Securing Data as a Storage (DaaS) In Cloud through Homomorphic Encryption

Ramanaiah Pade[1], Dr. Venkata Ramana[2]
[1]*Student, Master of Computer Applications, KMM Institute of Post Graduate Studies, Tirupati*
[2]*Associate Professor, Master of Computer Applications, KMM Institute of Post Graduate Studies, Tirupati*

***Abstract*—Go to the cloud, has dependably been the fantasy of man. Distributed computing offers various advantages and administrations to its clients who pay the utilization of equipment and programming assets (servers facilitated in server farms, applications, software...) on request which they can get to through web without the need of costly PCs or a vast stockpiling framework limit and without paying any gear upkeep expenses. Be that as it may, these cloud suppliers must give ensures on the insurance of protection and touchy information put away in their server farms shared between different customers utilizing the idea of virtualization.**

I. INTRODUCTION

Distributed computing has risen as a critical worldview that has pulled in significant consideration in both industry and the scholarly world. Distributed computing as of now existed under various names like "outsourcing" and "server facilitating." But the poor execution of processors utilized, moderate Internet associations and the excessive expenses of the materials utilized, don't permit the utilization of administrations and storage rooms. Be that as it may, late advances in current innovation (through virtualization) prepared for these tasks with quicker handling.

Distributed computing security difficulties and it's additionally an issue to numerous specialists; first need was to center around security which is the greatest worry of associations that are thinking about a move to the cloud. The utilization of distributed computing brings a great deal of points of interest including decreased costs, simple upkeep and provisioning of assets. The principal genuine utilization of the idea of distributed computing was in 2002 by wither their VM occurrences run. It is up to the cloud supplier to ensure the hidden physical machines (PMs) have adequate assets to address their issues. VM live movement innovation rolls out it conceivable to improvement the mapping amongst VMs and PMs While applications are running. The limit of PMs can likewise be heterogeneous in light of the fact that numerous eras of equipment exist together in a server farm.

The virtualization is all the specialized material and additionally programming that can keep running on a solitary machine numerous working frameworks as well as different applications, independently from each other, as though they were dealing with partitioned physical machines. Virtualization and solidification can streamline the administration of the server's stop, by decreasing the quantity of machines to be kept up by advancing the utilization of assets and empowering high accessibility. However, the reception and the entry to the Cloud Computing applies just if the security is guaranteed. How to insurance a superior information security and furthermore how might we keep the customer private data secret? There are two noteworthy inquiries that present a test to Cloud Computing suppliers.

1. Different Types of Services Provide by the Cloud:

Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.

Third-party clouds enable organizations to focus on their core businesses instead of expending resources on computer infrastructure and maintenance.[7]

Advocates note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to meet fluctuating and unpredictable demand.[7][8][9] Cloud providers typically use a "pay-as-you-go" model, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models.[10]

Since the launch of Amazon EC2 in 2006, the availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing has led to growth in cloud computing.[11][12][13].

1.1 Software as a Service (SaaS):

The traditional model of software distribution, in which software is purchased for and installed on personal computers, is sometimes referred to as Software-as-a-Product. Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Mean-while, broadband service has become increasingly available to support user access from more areas around the world. Examples are Google's Gmail and Apps, instant messaging from AOL, Yahoo and Google.

1.2 Platform as a Service (PaaS):

Cloud computing has evolved to include platforms for building and running custom web-based applications, a concept known as Platform-as-a-Service. PaaS is an outgrowth of the SaaS application delivery model. The PaaS model makes all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet, all with no software downloads or installation for developers, IT managers, or end users. Examples include Microsoft's Azure and Salesforce's Force.com.

