SECURITY OF DATA IN CLOUD COMPUTING USING HOMOMORPHIC ENCRYPTION

ALEEMA JOSE

Student

MSc computer science

St.Joseph's college (autonomous)

Irinjalakuda ,India

Abstract : The cloud computing is used to store the user data in a cloud storage for the future use and it keep the data secure. The data stored in encrypted form. This means that the data we entered in the plain text and the user use the encryption algorithms to secure the data, then it is in the form of ciphertext and this encrypted data can be decrypted whenever the user want it is to be processed. The encrypted data can be decrypted only by the authorized person. Cloud is used to secure our data, software, hardware and all services in the internet. This paper is indended for storing the data in a cloud and using homomorphic encryption. Homomorphic encryption is used to ensure the security of stored data and details. Homomorphism ia a property and if problem of one system can converted to a problem into another system and make solution and it translated back effectively.

IndexTerms - homomorphic, encryption, ciphertext, decryption, cloud storage.

I. INTRODUCTION

The cloud computing is used to manage and process data in a local server or personal systems. This is a new method in information technology and it provide variety of services. And it is applicable or run anywhere in the world to its users through the internet. It provide a strong security in all level like application, host etc.the cryptosystem provide security of data. The data is always encrypted in cloud ,the encrypted data can be decrypted before computation. The cloud computing is used in business field for the purpose of accessing the sensitive data. The homomorphic encryption algoritham is used to decrypt the encrypted data

This article is structured is as follows: section 1 cloud characteristics and architecture. Section 2 security in cloud computing and its challenges and issues. Section 3 homomorphic encryption.

A.Cloud Characteristics

The five important characteristics of cloud computing.

1. On demand self-service:-This process provide an opportunity to reduce the costs significantly. Therefore, in case you can access any information quickly . Then you can approach the service provider and extract the particular information without any difficulty. This is the important characteristics .
2. Network access:- Cloud computing simply a network access from anywhere worldwide.
3. Resource pooling:- This is access several clients into a single pool of servers or storage or other type of specific resource. The all things are managed in resource pooling.
4. Elasticity:- Sometimes we need additional resources or data in a small period of time and this time use cloud computing
5. Usage fee:- The cloud computing is comes with a pay per use method. This reason why more and more companies are accessing it for the purpose of storage. The usage of fee of cloud computing is never a big problem if you need to pay for the services that you make use of it.

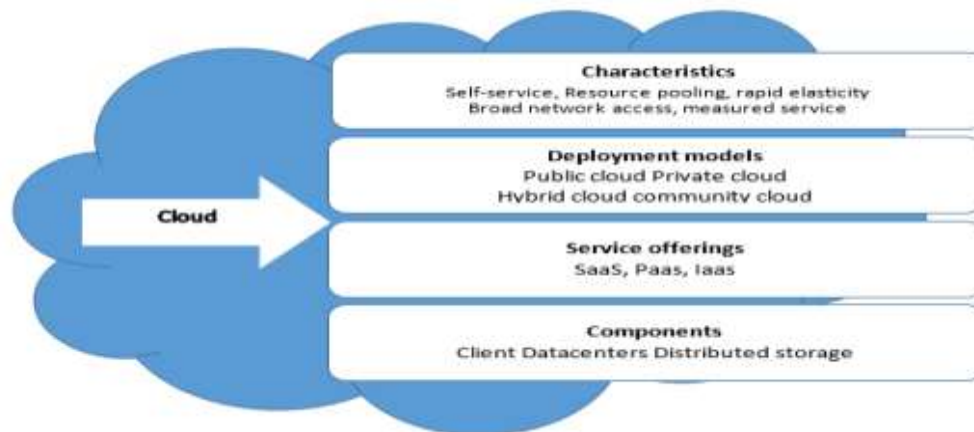The following (fig. 1) is used to describes the communication, development , storage are normally in cloud.

Fig .1 cloud computing paradigm[1]

B.Cloud architecture

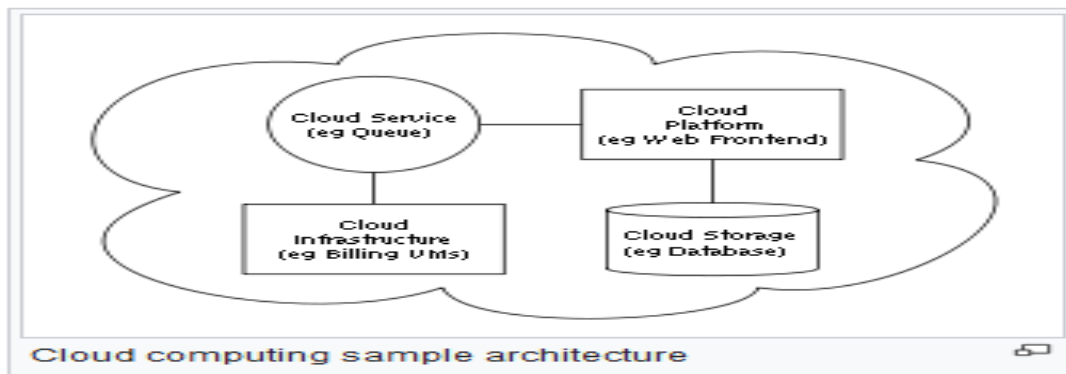The cloud computing architecture is cloud solution it is a structure of a system. It is also a documentation.

