave Dishita A, Mr. Rikin Thakkar

I. INTRODUCTION

Cloud Computing is becoming next stage platform in the evolution of the internet. It provides the customer an enhanced and efficient way to store data in the cloud with different range of capabilities and applications. The data in the cloud is stored by the service provider. Service provider capable and having a technique to protect their client data to ensure security and to prevent the data from discloser by unauthorized users.

Cloud Computing provides the way to share distributed resources and services that belong to different organizations or sites. Since Cloud Computing share distributed resources via network in the open environment thus it makes security problems. All types of users who require the secure transmission or storage of data in any kind of media or network. Since the data transmission on the internet or over any networks are vulnerable to the hackers attack. We are in great need of encrypting the data. I propose a method to build a trusted computing environment for Cloud Computing system by providing Secure cross platform in to Cloud Computing system. In this method some important security services including authentication, encryption and decryption and compression are provided in Cloud Computing system. The need for this software can be categorized in two categories: Encryption and Decryption, Compression.

Internet, it is a large collection of networks where resources are globally networked, In internet cloud computing plays a major role In order to share the data and one of the important technology in the cloud computing is virtualization. Mainly it is used to maintain the collection IT resources which are used by the cloud providers. The main aim of the virtualization is ability to run the multiple operating systems on a single machine buy sharing all the resources that belong to the hard ware. cloud computing promises lower costs,rapid scaling, easier maintenance, and service availability anywhere, anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely.

II. THREE TYPES OF CLOUD

1. PUBLIC CLOUD
2. PRIVATE CLOUD
3. COMMUNITY CLOUD
4. HYBRIDE CLOUD

cloud computing is classified into private clouds, public clouds, and hybrid clouds. Public clouds provide shared services through large-scale data centers that host a very large number of servers and storage systems.

III. PUBLIC CLOUD

The purpose of a public cloud is to sell IT capacity based on open market offerings.

Public clouds are the latest evolution of computing, offering tremendous value to businesses in terms of better economics, agility, rapid elasticity, etc. The public cloud infrastructure is operated by a cloud service provider and the services are offered over the internet. This very nature of public clouds offers various advantages such as better ROI and faster time to market, while also raising concerns about lack of visibility, security, reliability, etc. Public clouds are well suited to meet the collaborative needs of today's global workforce distributed across different geographies and time zones. A cloud infrastructure is provided to many customers and is managed by a third party and exist beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted

and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Examples of a public cloud includes Microsoft Azure, Google App Engine.

IV. PRIVATE CLOUD

The purpose of private clouds is to provide local users with a flexible and agile private infrastructure to run workloads within their own administrative domain. Due to the resource limitation in the private cloud, it is hard for the private cloud to provide services which can fit the user's SLA. Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider . This uses the concept of virtualization of machines, and is a proprietary network. Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems.

V. COMMUNITY CLOUD

Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider. Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a Community Cloud includes Facebook

VI. HYBRID CLOUD

The hybrid cloud can provide public computing resource to the user, while retaining the performance advantages of a private cloud and control effectiveness. It is necessary to create system architecture of hybrid clouds, propose an effective mechanism for public and private clouds at the same time. Hybrid cloud computing has receiving increasing attention recently, several research works has been launched in this area. A complete hybrid cloud platform includes a number of private cloud platform, a large number of independent users. and public cloud platform. In private cloud platform of hybrid cloud, the users' requests will be processed by own cloud platform if the platform could allocate the appropriate resources for the requests. Otherwise, the private cloud will send requests to public cloud for extra resources. Private cloud platform and public cloud platform are connected together as a star topology through the network. A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services [5]. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds. which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

security of a private cloud and the functionality and cost savings of a public cloud. More precisely, such a service should provide (at least):

- **confidentiality**: the cloud storage provider does not learn any information about customer data.
- **integrity**: any unauthorized modication of customer data by the cloud storage provider can be detected by the customer.

while retaining the main benets of a public storage service:

- **availability**: customer data is accessible from any machine and at all times
- **reliability**: customer data is reliably backed up
- **efficient retrieval:** data retrieval times are comparable to a public cloud storage service
- **data sharing:** customers can share their data with trusted parties.

VII. CLOUD SERVICES

Cloud computing can be classified based on the services offered and deployment models. According to the different types of services offered, cloud computing can be considere to consist of three layers. Infrastructure as a Service (IaaS) is the lowest layer that provides basic infrastructure support service. Platform as a Service (PaaS) layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications. Software as aService (SaaS) is the topmost layer which features a complete application offered as service on demand.

IaaS (Infrastructure as a Service) - Shared infrastructure such as servers, storage and network are delivered as a service over the internet. Some examples include Amazon Web Services, Rackspace Cloud, etc. IaaS offers the most control to the users and generally the least security from the service provider. The users are expected to be responsible for ensuring the security of their cloud infrastructure as well as the applications built on top of them. Infrastructure as a Service is an equipment which is used to support hardware, software, storage, servers and mainly used for delivering software application environments. It is totally depend on pricing model i.e. pays on as per use basis.

