ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Achieving Big Data Privacy for Colour Images via Hybrid Cloud

Onkar S. Undale[1], Prof. Bharati Kale[2]

M.E. Student, Dept. of Computer Engineering, DPCOE, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering, DPCOE, Pune, India[2]

ABSTRACT: In recent 5 to 6 years' cloud computing have been acquired by all over the Industry, due to rapid growth in information digitization, electronic communication and mobile device technology. User data Privacy preservation in cloud environment is most difficult challenge in terms of security of big data in cloud computing. Because big data platform is collection of sensitive as well as non-sensitive information. To work with these two different platforms together, organization comes with Hybrid cloud approach to provide solution. There are many small scale industries arising and making business with other organization. Data owner of organization or customers don't want to expose or scan their database by the cloud service provider such as Amazon EC2, Open Stacks. To improve performance in term of security cloud uses Cryptographic format of original data in public cloud. Proposed survey carried out how to improve performance of image data privacy preserving in hybrid cloud and also we are going to compare different data privacy preserving technique of hybrid cloud with standard AES cryptographic approach in public cloud.

KEYWORDS: Big data; Image data; cloud service provider; Hybrid cloud; Privacy preserving

I. Introduction

Big data is Collection of huge volume of data and applying analytics to implicate privacy violations to largest Internet organizations such as Google, Yahoo!, Facebook, Twitter, LinkedIn, and Amazon. Privacy protection has been more challenging as we are living in a digital world where people, devices, and sensors are connected and data is generated, accessed and shared widely with each other. There many big mobile networks use to carry large amount of sensitive data about their customers. Big data refers database and performing operations on huge data remotely from the data owner's enterprise. Therefore, a key value proposition for big data is access to data from multiple domains. Therefore, security and privacy will play important role in big data research and technology. There is another threat of attacker to database system, with the help of malicious program tries to break security of database otherwise he will try to destroy entire database system. So, a question is what type of security and privacy preserving technology is adequate suitable for efficient direct access to big data. [1] These issues are concerned with velocity, volume, and variety of big data and large-scale cloud infrastructures, information from different data sources and formats, streaming of data and huge volume of information inter-cloud migration. Therefore, traditional security mechanisms, which are tailored with new concept of hybrid cloud infrastructure. [4]

Objective is to go and protect data, when data is process and becomes information, so data is to be protected and should not be corrupted. Data manipulation is done by the cloud application level security. i.e. application need to go and protect data, the data manipulation by application. [5]

Data life cycle? Data born and dies, between birth and death of data it should be kept clear that data necessity, confidentiality, integrity, availability of data, when some application need it. The impact of cloud infrastructure on different phases of data lifecycle may appear and it will affect the data security policy. [5]

DOI: 10.15680/IJIRCCE.2015. 0311028

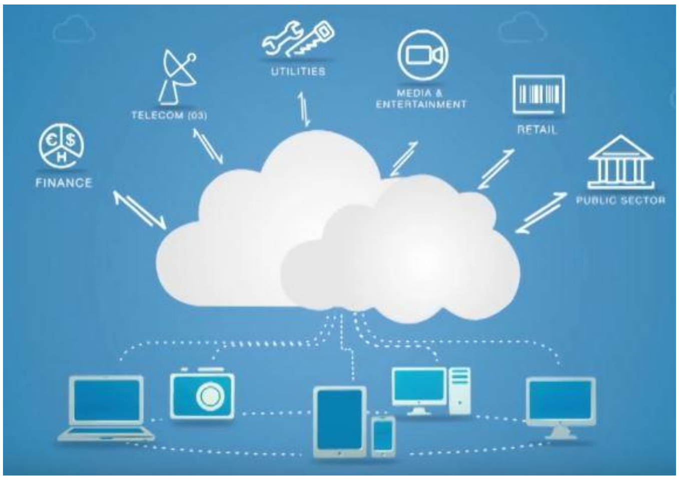

Fig. 1. Cloud Organization Sectors

Nowadays many sectors are work with cloud technology, as shown in Fig.1 Finance, Telecom, Utilities, Media and entertainment, Retail and Public sectors such different industries in different sectors are work together on multiple nature of cloud platform. Cloud service provider (CSPs), who provide infrastructure to their customer. Customer don't want to scan their database even by CSPs for advertisement of or any other technical reason. [1]

