IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-3, Issue-5 E-ISSN: 2347-2693

A Survey on Cloud Computing with different Encryption Techniques to Secure Cloud Data

Kiran prajapati[1*], Jaytrilok choudhary[2*]

[1,2*] *Department of Computer Sscience, MANIT Bhopal, MP, India*

prajapatikiran17@gmail.com, jaytrilok@gmail.com

www.ijcseonline.org

Received: Apr/26/2015 Revised: May/06//2015 Accepted: May/22/2015 Published: May/30/ 2015

***Abstract*—** Cloud provides facility of assigning data to a great number of scattered computers, rather than local computer or remote server. This paper briefly surveys the issues in cloud computing security. The fact is that the data shared with the cloud service provider is identified as the core scientific problem that separates cloud computing security from other topics in computing environment. The paper also describes different encryption techniques to secure the cloud data from unauthorized users.

***Keywords*—**Component Cloud computing security, Obstacles in cloud, Attribute based encryption, Homomorphic encryption.

I. INTRODUCTION

The term "cloud" is defined as "internet" and "computing" defines the delivery of different types of services over the internet. The internet computing is defined as cloud computing where virtual shared servers prepare the software, infrastructure, platform devices and other resources. The hosting to customers is provided on a pay-as-you-use basis. Users can access all the services available on the "internet cloud" without having any previous knowledge that how resources are involved. Cloud computing is an innovative Information System architecture. Cloud computing has leveraged users from hardware requirements, although overcome all the client side demand and complexity.

II. EASE OF USE

Email services as Gmail, Hotmail, yahoo, VoIP (e.g., Skype, Google Voice), social applications (e.g., Facebook, Twitter, and LinkedIn), media services (e.g., Picasa, YouTube, and Flickr), content distribution (e.g., BitTorrent), financial apps (e.g., Mint) and many more.

III. CHARACTERISTICS OF CLOUD COMPUTING

On-demand self-service: Various Computing capabilities available via cloud such as server time and network storage are provided automatically without requiring any third party interaction with each service provider [1].

Broad network access: Cloud access through a broad network is available over the network and also spread over the standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).

Rapid elasticity: It allows users to automatically request additional space in the cloud or different kind of services. Due to the structure of cloud computing services, capabilities of cloud have elastically released and growing as per requirement.

Resource pooling: The customers can access the information which is merged to serve multiple consumers using multitenant ideas, with different virtual and physical resources dynamically assigned and reassigned according to consumer demand.

IV. TYPES OF CLOUD

There are mainly four kinds of cloud [3]:

- Public Cloud – In public cloud any subscriber can access information from the cloud space with an internet connection.
- Private Cloud - A private cloud is found for a specific group or organization and restrict access to just that group.
- Community Cloud - In community cloud, two or more organizations that have similar cloud requirements, share their intelligence.
- Hybrid Cloud – hybrid cloud comprises of the combination of minimum two clouds, and that cloud should be mixture of public, community or private cloud.

V. CHOOSING CLOUD PROVIDER

1. *Software as a Service*

A SaaS provider provides Subscriber access to both resources and applications. Software-as-a-Service is

Corresponding Author: *Dr. Jaytrilok Choudhary, jaytrilok@gmail.com*
Department of Computer science, MANIT Bhopal, India

software that does not need to be installed on your regional setup. Instead, you access a remote system which hosts the software for you.