IaaS companies provide off line server, storage and networking hardware as per rent basis and can be access over the Internet. So it becomes easier to get access to run their applications on this hardware anytime without wasting office space. Some of the example of IaaS are Amazon, Microsoft, VMWare and Red Hat.

PaaS (Platform as a Service) - Application development framework offered as a service to developers for quick deployment of their code. Some examples for PaaS include Google App Engine, Heroku, Cloud Foundry, etc. PaaS offers no control over the underlying infrastructure while offering some control over the applications and its configuration. While the provider takes care of the security of the underlying infrastructure, the developer is responsible for application security. Platform as a Service provides a high level environment to design, build, test deploy and update online cloud applications. Paas is a paradigm which mainly deals for delivering operating systems and other services over the internet. In Paas there is no need of downloading or installation of hardware, operating systems over the internet. This saves customers money on purchasing of hardware. PaaS provides solutions for developing as well as deploying applications over the internet such as operating systems and virtualised servers.

Application design, web application Management, storage, security etc are all comes under this category. Today the biggest PaaS providers are Google App Engine, Salesforce‟s Force.com, the Salesforce owned Heroko and Engine Yard.

PaaS provides infrastructure to customer on which software developers can build new applications, software without investing money for managing hardware and software. This would help user for developing his own solutions.

Characteristics of PaaS:

 No need of downloading and installing operating System
 It saves Customers money
 It mainly deals for delivering operating systems over Internet
 Software can be developed, tested and deployed

SaaS (Software as a Service) - Application software offered as a service using a multitenant
model which can be consumed using web browsers. Some examples are Gmail,
Salesforce, etc. With SaaS solutions, service providers are responsible for security
because they control the infrastructure and applications. However, because service
providers retain control, SaaS offers the customer very little visibility and customizability
over the infrastructure underneath or even application configuration.

Software as a Service is nothing but a software distribution model which are made available to customers over a network such as server or Internet . The application of SaaS are hosted by Service Providers. Saas is an interface between cloud applications and customers to offer them on demand network. Even Saas can be provided many times fee based access to the software through web browsers. IT managers and its license holder users required Software as a Service in which they pay as per their uses.

Cloud Service Providers can update their software or cloud applications without user. Because all cloud software resides on servers. Cloud Service Provider has a high administrative authority to control on application and is responsible for update, maintenance and security. The example of SaaS are Google Apps, Cisco‟s WebEx, Salesforce CRM.

As SaaS is available to the user as and when required. Hence it is also known as “Software on demand”. Through SaaS its become possible to access from any location, rapid scalability, high security. SaaS is one of the oldest and mature domain of cloud computing.

Characteristics of SaaS:

 Its easy to work under administration
 It can be globally access
 The software can be updated automatically
 All license holder user will have same version of software

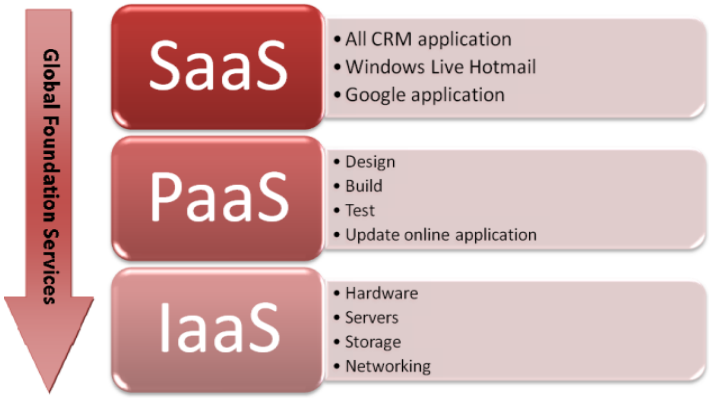

Fig. Cloud Environment

Deployment of cryptoanalysis methods in cloud computing :

Different encryption methods applied to cloud computing will be discussed briefly. With growing communication networks and digital communication, secure communication and data security is of paramount importance. Today one way to achieve secure communication is by the use of cryptography [1], [2], which concurrently ensures confidentiality of data in communication and in storage. For storing and accessing data securely there exist many ways which can guarantee privacy and confidentiality, such as data encryption and tamper resistance hardware. However, the problem becomes quite complex when it is required to compute publicly private data or to modify a function or algorithm in such a way that they are still executable while their privacy is ensured.

VIII. ENCRYPTION AND DECRYPTION

Encryption is the conversion of data into a form, called a ciphertext that cannot
be easily understood by unauthorized people and decryption is the process of converting
encrypted data back into its original form,so that the authorized recipient can understand it.

According to Kerckoffs’ principle [6], [7], security must rely upon the secrecy of the scheme, but
not on the obfuscation of the code. A cryptography scheme is assumed to be publically known
whereas the secret piece of information such as key is responsible for the secrecy of the scheme.

According to key management, encryption schemes are of two types: Symmetric and
Asymmetric encryption schemes.

Symmetric Encryption

An encryption system in which the sender and receiver of a message share a
single, common key that is used to encrypt and decrypt the message is called as Symmetric
Encryption. Symmetric-key systems are faster, but their main drawback is that two parties
wishing to communicate have to exchange the key in a secure way. In addition, scalability is
problem as the number of users increase in the network. Due to its secret nature, symmetric-key
cryptography is sometimes referred as secret-key cryptography.