II. RELATED WORK

Our survey focuses on the existing present field of Privacy Preserving Image Data. We found that there is no such single methodology suitable for all domains application. All techniques performing in a different way depending on type of application or domain where to implement such as medical, security using biometric data, Image sharing social network application such as Facebook, Instagram, Picasa. We realize that Cryptography methods perform very well than the other existing methods. [1] So Cryptography is best Implementation approach for encryption of sensitive data. There for in our survey we are focuses on Hybrid cloud computation as well as different image cryptographic techniques for image data privacy preservation. [6]

A. Data Privacy in Cloud Computing

To get fine-access to data in cloud there are certain standard techniques are used to access cryptographic data in cloud, such as Attribute based encryption (ABE), Proxy encryption. [1] Here we are providing expressive access methodology to access different isolated attribute of file, i.e. each separate data file has been associated with set of attribute. This approach run with hybrid cloud. [4]

B. Types of Cryptography

1. Using Secret Key Cryptography
   In this scenario, cryptographic algorithm uses a single key i.e. symmetric encryption. The sender and receiver applies same key to encrypt and decrypt a message. The problem with this technique is the distribution of key between sender and receiver because this type of algorithm is only effective for secure type of connection between source and destination. [2]

2. Using Public Key Cryptography
   In this scenario, involves two key based cryptographic systems through, secure communication can take place between source and destination over the insecure communication network. [2] Since a pair of keys (public key, private key) is applied. It also known as asymmetric encryption.

3. Using Hash Functions
   Using hash function any key, uses a fixed length hash value that is computed on the basis of the plain text message. Basically hash functions are useful to check the integrity of the message and to assured that the message has not been altered during transmission, [2] compromised changes or any part of data affected by virus.

Table 1. Image Cryptographic Techniques

Sr. No	***Technique***	***Parameter Achievement***	***Work And Use***
1	Region Based Selective image Encryption	Reduce the overhead involved in data transmission over secure channels.	Uses of this algorithm is in Medical field. i.e. no need transmit entire image.
2	Selective Image Encryption Using Chaotic Map	It is specifically designed for the coloured images.	Expansion of networks and the huge amount of content to transmit.
3	Image Encryption using Blocked based transformation algorithm	Strong Encryption and decreases correlation.	Large size of image can be transmitted over non secure communication channel.

As Shown in Above Table.1 three different type of image cryptographic techniques are possible to provide a solution for given problem statement. The survey has been proposed according to comparative study of techniques on basis of parameter achievement and application use.