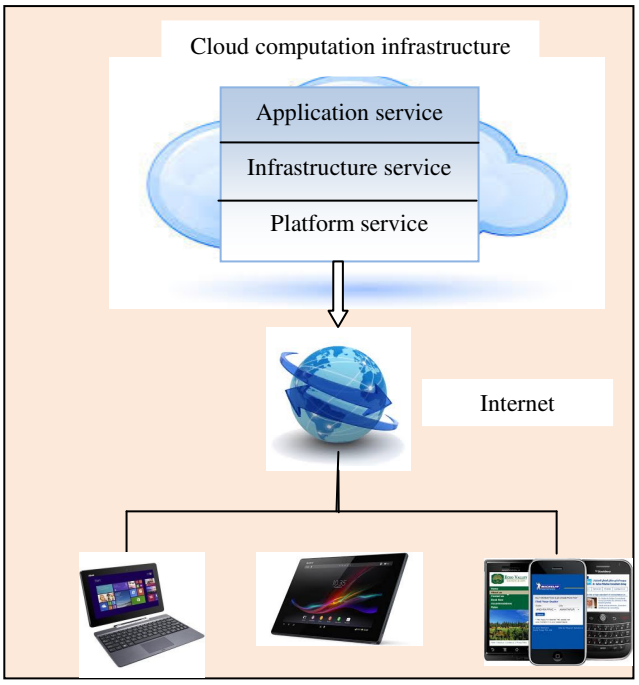

Figure 1. Cloud computing the business perspective [2].

2. Platform as a Service

PaaS is more advanced Than Software as a Service. PaaS providers host development environment, featuring a number of libraries and tools which can be used to develop and deploy custom cloud-based applications.

3. Infrastructure as a Service

Initially IaaS pact with computational infrastructure. In IaaS agreement, the user is entirely connected from outside storage and assets which they need, such as hardware and software. Infrastructure-as-a-Service is one of the fastest-growing flavours of cloud computing within the business space [3].

VI. SECURITY PROBLEMS IN THE CLOUD

There are a lot of personal information and potentially secure data that people store in their computers. These data stored in the cloud which is not reliable. The main concern with cloud computing is the management of the data which might not be fully authoritative.

This makes it critical for you to understand the security measures that your cloud provider has, and subscriber take personal precautions to secure their data. No matter how careful you are with your personal data, by subscribing for the cloud data you will be giving up some control to an external source [4]. This distance between you and the physical location of your data creates a barrier. It is easy to create more space for an unauthorized user to access your information.

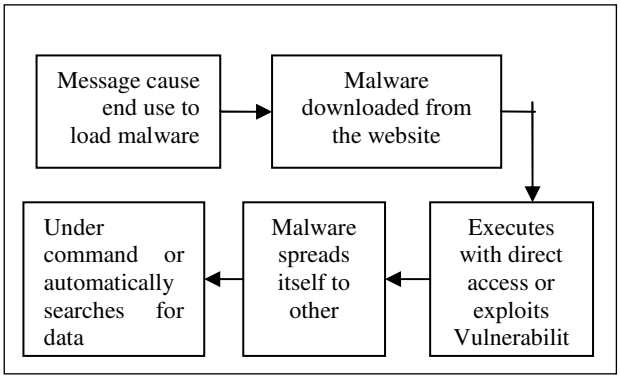

Figure 2. Illustration of the generic attack method using the end user as a vector [4].

TABLE 1. TYPES OF SECURITY OBSTACLES

Obstacle	Opportunity
Availability of Service	Use Multiple Cloud Providers to provide Business Continuity; Use Elasticity to Defend Against DDOS attacks [5].
Data Lock-In	Standardize APIs; Make compatible software available to enable Surge Computing.
Data Confidentiality and Audit-ability	Deploy Encryption, VLANs, and Firewalls; Accommodate National Laws via Geographical Data Storage.
Data Transfer Bottlenecks	FedExing Disks; Data Backup/Archival; Lower WAN Router Costs; Higher Bandwidth LAN Switches.
Performance Unpredictability	Improved Virtual Machine Support; Flash Memory; Gang Scheduling VMs for HPC apps.
Scalable Storage	Invent Scalable Store.
Bugs in Large-Scale Distributed Systems	Invent Debugger that relies on Distributed VMs.
Scaling Quickly	Invent Auto-Scalar that relies on Machine Learning; Snapshots to encourage Cloud Computing Conservationism [5].
Reputation Fate Sharing	Offer reputation-guarding services like those for email.
Software Licensing	Pay-for-use licenses; extent use sales.