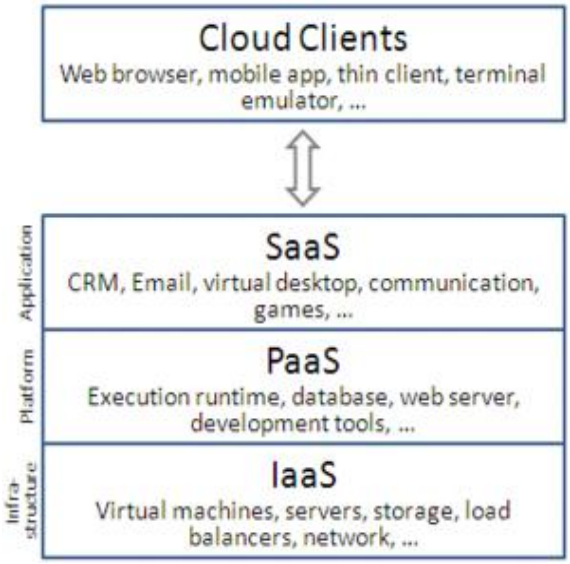

Figure 1. Different Types of Cloud Services

1.3 Infrastructure as a Service (IaaS):

The capability provided to the consumer is the provision of grids or clusters or virtualized servers, processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems. The highest profile example is Amazon's Elastic Compute Cloud (EC2) and Simple Storage Service, but IBM and there traditional IT vendors are also offering services, as is telecom-and-more provider Verizon Business.

II. PREVIOUS WORK

2. Security Issues For Cloud Computing:

2.1 Security Issue In Saas:

The meaning of distributed computing that we specified in the past segment doesn't say any security idea of the information put away in the Cloud Computing notwithstanding being a current definition. In this way we comprehend that the Cloud Computing is deficient with regards to security, privacy and deceivability. To Provide Infrastructure (IaaS), Platform Service (PaaS) or Software (SaaS) as a Service isn't adequate if the Cloud supplier does not surety a superior security and classification of client's information.

By tradition, we consider as Cloud Computing any treatment or capacity of individual or expert data which are acknowledged outside the concerned

structure (i.e outside the organization), to secure the Cloud implies secure the medicines (computations) and capacity (databases facilitated by the Cloud supplier).
Cloud suppliers, for example, IBM, Google and Amazon utilize the virtualization on their Cloud stage and on a similar server can exist together a virtualized stockpiling and treatment space that have a place with simultaneous undertakings.

2.2 Security Issues In Paas:
Heterogeneous hardware and software resources are unified for efficient use in cloud environments. Heterogeneity may cause flaws as security settings may differ for different kinds of resources [20]. Information leakage is another problem caused by shared resources as each shared resource is actually a communication channel [15], [18]. Finally, protection of user objects stands as the most serious problem of PaaS clouds.

2.2.1 Lack of Interoperability: Diverse computational resources may lead to security breaches if objects' access to the resources cannot be handled in a standard way. This may cause a set of resources to halt or a setting that is proven to be secure for a specific resource to be a breach for another. A simple example is a security breach that is caused by different case sensitivity defaults. A person who is authorized for a file named "file" can gain access to a secret file named "FILE" by mistake.
Interoperability can be maintained by providing common interfaces to objects for resource access. Resource interfaces must be designed carefully to support all possible access scenarios.

2.2.2 Vulnerable Hosts: Multi-tenancy has been studied since the earliest multi-user operating systems [17]. Today, the concept covers a wider perspective where the user objects are spread over interconnected multi-user hosts. Not only objects but also hosts must be protected from possible attacks in a multi-tenant environment. Such a protection can be achieved by evaluating resource access requests of every single object on the host. If the security of a host is breached, an attacker can access the host's resources as well as all of its tenant objects. Therefore, protection against third parties is also a necessity for the host. Taking the essential network security measures is the responsibility of the provider.

2.2.3 Vulnerable Objects: The security of an object can be breached in one of the following three ways in PaaS clouds. First, service provider may access any user object that reside on its hosts. Second, users may mutually attack each other's objects that are the tenants of the same host. Finally, a third party may directly attack a user object. Service provider access to the objects is natural and it is required for the most basic function of a cloud: executing an object. An object is eventually executed unless it is put into the cloud just to be stored.

2.3 Iaas Security Issues:
Most administrators will be agreeable and acquainted with IaaS since it is like work that we do in data centers. We save money on energy taken by conveying server solidification intend to diminish physical server impression in data centers. After server unification, cloud highlights like – self-benefit, computerization is utilized. In any case, before these elements are really utilized, different security suggestions of IaaS should be considered. Security issues are fluctuated relying upon whether we utilize open cloud or private cloud execution of IaaS. With private cloud, we have control over arrangements through and through. With IaaS out in the open cloud, we control VMs and administrations running on VMs. For both situations, we consider the following security issues:

2.3.1 Data Leakage Protection and Usage Monitoring: Data stores in IaaS in both private and public clouds needs to be monitored. The monitoring of IaaS Cloud is essential when it is deployed in public cloud, because it should be important to know that who and how the information is accessed and what happened to accessed information later. These problems can be solved by using modern Rights Management services applying restriction to business data and also there are certain new policies that are need to be created and deployed.