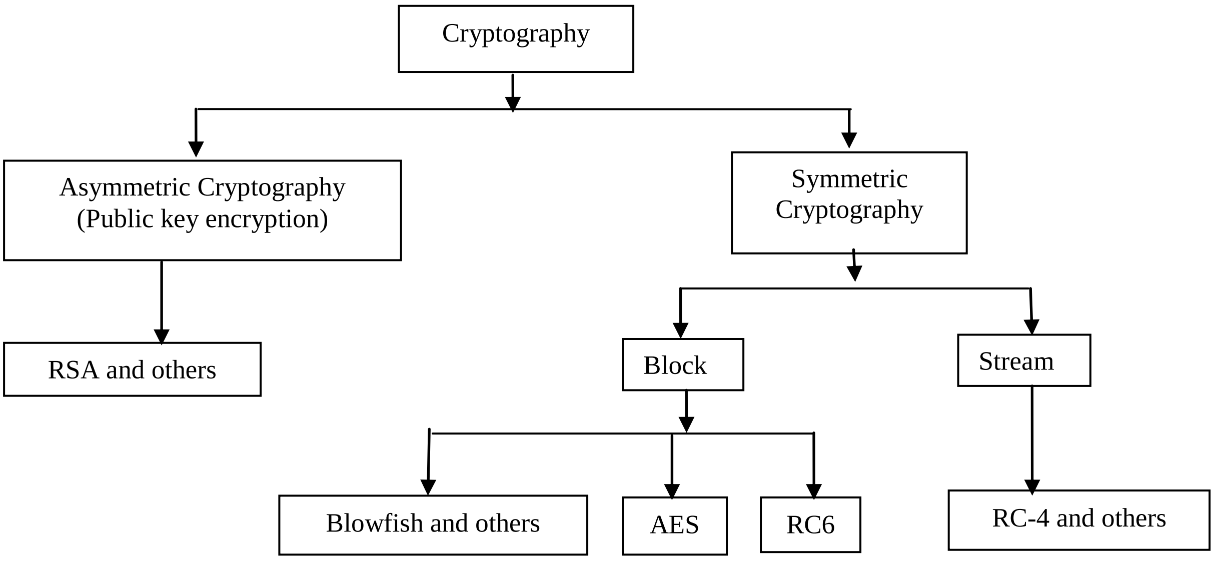

Fig 2. Cryptographic Algorithms Categories

Fig.2 shows cryptographic algorithm selection is done on, what type of application and data to be used for privacy preservation? Symmetric cryptography has two categories block and stream, on the basis of application requirement we are going to select well suitable algorithm for application. Hence before implementation of any algorithm you should know information about application and database workflow.

III. PROPOSED WORK

As shown in Fig. 3 we have to protect image data privacy which is stored in public cloud, using hybrid cloud structure. So, by removing sensitive data form original data and store them separately in trusted private cloud. [1] Rest remaining the processed data stored in un-trusted public cloud. [4] (i.e. non sensitive data) If we decided to store entire image as sensitive data in private cloud then, may be it would require highly storage space in private cloud. Some performance factor we have to consider for image data privacy via hybrid cloud and at the same time try to reduce the following overheads: (1) load ratio of data stored in private cloud, (2) private and public cloud communication overhead and (3) Over all delay introduced between private and public cloud communications to complete data life cycle. [3][5][6]

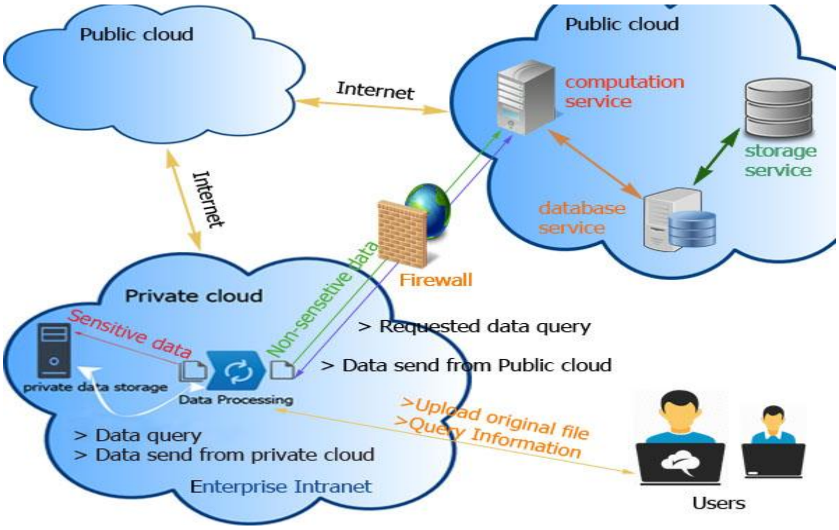

Fig. 3. Architecture of Big Data Privacy Preserving in Hybrid Cloud Environment

As shown in Fig. 3 both cloud uses storage space, it is very difficult to decide performance of hybrid cloud for overall architecture. To understand performance of hybrid cloud, refer Table. 2 as shown below. [1][4][5]

