Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P) Vol. 7 No. 2, 2018, pp.67-73

DOI: https://doi.org/10.51983/ajeat-2018.7.2.1007

Privacy Preserving Technique for Data Storage in Cloud Computing

Jagpreet Kaur[1] and Nitin Goel[2]
[1&2]Department of Computer Science, Chitkara University, Punjab, India
E-Mail: jagpreet.kaur@chitkara.edu.in, nitin.goel@chitkara.edu.in

(Received 20 June 2018; Revised 10 July 2018; Accepted 30 July 2018; Available online 10 August 2018)

***Abstract* - With the emergence of Cloud computing, the traditional computing process has undergone a sea change. Cloud Computing has been proving to be a boon for IT industries in terms of its ability to provide cost effective, power efficient, extensible and pliable computing. Because of its substantial flexibility, Cloud Computing has become an escalate platform for the services of next generation. But inspite of all the advantages, security and privacy of the data being shared on Cloud remains a cause of concern for the users as well as service providers. This paper proposes a 'Tortoise technique' aiming to provide more privacy to user's data without any kind of security threats from outside. As a part of the technique, reduced data is sent to cloud instead of the original encrypted data. We observed an improvement to an order of 2^n in the security of data with the help of the proposed technique.**

Keywords: **Edge Detection, Cloud Computing, Privacy, Randomisation**

I. INTRODUCTION

Quantifying the volume of data that exists all around the globe is arduous. What is clear is that every organization has abundant of data, and that too increasing at a terrific rate day by day. Today the availability of plentiful information allows medium and large organizations to recognize that just by moving into the cloud they can acquire ample amount of storage or raise their infrastructure resources, all at a very low cost. According to Gartner (Heiser,2009) Cloud Computing is "a way of computing where enormously scalable IT- enabled capabilities are delivered 'as a service' to external customers using Internet technologies". Hence, internet plays a vital role in the society by providing exchange of information and communications of a heavy volume. With the great use of advances in technology, the internet has stepped into a new field. Rather than running software locally on a system, one can be able to use the "Cloud". The phrase "Cloud Computing-successor of internet" is not wrong (Mell, 2011;Dikaiakos, 2009). But Cloud Computing and internet computing is not exactly one and the same thing. While Internet is a tool, Cloud Computing is a service. One can ingress this service via internet, whenever needed.

Cloud Computing is defined as an umbrella which is being put into use under multiple conditions. It is neither a particular technology, nor a particular architecture. On the other hand, it is an inceptive and quickly evolving model which consists of an existing technology combined with a new technology paradigm so as to provide the market with heavy cost reduction. The term "Cloud" is a collection of servers, storage systems and devices in which instead of running software locally on a system, it is being used remotely (Brian, 2008). One can also learn about Cloud Computing paradigm in the same way as- "At home you don't have electricity generators, but your home is connected with a set of wires, demanding a service from a provider company and you pay for what you use. The more electricity you use, the more money you pay." The idea of Cloud Computing is pretty much the same, replacing electricity by Cloud Computing services and the wires by an Internet connection. Because of its huge quantum of flexibility, Cloud Computing has the prospective to be the imminent unruly wave. There is no single meaning of Cloud Computing as yet, however the National Institute of Standards and Technology (NIST) have defined it as follows (Mell, 2011). Figure1 is illustrative of the summary of capabilities of Cloud Computing system.

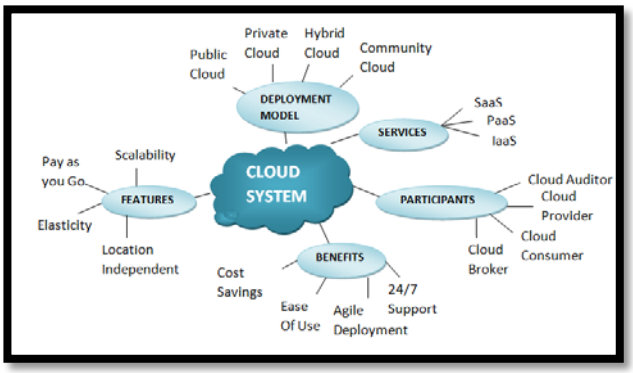

Fig. 1 Capabilities of Cloud System

A.The Cloud Deployment Models

Cloud Deployment Models are based upon the standards for retrieving and, securing applications and data. Depending on these standards, Clouds are classified into four types as described below (Mell, 2011).