2.3.2 End To End Logging And Reporting This is very important because the deployment of IaaS needs comprehensive logging and reporting from where client is logging into keep track of where the information is, who accesses it, which machines are handling it and which storage arrays are responsible for it the logging must be robust.

2.3.3 Authentication and Authorization For getting effective data Loss Prevention Solution The authentication and authorization policies must be robust. For every application, just user name and password is not secure authentication mechanism. We need to consider tiering access policies based on level of trust.

2.3.4 Infrastructure Hardening VM and VM layouts should be solidified and cleaned. This should be possible while pictures are made. On general premise, testing of these ace pictures should be finished.

2.3.5 End To End Encryption Iaas as a Service, both out in the open and private Cloud, needs to exploit encryption from end-to-end. We can make utilization of entire plate encryption to encode every one of the information including client documents on the circle. This avoids disconnected assaults. In expansion to plate encryption, all correspondences to have OS and VMs in the IaaS foundation are encoded. This should be possible over SSL/TLS or IPsec.

III. PROPOSED SYSTEM

3. Homomorphic Encryption:

Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. In mathematics, homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets. The term is derived from the Greek words for "same structure." Because the data in a homomorphic encryption scheme retains the same structure, identical mathematical operations -- whether they are performed on encrypted or decrypted data -- will yield equivalent results.

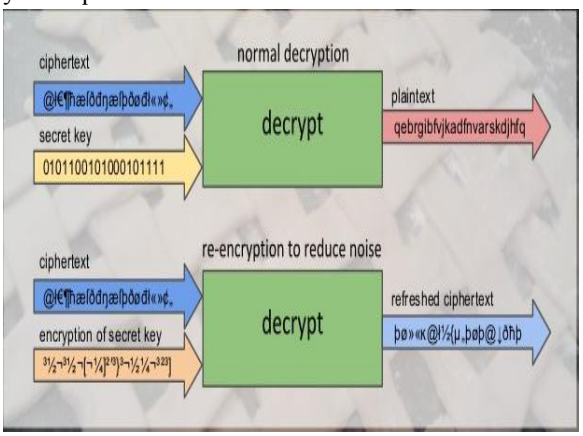

Figure 2. Sample Data Encryption Using Homomorphic

Technique Homomorphic encryption is expected toplayan important part in cloud computing, allowing companies to store encrypted data in a public cloud and keadvantage of the cloud provider's analytic services.

3.1 Homomorphic Encryption Applied To Cloud Computing Security

At the point when the information exchanged to the Cloud we utilize standard encryption techniques to secure the activities and the capacity of the information. Our essential idea was to scramble the information before send it to the Cloud supplier.

Be that as it may, the last one needs to decode information at each activity. The customer should give the private key to the server (Cloud supplier) to unscramble information before execute the counts required, which may influence the classification and protection of information put away in the Cloud.

In this paper we are proposing an utilization of a technique to execute tasks on encoded information without decoding them, which will give an indistinguishable outcomes after computations from in the event that we have worked straightforwardly on the crude information.

Homomorphic Encryption frameworks are utilized to perform activities on encoded information without knowing the private key (without unscrambling), the customer is the main holder of the mystery key. When we decode the consequence of any activity, it is the same as though we had completed the count on the crude information.

In abstract algebra, a homomorphism is a structure-preserving map between two algebraic structures, such as groups. A group is a set, G, together with an operation ı (called the group law of G) that combines any two elements a and b to form another element, denoted a ı b. To qualify as a group, the set and operation, (G; ı), must satisfy four requirements known as the group axioms:

- E_k is an encryption algorithm with key k.
- D_k is a decryption algorithm.

Let n=pq where p and q are primes. Pick a and b such that ab=1(mod Φ (n)). n and b are public while p,q and a are private.

$$e_k(X) = X^b \bmod n$$

The first property is called additive homomorphic encryption, and the second is multiplicative homomorphic encryption. An algorithm is fully homomorphic if both properties are satisfied simultaneously.

3.2 Multiplicative Homomorphic Encryption (Rsa Cryptosystem):

Several partially Homomorphic encryption schemes have been developed already. Implementations of these schemes have even performed well enough to find applications in systems today, such as anonymous voting systems [5].