Asymmetric Encryption

An encryption scheme is called asymmetric encryption if it uses two keys instead of one key as in symmetric encryption. One key encrypts the data and the other decrypts. It is also changeably referred to as public key cryptography. An important element of the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only its corresponding private key can be used to decrypt them.Moreover, it is virtually impossible to deduce the private key even if the public key is known.Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman [1],[2] and the scheme was called Diffie-Hellman encryption. Security of this type of scheme is based on hard problems in mathematics, which are difficult to solve in polynomial time. However, the downside is that they are slower than the symmetric schemes due to non-trivial mathematical computations. That is why this encryption scheme is used only for encryption of small data or keys while symmetric scheme can be used for larger ones.

Encryption Methods for Data Security In Cloud :

Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval. The following three papers analyze the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage.

Implementing DES Algorithm in Cloud for Data Security:

Research paper [6] described Data security system implemented into cloud computing using DES algorithm. This Cipher Block Chaining system is to be secure for clients and server.The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. There is no danger of any data sent within
the system being intercepted, and replaced. The system with encryption is acceptably secure, but
that the level of encryption has to be stepped up, as computing power increases. The algorithm
steps are follows.

1. Get the Plaintext.
2. Get the Password.
3. Convert the Characters into binary form.
4. Derive the Leaders (L1 to L16) from the Password.
5. Apply the Formula to get the encrypted and decrypted message.

In order to secure the system the communication between modules is encrypted using symmetric key. Though many solutions have been proposed earlier many of them only consider one side of security; the author proposed that the cloud data security must be considered to analyze the data security risk, the data security requirements, deployment of security functions and the data security process through encryption. The main contribution of this paper is the new view of data security solution with encryption, which is the important and can be used as reference for designing the complete security solution.

Data Security in Cloud computing using RSA Algorithm:

In research paper [12] have proposed a method by implementing RSA algorithm to ensure the security of data in cloud computing. RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. The purpose of securing data, unauthorized access does not allow. User data is encrypted first and thenit is stored in the Cloud. When required, user places a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In the Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud

service provider anddecryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

Homomorphic Encryption Applied to the Cloud Computing Security :

Maha TEBAA et al [10] have proposed an application of a method to execute operations on encrypted data without decrypting them which will provide the same results after calculations as if the authors have worked directly on the raw data. Homomorphic Encryption systems are used to perform operations on encrypted data without kno wing the private key (without decryption), the client is the only holder of the secret key. When the author decrypts the result of any operation, it is the same as if they had carried out the calculation on the raw data.In this paper cloud computing security based on fully Homomorphic encryption, is a new concept of security which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, with respect of the data confidentiality. The author work is based on the application of fully Homomorphic encryption to the Cloud Computing security considering: The analyze and the improvement of the existing cryptosystems to allow servers to perform various operations requested by the client. The improvement of the complexity of the Homomorphic encryption algorithms and compare the response time of the requests to the length of the public key.

Definition:

An encryption is homomorphic, if: fromEnc(a) and Enc(b) it is possible to compute Enc(f (a, b)),where f can be: +, ×, ⊕ and without using the private key.Among the Homomorphic encryption we distinguish,according to the operations that allows to assess on raw data, the additive Homomorphic encryption (only additions of the raw data) is the Pailler [2] and Goldwasser-Micalli [3] cryptosystems, and the multiplicative Homomorphic encryption (only products on raw data) is the RSA [4] and El Gamal [5] cryptosystems.

How does it work?

Homomorphic encryption allows complex mathematical operations to be performed on encrypted data without revealing the contents of the original plain data.For plain texts P1 and P2 and corresponding ciphertext C1 and C2,a homomorphic encryption scheme permits meaningful computation of P1 Θ P2 from C1 and C2 without revealing P1 or P2.The cryptosystem is additive or multiplicative homomorphic depending upon the operation Θ which can be addition or multiplication.

Some Applications of Homomorphic Encryption Schemes :

- Protection of mobile agents
- Secret sharing scheme
- Zero-knowledge proofs

A homomorphic encryption scheme consists of the following four algorithms [3]:
RSA :

1. **ElGamal**
2. **Goldwasser-Micali**
3. **Benaloh**
4. **Paillier**

Characteristics	***DES Algorithm***	***RSA Algorithm***	***Homomorphic Encryption***	***elgmal Algorithm***	***Paillier Algorithm***
Platform	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing	Not Cloud Computing
Keys Used	Same key is Used for encryption and decryption Purpose.	Different keys Are used for Encryption and decryption Purpose.	private key is used(without decryption)	private key is used(without decryption)	private key is used(without decryption)
Scalability	It is scalable Algorithm due To varying the Key size and Block size.	Not scalable	Scalable decryption	Scalable decryption	Scalable decryption
Security applied to	Both providers And client side	Client side Only	Cloud providers only	Cloud providers only	Client side Only
Authentication Type	Message authentication used	Robust Authentication implemented	Authentication never used	Authentication never used	Authentication never used