Fig .2 cloud computing architecture[2]

II. SECURITY IN CLOUD COMPUTING

This section mention the challenges and issues in the cloud computing. [3]

A. Challenges

1)   Outsourcing: Privacy terms can occur in the customers side, actually it lose the control on their data and tasks.
2)   Multi-tenancy: New error and security issues occur at the shared nature of clouds between multiple users.
3)   Massive data and intense computation: the old and traditional security techniques it can not be applicable in cloud due to large computation
4)   Heterogeneity: Integration problems arise between the cloud providers.it can occur using different security and privacy techniques.
5)   Service level Agreement: the action mechanism between provider and consumer or user of services need to be established

B. Cloud computing security issues

There are some security issues given below that are,[4]

1) Trust: The cloud service provider is to provide an sufficient security policy and it to be minimize the risk of data loss or data manipulation.
2) Confidentiality: The confidentiality can be provide an security for data and it as sharing or storage of information on remote servers and it is done in cloud computing which is to be accessed through the internet.
3) Privacy: It provide protection of data from unauthorized access. It is an illegal admittance to user's sensitive data and it will bring security issues.
4) Integrity: It is to guarantee the precision and correctness of data. The Cloud service provider should be provide security against insider attacks on data.
5) Reliability and availability: Trustworthiness of cloud service provider deduces when a use's data get leaked or lose.
6) Authentication and authorization: To prevent unauthorized access, software is required outside the organization's firewall. The firewall provide the data security .
7) Data Loss: Removal or modification of data can be lacking any backup could lead to be data loss.
8) Easy Accessibility of Cloud: Cloud services are able to be used by anybody or by the user by a simple registration model.

III. HOMOMORPHIC ENCRYPTION

The homomorphic encryption technique is used to enabling the encrypted data. The encrypted data can read only by decrypt and use. It provide a security for unauthorized access. In the cloud the data in a encrypted state.

The homomorphic encryption have two types that are partial and fully homomorphic.

1) Partial homomorphic : it provide less effort to encryption or decryption.it perform faster than the fully homomorphic encryption
2) Fully homomorphic: it provide the user to perform multiple task.Only one kind of operation is allowed to perform in a partially homomorphic encryption technique .
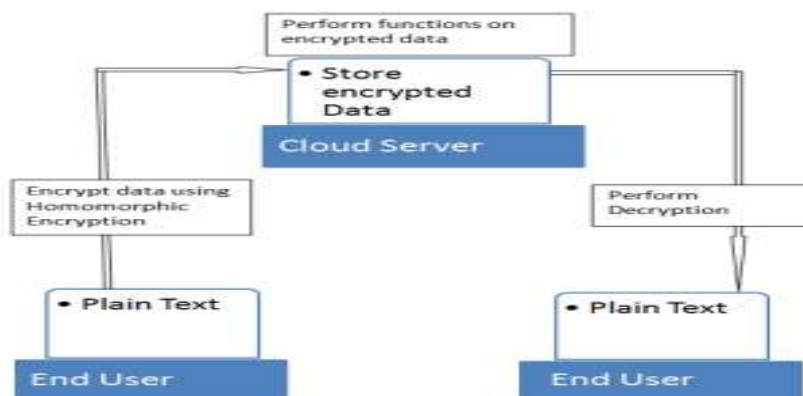
The (FHE) can provied a proposed system given below.

Fig.3 FHE proposed system[5]

It can perform multiple operation and it take more effort and it perform slower.

IV. CONCLUSION

The security of cloud computing using homomorphic encryption. This method is used to make our data in seured one. The users increasing daya by day because it is very helpful. The homomorphic encryption is used to improving the privacy cloud storage data. There are various simple algorithms are used to encrypt the data. This document is provide certain security and it overcomes the issues in security.

V. REFERENCES

[1] .Abdullah Gani, Md Whaiduzzaman, Mehdi Sookhak , Rajkumar Buyya "A survey on vehicular cloud computing" ,Journal of Network and Computer Applications40 (2014),www.elsevier.com/locate/jnca, pp. 325–344.

[2] "Building GrepTheWeb in the Cloud, Part 1: Cloud Architectures".   Developer.amazonwebservices.com. Retrieved 22 August 2010.

[3] Banafar H, and Sharma S. (2014), „Secure Cloud Environment Using Hidden Markov Model and Rule Based Generation?, International

Journal Of Computer Science & Information Technologies, Vol. 5 No.3 pp. 4808-4817.

[4]Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.", 2009.

[5] Samyak Shah, Yash Shah, Janika Kotak, "Somewhat Homomorphic Encryption Technique with its Key Management Protocol", Dec 14 Volume 2Issue 12 , International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169, PP: 4180 - 4183