Table 2. Types of Cloud environment

Points	***Public cloud***	***Private cloud***	***Hybrid cloud***
Storage and Access	Storage is on premises of cloud storage service provider, and is accessed using network services.	Storage is on client's premises OR client's dedicated environment. Accessed Using the client's intranet.	Public and private mixed premises for storage data and access.
Database Management Tasks	Database tasks such as database storage, upgrading and replacing, are carried out by the cloud storage service provider.	Database task carried out by client OR can be (Outsourced) to a service provider.	Task can be handled with public and private cloud communication, sensitive data is stored on private cloud and non-sensitive data is on public cloud.

Security of Data	Acquiring CAPEX storage facility so, in concern of security facility public cloud is less secure.	Storage is more secure behind the enterprise firewall.	It is more secure than private and public cloud because storage operation of data is divided on two clouds. (public and private)
Over all Resources Allocation and Costing	Resources allocation are scalable, up or down to meet the customer requirements. Costing is much more than private cloud. Due to CAPEX.	Are scalable and costing is less than public because of its own infrastructure.	Resource allocation and costing is Depends on the public and private resource infrastructure strength. More efficient fast access but not as private cloud.
Property of Multi-tenancy and virtualization	Satisfies but consistency of data is insecure.	Satisfies with data consistency, Due complete private infrastructure.	This property is depends on application type in hybrid cloud.
Service Applications Examples	Services Applications such as Amazon EC2, Gmail, and Office365 and Drop box.	Application used by small scale Industries IT as well as non IT companies.	Business critical data application such as (payroll processing, HR, finance)

As shown in Table. 2, we proposed comparative survey of public, private and hybrid cloud environment.

IV. Privacy preservation of image data

In this section survey carried out to show Different Image encryption algorithm and there performance to implement in cloud application. [3] There is lot scope for image privacy preservation in hybrid cloud application such Home security application, [2] Bank transaction, medical data analysis such as cancer patient. [1] Here Fig. 4 shows original image before encryption and Fig. 5 shows image after encryption.

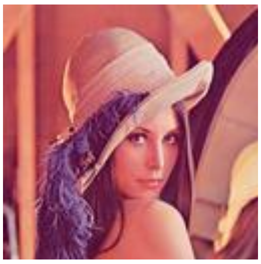

Fig. 4. Original Image

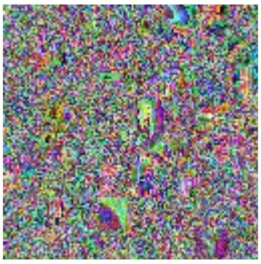

Fig. 5. Encrypted Image

A. Image encryption Survey points on cloud environment

- As shown in Table. 3 These comparison factors are taken on basis of survey.
- We are going to compare Symmetric block cryptographic algorithm for example AES, Blowfish and RC6. [3]
- Due to Hybrid Cloud nature it is efficient to implement Symmetric block cryptographic algorithmic approach to separate the sensitive data and non-sensitive data. [3]
- Image size is not matter for block level cryptography. [1]
- We have to consider such Encryption algorithm that will reduce the communication delay between Private and public cloud communication. [1]

- Different image encryption algorithms has been proposed for security analysis. Simulation able take on all parts of the image encryption system using MATLAB. Here in Security analysis covers 1) histogram analysis, 2) correlation analysis, 3) entropy analysis histogram analysis, shows that histogram of cipher image is flat or uniformly distributed. [2]