The Homomorphism: Suppose x1 and x2 are plaintexts. Then, ek(x1) ek(x2) = x1b x2b mod n = (x1 x2)b mod n = ek (x1 x2)

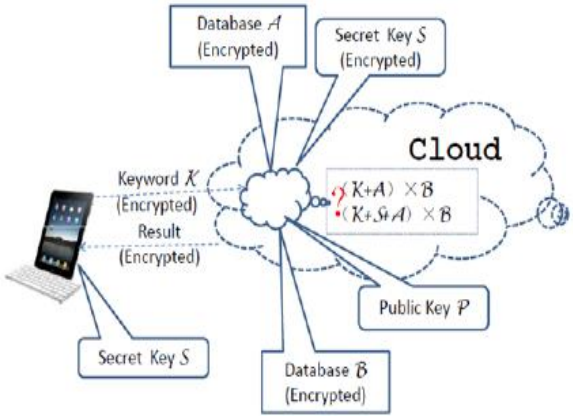

Figure 3. Multiplicative Homomorphic Encryption Applied to Cloud Computing

3.3 Additive Homomorphic Encryption (Paillier Cryptosystem):

Pick two large primes p and q and let n=pq. Let λ denote the Carmichael function. That is, λ (n) =LCM (p-1, q-1). Pick random $g \epsilon Z^{k}{}_{n}{}^{2}$ such that L ($g^{\lambda} \bmod n^2$) is invertible modulo n (where L(u)=(u-1)/n). N and g are public; p and q (or λ) are private. For plaintext X and resulting cipher text y. Select a random $r \epsilon Z^{k}{}_{n}{}^{2;}$ Then

$$e_k(x,r)= g^x \ r^n \bmod n^2$$
$$d_k(y)= (L(y^{\lambda} \bmod n^2)/ L(g^{\lambda} \bmod n^2)) \bmod n$$

• Multiplicatively homomorphic: RSA.
c1 = m e 1 mod N
c2 = m e 2 mod N
⇒ c1 · c2 = (m1 · m2) e mod N
• Multiplicatively homomorphic: RSA.
c1 = m e 1 mod N
c2 = m e 2 mod N
⇒ c1 · c2 = (m1 · m2) e mod N
• Additively homomorphic: Paillier
c1 = g m1 mod N 2
c2 = g m2 mod N 2
⇒ c1 · c2 = g m1+m2 [N] mod N 2
• Fully homomorphic: homomorphic for both addition and multiplication.

To perform addition and multiplication on encrypted data stored in the cloud provider, the client must have two different key generators (one for RSA and one for Paillier). We present in what follows the El Gamal cryptosystem that is basically a multiplicative homomorphic cryptosystem but by modifying coding mode we can make it additive.

IV. SIMULATION/EXPERIMENTAL

In this paper we are using homomorphic encryption. By using this algorithm we can store the files very securely. We can generate multiple keys for every user.

By using following method
c1 = m e 1 mod N
c2 = m e 2 mod N
⇒ c1 · c2 = (m1 · m2) e mod N

After the user will login and the user will shows the files based on their key.

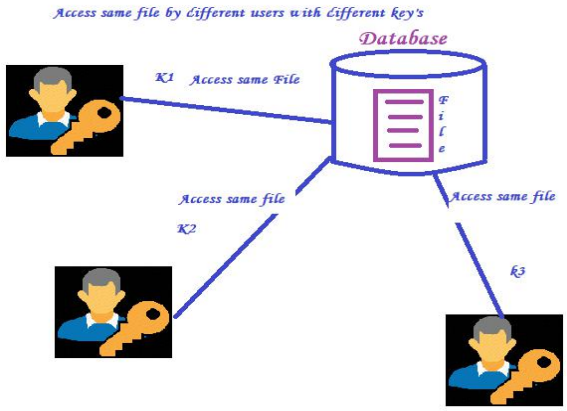

Figure 4. Multiple Users can Access a Same File by using Different Key's

They are ones where mathematical operations on the cipher text have regular effects on the plaintext. A very simple demonstration of the mathematical consistency required: with respect to multiplication

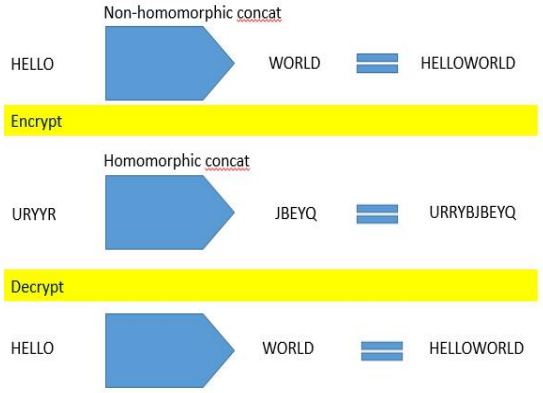

Figure 5. Example for Difference between normal encryption and Homomorphic encryption.

