A SURVEY ON CRYPTOGRAPHY: A IMPORTANT TERM IN CLOUD COMPUTING

[1]Priya Chaturvedi,[2]Umang Thakkar
[1]Student,[2]Assistant Professor
[1]Department of Computer Engineering
[1]Silver Oak College of Engineering & Technology, Ahmedabad, Gujarat, India

Abstract : Cloud computing is now a new term to use internet and store the information on the cloud. Cloud computing is a internet based technique where shared resources ,software, and data or information are provides on demand on consumer need. While all the information is store on cloud it essential that to build a secure cloud environment , this can be assured by only the security and cryptography. All the services of cloud is provided by the service provider , so its important to mask the data from the provider and the user can be trust their data to cloud provider. Our main concern to assure the privacy and security of the data and the different term that involve in the cryptography. On this paper we survey the cryptography importance to shared data to cloud through the cloud service provider.

IndexTerms **– Cloud Computing, cryptography, symmetric and asymmetric method**

I. INTRODUCTION

cloud computing become a progressively fashional in disrtibuted computing environment. As coud computing provide many services like SaaS, PaaS, Iaas . cloud computing is term as provided different services as on demended by the user. Its is as pay per use services. SaaS provide on demand software service , PaaS provided the platform to create the application , IaaA provide the different infrastructure to create the application on cloud[1].

Ther are so many adavantages of using of cloud computing like it mprove flexibilitywith re provisioning by adding and expanding the technology, cost reduction as per by the type of service provider like public, private and hybrid cloud, device and location independence like no need to access the cloud from one place we, can access the cloud from any device and any places. Maintenance , no need to maintain and upgrade the software that all services is provided by the service provider. Performance is monitored by IT experts from the service provider and consistent and loosely coupled architecture are provider. Reliability and scalability are provided by provide the fine gained access to cloud and dynamically provided.

As per the advantages their are so many main disadvantages of cloud computing that are privacy and security. Privacy is the main concern in cloud computing because service provider can access the private data on cloud any time, many service provider can share information with third partyif necessary without any warranting. So, its is important to protect data user have to encrypt data before stored on cloud to prevent unauthorized access.[1]

So for the privacy and access and security concern the cryptography is important .

II. BACKGROUND

So the security of data is one if the broad and key issues in computing .. Cryptography is the process of creating secret codes to protect the original message from attacks and maintain its integrity. Many applications use cryptography to protect sensitive data and messages. Cryptography is used to ensure that data or message remains unaltered . The original message is called plain text and cipher text is the encrypted text or message. This is shown in Fig 1 basic process of text conversion in cryptography.[2]

For the proper communication through the communicable channel the cryptography term is introduced for the reason that if the communication channel is not protect any intruder can take advantage of that and try to hack the private data .

For this reason the protection of the data is necessary to protect the anyone private data to transfer it from one person to another

Cryptography term:for the security of the data six term is explain that is plain text, ciphertext, encryption and decryption algorithm , key and ciphertext . its is necessary to understand the term to understand the cryptography and how it work to secure the data while transferring the private data from one person to another .

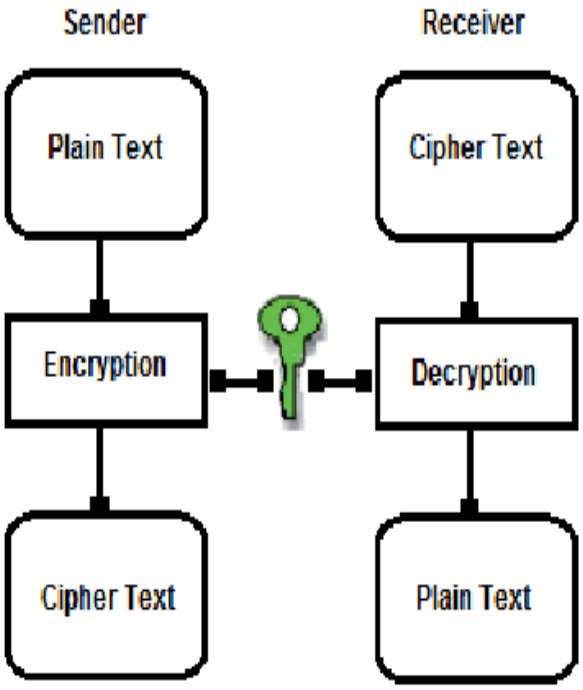

Figure 1: term of cryptography

2.1 Plain Text

Plain text: **Plaintext** is a term used in **cryptography** that refers to a message before **encryption** or after decryption

.

2.2 Cipher Text

Ciphertext is encrypted text. Plaintext is what you have before **encryption**, and**ciphertext** is the encrypted result.

2.3 Key

A **cryptographic key** is a string of bits used by a **cryptographic** algorithm to transform plain text into cipher text or vice versa. This **key** remains private and ensures secure communication.

2.4 Encryption

encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

2.5 Decryption

Decryption is the process of transforming encrypted information so that it is intelligible again..

2.6 Encryption And Decryption Algorithm

Encryption and decryption algorithm: An **encryption algorithm** along with a key is used in the **encryption and decryption** of data.

III. TYPE OF CRYPTOGRAPHY

3.1 Symmetric Key Cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.example DES(data encryption standard), AES(advanced encryption standard).[2]

3.2 Asymmetric Key Cryptography

cryptography in which two different but mathematically related keys are used—a *public* key and a *private* key. Any one key use to create cipher text and other key use for decryption process to convert back to its plain text. example RSA

The difference between of symmetric and asymmetric cryptography technique is varied that is,Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating. Symmetric encryption is an old technique while asymmetric encryption is relatively new. Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetrical encryption model, eliminating the

need to share the key by using a pair of public-private keys. Asymmetric encryption takes relatively more time than the symmetric encryption.