Some security issues which customer should keep in their mind [6]:

1. *Privileged user access*: Customer should have knowledge about those users who have given privileged access, to supply specific information. On the hiring and oversight of honored administrators, and the controls over their usage.
2. *Regulatory compliance*: Customers have the responsibility for security and confidentiality for their own data, even when it is held by a service provider [6].
3. *Data location:* Cloud only stores our data in their storage space user exactly don't know the location of data that where is it stored? User should find the data source report from the cloud provider.
4. *Data segregation:* The cloud provider should have ability for secure delivery of cloud data, for privacy the best encryption techniques applied on cloud data; this must be ensured by cloud provider.
5. *Recovery:* The backup or restoration process should be available in the system in the case of any disaster or failure.
6. *Investigative support:* Investigation of cloud data are latterly difficult process because of signing in and using data for various customers might be co-located and also may spread over different hosts and data centers. After the contractual commitment to support specific forms of investigation, with guaranty that the cloud provider has already successfully supported such activities, you allow yourself to use those cloud data.
7. *Long-term viability:* If your cloud provider gets acquired and swallowed then you must be sure your data will remain available even after such an event. User/subscriber should ask to the cloud provider about the data replacement or restoration of system in the case of any requirement.

VII. ATTRIBUTE-BASED ENCRYPTION SCHEME

Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang have surveyed on ABE scheme [7]. Attributes have been used to setup a public key for encrypting data and have been used as an access policy to control user's access. Attributes play a very crucial aspect.

Advantages provided by ABE scheme are:

- Reduce the communication overhead of the Internet.
- Provide a fine-grained access control.

The data encryption process follows traditional public key infrastructure, and the data owner uses data users public key to encrypt this data before uploading to the cloud. If the user wants to access data and sends the request to the cloud, then the cloud would return the analogous cipher text to the data user. A user would use his private key to decrypt this data.

But this manner would lead to some problems:

1. The third party is able to encrypt data. Because The public key is also shared with cloud provider.

2. A lot of storage overhead would spend because There by using different public keys obtaining the same plain text.

To resolve these disadvantages, attribute-based encryption (ABE) has proposed. In ABE method identity of user brings as attribute, familiarly firm of attributes were allow to encrypt and decrypt data.

There are authority, data owner (also be called sender) and user (also be called receiver). In this method, the authority's act is to setup the keys for data owners and users to encrypt or decrypt data. The authority generates public key and master key, according to attributes, where attributes should predefine.

If user who wants to add to any data in this system, and he owns to attributes and not include predefined attributes. The authority will reformulate the attributes and give a public key and master key again. A data user's act is to decrypt the encrypted data with his private key directed from the authority, and then he can obtain the needed data. For decrypting the data, attributes in data user's private key will audit by matching with the attributes in encrypted data. If the number of "matching" is at least a threshold value d, the data user's private key will be permitted to decrypt the encrypted data.

In this scheme, there are four algorithms to be executed:

Setup, KeyGen, Encrypt, and Decrypt.

Let G1and G2 are two bilinear groups of prime order p, and let g be a generator of G1. And let e: G1 × G1 → G2 denote the bilinear map, and let d is a threshold value.

1) Setup (d): The authority uniformly and randomly

Chooses t_1...., t_n, y from Z_q, and publishes the public key, PK = (T1 = g^{t1}..... $T_n = g^{tn}$; Y = e (g, g)^y). And the master key is M_K = (t_1.... t_n, y).

2) Key Gen (A_U, P_K, M_K): The authority executes and generates a private key for the data user U. Pickup a

d - 1 degree polynomial q randomly such that q(0) = y. The data user's private key D is $\{D_i = g^{q(i)/ti}\}$ $i\epsilon_{AU.}$.