B. Comparison of Algorithms and Performance Review

Table 3. Comparison of AES, Blowfish and RC6 Symmetric cryptographic algorithm

Comparison Factors	***AES***	***BLOWFISH***	***RC6***
Length Of Key	128, 192 OR 256 bits	32-448 bits	128, 192 OR 256 bits
Cipher type	Symmetric Block Cipher	Symmetric Cipher Algorithm	Symmetric Algorithm
Block Size	128,192 OR 256 bits	64 bits	128 bits
Developed	In 2000	In 1993	In 1998
Properties in Terms of Resistance Cryptanalysis	Strong against differential, Truncated, Linear, Interpolation And square attacks	Vulnerable to differential Brute force attacker	Vulnerable to differential Brute force attacker
Security	Considered secure	Vulnerable	Vulnerable
Rounds	10(128-bits) 12(192-bits) And for 14(256-bits)	16	20
Possible Keys	2^128, 2^192 OR 2^256	2^32, 2^448	2^128, 2^192 OR 2^256
Possible ASCII Printable Character Keys	95^16, 95^24 OR 95^32	95^4, 95^56	95^16, 95^24 OR 95^32
Time Required to Check all Possible Keys at 50 Billion Keys Per Second	For 128-bit key: 5*10^21 Years	For 448-bit key: 10^116 Years	For 192-bit key 10^40 Years

Here in Table. 3 we did comparative study of three different block symmetric cryptographic algorithm AES, Blowfish and RC6.

V.Conclusion and Future Work

To promote Hybrid cloud computing is an efficient solution for big data privacy preservation. Our proposed survey carried out for image big data privacy preservation, select proper image cryptographic technique to reduce delay or communication overhead between public and private cloud. To make an efficient solution and to make an NP Complete solution of image encryption problem on hybrid cloud environment. AES algorithm is standard algorithm comparison to select an effective algorithm for proposed architecture. In cryptographic algorithm survey we test that performance of image encryption algorithm and review of different image cryptographic approach for hybrid cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

REFERENCES

1. Xueli Huang and Xiaojiang Du, "Achieving big data privacy via hybrid cloud", IEEE INFOCOM Workshops: 2014 IEEE INFOCOM Workshop on Security and Privacy in Big Data, 978-1-4799-3088-3/2014.
2. Rajinder Kaur[1], Er. Kanwalpreet Singh[2], "Comparative Analysis and Implementation of Image Encryption Algorithms", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue. 4, pg.170 – 176, April 2013.
3. Ms. Ankita Umale[1], Ms. Priyanka Fulare[2], "Comparative Study of Symmetric Encryption techniques for Mobile Data Caching in WMN", The International Journal of Engineering and Science (IJES) Volume 3 Issue 3 Pages 07-12 2014.
4. Larry Coyne[1], Shivaramakrishnan Gopalakrishnan[2], John Sing[3], "Public and Hybrid Cloud Storage Solutions", International Technical Support Organization IBM Private, Public, and Hybrid Cloud Storage Solutions, © Copyright International Business Machines Corporation 2012, 2014 REDP-4873-01. July 2014.
5. Sreeranga Rajan[1], Wilco van Ginkel[2], Neel Sundaresan[3], "Cloud Security Alliance Top Ten Big Data Security and Privacy Challenges", Cloud Security Alliance © Copyright 2012.
6. Kalyani Shirudkar[1], Dilip Motwani[2] "Big-Data Security", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 3, March 2015.
7. Anjana Gosain[1], Nikita Chugh[2], "Privacy Preservation in Big Data", International Journal of Computer Applications (0975 – 8887), Volume 100 – No.17, August 2014.
8. Alexandre Devaux[1], Nicolas Paparoditis[2], Fr´ed´eric Precioso[3], and Bertrand Cannelle[4], "Face Blurring for Privacy in Street-level Geoviewers Combining Face, Body and Skin Detectors", MVA2009 IAPR Conference on Machine Vision Applications, May 20-22, 2009.
9. Hsinchun Chen[1], Roger H.[2], L. Chiang[3], "BUSINESS INTELLIGENCE AND ANALYTICS: FROM BIG DATA TO BIG IMPACT" *MIS Quarterly Vol. 36 No. 4, pp. 1165-1188/December 2012.*
10. Anjana Gosain, Nikita Chugh, "Privacy Preservation in Big Data", International Journal of Computer Applications (0975 – 8887) Volume 100 – No.17, August 2014.

DOI: 10.15680/IJIRCCE.2015. 0311028