At first, the notion of processing data without having access to it may seem paradoxical, even logically impossible. To convince you that there is no fallacy, and to give you some intuition about the solution, let us consider an analogous problem in the physical world. Site owns a jewelry store. She has raw precious materials gold, diamonds, silver, etc. She wants her workers to assemble into intricately designed rings and necklaces.

But she distrusts her workers and assumes that they will steal her jewels if given the opportunity. In other words, she wants her workers to process the materials into finished pieces, without giving them access to the materials. For that she uses a transparent impenetrable glove box, secured by a lock for which only she has the key. She puts the raw precious materials inside the box, locks it, and gives it to a worker. Using the gloves, the worker assembles the ring or necklace inside the box.

Since the box is impenetrable, the worker cannot get to the precious materials, and ures he might as well return the box to Sita, with the finished piece inside. Sita unlocks the box with her key and extracts the ring or necklace. In short, the worker processes the raw materials into a finished piece, without having true access to the materials. Of course, Sita's jewelry store is only an analogy.

V. CONCLUSION

The Security of Cloud Computing based on fully Homomorphic Encryption is a new concept of security which is enable to provide the results of calculations on encrypted data without knowing the raw entries on which the calculation was carried out respecting the confidentiality of data. This paper analyzes the application of different Homomorphic Encryption cryptosystems on a Cloud Computing platform. They are compared based on four characteristics; Homomorphic Encryption type, Privacy of data, Security applied to and keys used. In future, we are going to analyses the behavior of Homomorphic Encryption cryptosystems compared to the length of the public key and the time of the treatment of the request by the Cloud provider depending on the size of the encrypted messages.

REFERENCES

[1] Sean Marston and al. “Cloud computing — The business perspective”, Volume 51, Issue 1, Pages 176–189, http://www.sciencedirect.com, April 2011.

[2] Nivedita Manohar, “A Survey of Virtualization Techniques in Cloud Computing”, Proceedings of International Conference on VLSI, Communication, Advanced Devices, Signals & Systems and Networking (VCASAN-2013), Volume 258, 2013, pp 461-470, springer, 2013.

[3] Vic (J.R.) Winkler, “Securing the Cloud, Cloud Computer Security, Techniques and Tactics”, Elsevier, 2011.

[4] Sean Carlin, Kevin Curran, “Cloud Computing Technologies”, International Journal of Cloud Computing and Services Science (IJ-CLOSER), Vol.1, No.2, pp. 59~65, June 2012.

[5] John Mutch, Brian Anderson, “Secure Multi-Tenancy for Private, Public, and Hybrid Clouds”, in Preventing Good People from doing Bad Things, Springer, 2011.

[6] Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, Sep. 2011.

[7] Baburajan, Rajani (2011-08-24). "The Rising Cloud Storage Market Opportunity Strengthens Vendors". It.tmcnet.com. Retrieved 2011-12-02.

[8] Oestreich, Ken, (2010-11-15). "Converged Infrastructure". CTO Forum. Thectoforum.com. Archived from the original on 2012-01-13. Retrieved 2011-12-02.

[9] "Where's The Rub: Cloud Computing's Hidden Costs". 2014-02-27. Retrieved 2014-07-14.
[10] "Cloud Computing: Clash of the clouds". The Economist. 2009-10-15. Retrieved 2009-11-03.
[11] "Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner. Retrieved 2010-08-22.
[12] Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld. Retrieved 2009-06-02.
[13] Jump up to:a b "Announcing Amazon Elastic Compute Cloud (Amazon EC2) - beta". Amazon.com. 24 August 2006. Retrieved 31 May 2014.
[14] Antonio Regalado (31 October 2011). "Who Coined 'Cloud Computing'?". Technology Review. MIT. Retrieved 31 July 2013