3) Encrypt (A_{CT}, P_K, M): Data owner encrypts message M C G2 with a set of attributes $A_{\epsilon T}$. Choose a random number s C Zq, and the encrypted data is published as T = (A_{CT}, E = MY^s = e (g; g)^{ys}; $\{E_i = g^{t s}_i\}$ $i\epsilon A_{U.}$

4) Decrypt (CT, P_K, D): Data user decrypts the encrypted data CT with the private key D. Choose d attributes from I ϵ $A_U \cap A_{CT}$ to compute $e(E_i;D_i) = e(g; g)^{q(i)s}$ if $| A_U \cap A_{CT} | \geq d$. And compute $Y^s = e(g; g)^{q(0)s} = e(g; g)^{ys}$ with the Lagrange coefficient, and the message $M = E/Y^s$ can be obtained.

In KenGen algorithm, the user's private key is generated with secret sharing. These shares of secret y are embedded in the components of the user's private key Di, and the secret key is associated with the random polynomial q. So every user's private key D cannot be combined to a new private key to perform the collusion attack.

For the purpose to remove its problems the new method i.e. key-policy attribute-based encryption (KP-ABE) scheme arrived that built the access policy into the user's private key and described the encrypted data with user's attributes [7]. The KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme. But the disadvantage of KP-ABE is that the access policy is built into a user's private key, so data owner can't choose who can decrypt the data except choosing a set of attributes which can describe this data. Monotonic access structure; it can't

And it is unsuitable in certain application because a data owner has to trust the key issuer. Besides, the access structure in KP-ABE is express the negative attribute to exclude the parties with whom data owner don't want to share data from memberships.

After that new policy proposed a cipher text-policy attribute based (CP-ABE) scheme that built the access policy into the encrypted data; a set of attributes is in a user's key. The CP-ABE scheme addresses the problem of KP-ABE that data owner only trusts the key issuer.

After all again new scheme arrived i.e. Hierarchical Attribute-based Encryption Scheme. This scheme uses the disjunctive normal form policy and generates the keys hierarchically. And this scheme assumed that all attributes in one conjunctive clause are administered by the same domain authority. Table 2 describes security analysis of all types of attribute based-encryption techniques.

VIII. SECURING THE CLOUD WITH HOMOMORPHIC ENCRYPTION

Homomorphic encryption concept refers that the encryption performed by the owner and information will be restricted to the cloud provider and will not share the secret key for decrypting the data.

When you need to alter/change your encrypted data in the cloud, then the secret key to decrypt your data need to be shared with the cloud provider. By sharing this secret key will grant the current cloud provider to access your information. The answer to this problem could be homomorphic encryption.

TABLE 2. SECURITY ANALYSIS OF ALL TYPES OF ATTRIBUTE-BASE- ENCRYPTION [7]

Item	ABE	KP-ABE	CP-ABE	ABE with non-monotoni-c	HABE
fine-grained access control	N	Y	Y	Y	Y
Data confidentiality	Y	Y	Y	Y	Y
Scalability	N	N	N	N	Y
user accountability	N	N	Y	N	Y
user revocation	N	Y	Y	Y	Y
Collusion resistant.	Y	Y	Y	Y	Y

There mainly two types of homomorphic encryption technique available first one is fully homomorphic encryption where arbitrary number of aggregate functions as OR, AND, NOT to be performed on encrypted data. The "noise" is limiting factor in FHE. Only cause of more computation its noise level become so high and resulting cipher text become indecipherable [8].

And the second is somewhat homomorphic encryption supports limited number of operations (i.e., any amount of addition, but only one multiplication) and more compact than FHE cryptosystems.

Bootstrapping technique:

To overcome the noise issue in FHE there use bootstrapping the idea of bootstrapping for double encrypting the data and, as processes runs, removing a layer of encryption Bootstrapping procedure adds another layer of encryption [9].