IV. CRYPTOGRAPHY IN CLOUD

As to upload and download the file again and again to cloud to its necessary to secure the file before and upload the data.it provide the three main advantages tp cloud user.[3]

In cloud cryptography is necessary to satisfied the

4.1Acess Control In Cloud

Access control is a mechanism that prevents un- authorized access to a resource. Consumer and enterprise users can store their data at public cloud, maintaining data confidentiality and integrity by means of cryptographic cloud storage.[4]

.

4.2Trust Management In Cloud

Trust management is an important aspect while implementing security at cloud, which is about sharing of resources between cloud and its consumer. It means that consumer needs to trust the cloud service provider. There should be some kind of trust management and negotiation contract or procedure to fulfill this requirement.[4]

4.3Privacy Management In Cloud

Secure storing and retrieval of resources at cloud is an important aspect of cloud security. Several technologies for resource and its information management are databases, symantic web and data mining. The fact of resource information collection and storage produces the terror of privacy.

V. ADVANTAGE OF USING CRYPTOGRAPHY IN CLOUD

Data breaches prevention: Strong data encryption can effectively prevent data breach - ensures that the multi-tenant cloud service database is properly designed and configured to keep hackers away from the system.

Data loss prevention: The prospect of seeing their critical information disappears without trace can be frightening to users. Not only data encryption may ward off hackers, the regularly updated offline data backups also reduce risks of data loss.

Account hijacking prevention: your service should offer solutions that protect users' credentials from being stolen. Without a secure platform, hackers may eavesdrop on out transactions, manipulate data and return falsified information that harms clients.

More secure APIs: APIs are important to maintain the availability and security of a cloud service. Your service should help users to identify and improve weak APIs that can expose the organization.

DoS prevention: Denial of service is a classic Internet threat and outages may cost users immensely. Solutions offered by a reliable cloud computing service will detect DoS attacks and provide effective responses to ensure 24/7 availability.

Reduction of malicious threats: your cloud computer service should provide a solid solution to prevent former employees, contractors and business partners from gaining access to a cloud network.

Proper due diligence: Organizations that embrace cloud computing technology should fully understand its unique environments and risks associated with them. As an example, improper uses of cloud may cause contractual problems with service providers over transparency and liability. A reliable cloud computing service provides consultation and reliable internal bureaucracy systems to prevent occurrences of legal issues.

Reduction on impacts of shared resources: Cloud computing solutions could be based on shared infrastructure such as processors, RAM, GPUs, caches and hard drives. A reliable cloud computing service will provide solid isolation properties for SaaS, PaaS and IaaS.

Cloud computing security is built upon the inherent, basic benefits of cloud technologies such as automated security management, disaster recovery, redundant system and homogeneity; making it safer for users with critical data to employ cloud solutions. Cloud users should include rigorous security as an inseparable part of their operational routines. Your provider can help to achieve that.

VI. CONCLUSION

Cloud computing is very useful for the latest communication and storage of the large amount of data , so its essential to secure those data from the unauthorized or from the service provider.

As the people saving their personal and sensitive information on cloud it's a main task to protect its confidentiality and integrity. So we analyze the key cryptography way to secure or masking the data to protect it integrity and confidentiality to data.

From this survey we conclude that the how much work is done on the field of cryptography for the privacy and security control of the data.

VII. FUTURE WORK

As cloud is a vast technology and there is lots of data upload and download on the cloud, as there is so many files of one person to to use a different key for different file its create a problem of learning so much key, so find a new technology to use a single key to encrypt and decrypt a large amount of data.

REFERENCES

[1] B.Harikrishna,Dr.S.Kiran,R.Pradeep kumar Reddy, "Protection on Sensitive Information in Cloud -Cryptography algorithms",IEEE,2016.

[2] Manju Khari , Manoj Kumar,V aishali , "Secure Data Transference Architecture for Cloud Computing using Cryptography Algorithms", IEEE, 2016.

[3] K.Priyadarsini, C.Thirumalai selvan," a survey on encryption schemes for data sharing in cloud computing", IJCSITS, 2012

[4] Omer K. Jasim Mohammad ,Safia Abbas ,El-Sayed M. El-Horbaty Abdel-Badeeh M. Salem ," Securing Cloud Computing Environment using a new Trend of Cryptography ", IEEE,2015.

[5] G Bhuvaneswari, Mr. K.Narayana, Erasappa Murali," Prediction System for Reducing the Cloud Bandwidth and Cost ",IJCER,2014.

[6] Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk," A Patient-Centric Attribute Based Access ControScheme for Secure Sharing of Personal Health Records Using Cloud Computing",IEEE,2016.

[7] Faiza Fakhar*, Muhammad Awais Shibli," Comparative Analysis on Security Mechanisms in Cloud",ICACT,2013

[8] Xianping Mao, Junzuo Lai, Qixiang Mei, Kefei Chen, Jian Weng Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption" ,IEEE,2015

[9] konda reddy. guddeti and gangadhara . P," An Efficient Attribute Based Encryption Data Retrieval in Cloud ",IEEE,2017.

[10] Guofeng Lin, Hanshu Hong, and Zhixin Sun," A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing ",IEEE, 2017