A) HOMOMORPHIC ENCRYPTION AND ITS POTENTIALS IN THE CLOUD

We already discussed about the homomorphic technique, the idea was first suggested by Rivest, Adleman and Dertouzos in 1978, referred to as privacy homeomorphisms [10]. RSA (invented by Rivest, Shamir and Adleman implied multiplicative homomorphism.
An encryption scheme can be said to be fully homomorphic if:

$$E(m1 \Theta m2) <\text{---} E(m1) \Theta E(m2); \forall m1, m2 \in M$$

Where M is the set of plaintexts, Θ - represents any arbitrary function and <--- means computation is done without the plaintexts being decrypted.

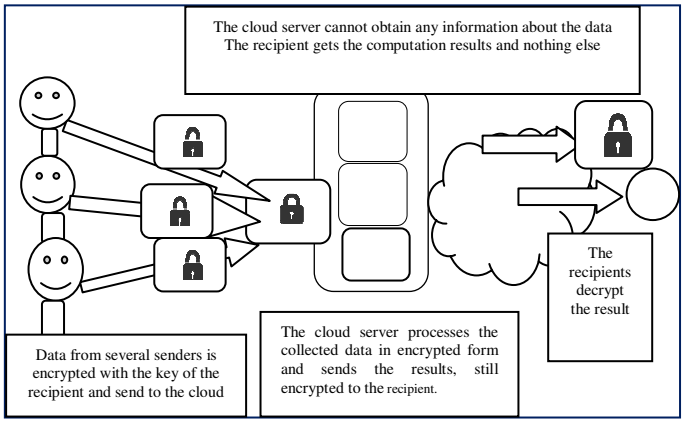

Figure 3. Anonymous data processing with fully homomorphic encryption [9].

Gentry's fully homomorphic encryption using ideal lattices

Gentry's fully Homomorphic encryption [10] method followed by four steps:
1. KeyGen - creates two keys i.e. the secret key s_k and the public key p_k.
2. Encryption - encrypts the plaintext m with the public key p_k to find cipher text c.
3. Decryption - decrypts the cipher text c with the secret key s_k to retrieve the plain text m.
4. Eval - outputs a cipher text c of f (m) such that Decrypt (s_k, m) = f (m).
It is ever seen that any arbitrary function is made up of an aggregate of addition, subtraction and multiplication functions (i.e. AND, OR and NOT gates). Here ideal lattices used in additive and multiplicative homomorphism for low circuit complications.
Van dijk et al [10], proposed a true variant of gentry's fully Homomorphic encryption over the Integers.
The algorithm shows:

1. KeyGen
   - The secret key p is an odd number.
2. Encrypt - To encrypt a 1-bit message m.
   - A large multiple of the secret key e.g. pq.
   - A small even number e.g. 2r where r is the noise and r < p/4 or 2r < p/2
   - The cipher text is c = pq + 2r + m.
3. Decrypt - to decrypt cipher text c
   - The cipher text c = pq + 2r + m.
   - c(mod p) = 2r + m(mod p)
   - message with noise (c mod p) mod 2 = r + m,

Here noise is as consistence as the message. We can easily retrieve the message if the noise remains small; it can yield by additive and multiplicative homomorphism.

Given, c1 = pq1 + 2r1 + m1
c2 = pq2 + 2r2 + m2
Additive Homomorphism implies:

- c1 + c2 = p(q1 + q2) + 2(r1 + r2) + m1 + m2
- [(c1 + c2) mod p] mod 2,
- Reading off the LSB gives us m1 + m2

Multiplicative Homomorphism:

- c1 × c2 = p.(c2q1 + c1q2 - q1q2) + 2.(r1r2 + r1m2 + r2m1) + m1m2
- [(c1 . c2) mod p] mod 2,
- Reading off the LSB gives us m1m2

Expansion of Noise according to cipher text is the main concern which tried to reduce in additive and multiplicative homomorphism scheme.
In 2012 Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI proposed encryption algorithm which included RSA and multiplicative homomorphic encryption [11].
RSA cryptosystem:

- Initially setup the public and private key:
- Randomly choose two large primes i.e. p, q
- computing their system modulus N=p. q
  - where ø(N)=(p-1)(q-1)
- selecting encryption key e randomly
  - where 1<e<ø(N),
  - gcd (e, ø(N))=1
- Find decryption key d
  - e. d=1 mod ø(N) and 0≤d≤N
- publish their public encryption key:{e, N}
- keep secret private decryption key:{d, p, q}

To encrypt a message M the sender:
Computes: $C=M^e \bmod N$, where $0 \le M < N$
To decrypt the cipher text C the owner:
Computes: $M=C^d \bmod N$
Suppose we have two ciphers C1 and C2 which accepted by RSA cryptosystem apply the function of the multiplicative Homomorphic encryption.

$$C1.C2 = m1^e\, m2^e \bmod n = (m1m2)^e \bmod n$$

Because if we assume that two ciphers C1, C2 analogous respectively to the plain text m1, m2 so

$$C1 = m1^e \bmod n$$

$C2 = m2^e \bmod n$

The client sends the pair (C1, C2) to the Cloud server; the server will perform the calculations requested by the client and sends the encrypted result (C1 × C2) to the client.

This scheme is better because here two layer encryption and two keys (public and private) are used.

Because if the attacker captures two ciphers C1, C2, which are encrypted with the same private key, it will be able to decrypt all messages exchanged between the server and the client. Because the Homomorphic encryption follows multiplicative property, i.e. the cipher of the product equals to the product of the ciphers.

IX. CONCLUSION

Switching to cloud computing is the next stage of an irrepressible trend in the mishap of the enterprise perimeter, both technically and organizationally. On one side cloud computing gives us advantages in vast field and on other side it also gives some negative effects as Cloud computing providers need to solve the common security challenges of traditional communication systems. To maintain the security there are different cryptography algorithms present to ensure the security challenges in the cloud.

REFERENCES

[1] Huth and J. Cebula, "The Basics of Cloud Computing," Carnegie Mellon University. pp. 1–4, **2011** [Online].

[2] S. Marston, Z. Li, S. Bandyopadhyay, J.Zhang, and A. Ghalsasi, "Cloud computing the business perspective," Decis. Support Syst.,vol. 51, no. 1, pp. 176–189, Apr. **2011.**

[3] P. Mell, T. Grance, and T. Grance, "The NIST Definition of Cloud Computing" Recommendations of the National Institute Of Standards and Technology, pp. 800-145, September **2011**.

[4] P. G. Dorey and a. Leite, "Commentary: Cloud computing – A security problem or solution?"Inf. Secur. Tech. Rep., vol. 16,no. 3–4, pp. 89–96, Aug. **2011**.

[5] M. Armbrust, A. D. Joseph, R. H. Katz, and D. A. Patterson, "Above the Clouds: A Berkeley View of Cloud Computing," University of California at Berkeley pp. 14-19, February 10, **2009**.

[6] B. J. Brodkin, N. W. Cloud, S. Risks, C. Computing, and G. A. Engine, "Gartner: Seven cloud-computing security risks," pp. 2–3, **2008.**

[7] C. Lee, P. Chung, and M. Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments," vol. 15, no. 4, pp. 231–240, **2013**.

[8] N. York, "Securing the cloud with homomorphic encryption," vol. 20, no. 3, pp. 1–4, **2014.**

[9] M. Tibouchi, "Fully Homomorphic Encryption over the Integers: From Theory to Practice," pp. 1–4, **2014.**

[10] A. Atayero and O. Feyisetan, "Security Issues in Cloud Computing : The Potentials of Homomorphic Encryption," vol. 2, no. 10, pp. 546–552, **2011**.

[11] M. Tebaa, S. E. L. Hajji, and A. E. L. Ghazi,"Homomorphic Encryption Applied to the Cloud Computing Security," vol. 1, pp. 8–11, **2012.**