*1. Public Cloud:*This model (GTSI, 2009;Krutz, 2010) is made accessible to all the cloud users. It can be possessed, maintained, and controlled by an enterprise, an educational institute, or a Government Company, or some integration of these, and exists on the premises of the Cloud. Moreover, it provides various advantages to users, including lower costs, no investment on infrastructure. However, users have low degree of control as it is shared with multiple untrustworthy parties which results in immense amount of security and privacy concerns. Examples: AmazonEC2, Windows Azure.

*2.Private Cloud:*Theinfrastructure is aimed to be used entirely by one company consisting of multiple users. This is also known as an internal Cloud. This system is maintained, possessed and operated completely by the organization, and may be 'on' or 'off' premises. Moreover, this model provides the highest degree of control over performance, security and reliability. Example: eBay, Attenda RTI.

*3.Community Cloud:*This is intended for organizations that share their framework among a few other organizations and support a particular group with some common interests (e.g., security necessities, consistence, location, and so on.).It might be overseen, headed and controlled by one or more organizations in the group, or a combination of the same, and may exist 'on' or 'off' premises. Examples: Zimory, RightScale, G-Cloud of UK.

*4.Hybrid Cloud:*This Cloud System is an amalgamation of two or more diverse cloud foundations that stay as unmistakable entities; however these are bound together by some institutionalized innovation that empowers information flexibility and information application mobility. These types of Cloud Systems are turning out to be progressively more prominent; however, integration of these Cloud Systems presents some security challenges. Illustration: Juniper.

B. The Cloud Service Models

Depending upon the abstraction level provided and the service model of providers, CSP's (Cloud Service Providers) offer the services to the users according to three basic delivery models (GTSI, 2009; Bohn, 2011;Ramgovind, 2010): *Software as a Service,Platform as a Service,Infrastructure as a Service*. The services offered are often categorised using the SPI delivery Models. This model represents the level of abstraction, and can be considered as a framework divided into various layers where resources of lower level layer have been being served to higher level. The descriptions of these delivery models are as under (Peng, 2009):

1. Software-as-a-Service (SaaS): This is the foremost layer (GTSI, 200).In the SaaS delivery model; customers take software on lease under a grant basis or on the basis of pay-per-use and access software through internet. Users' have privilege to access the software service but cannot modify it. Moreover, software is not installed on end user system but is assembled on the Cloud itself. Some examples of SaaS model are: Cloud9 Analytics, Antenna Software, CVM Solutions, Zoho.com (Zoho), Google Docs (Google Docs).

*2.Platform as a Service (PaaS):*This layer represents a development platform (GTSI, 2009), on which clients' can deploy, compose and oversee applications that run on the cloud. PaaS make use of dedicated API's (Application program interface) toolkits and standards for building web-applications. These tools are focused at providing monitoring of application and user activities, unification with external web services and databases, security, reliability and, scalability, multi-tenancy and billing mechanisms without excessive development. Instances of PaaS as shown in Table I below

TABLE I PAAS EXAMPLE

Cloud Service Provider	Runtime Environment
Acquia Cloud	Php
Webappcabaret	java, php, python, ruby, scala
Heirloom PaaS	cobol, java
OpenShift Enterprise	java, node, perl, php, python, ruby, extensible

*3.Infrastructure as a Service (IaaS):*This is the final and lowest layer (GTSI, 2009). In this delivery model, CSP offers highly elastic and superior IT infrastructure (virtualised servers, storage, processing power, database, memory, Content Delivery Network (CDN)...) used to run applications and operating system through virtualization technologies like Vmware (Vmware). Instances of IaaS model are Amazon Simple Storage Solution (S3), Amazon Elastic Compute Cloud (EC2), Rackspace Cloud, and Microsoft Live Mesh.Section 2 describes some existing security issues.Section 3 describes the background of problem. Section 4 serves the proposed solution, delivers the algorithm and the working principles of the proposed solution Section 5 draws the conclusion.

II. SOME EXISTING SECURITY ISSUES

Cloud Computing improves software capabilities and elevated IT to newer limits by providing cost effective, power efficient and pliable computing. As indicated by another expectation from International Data Corporation, worldwide devouring public IT cloud administrations was $47.4 billion in 2013 and according to new update it will reach $122.5 billion in 2017, and by 2020 it is expected to reach $203.4 billion worldwide(IDC, 2017). Besides the success cloud lies in the term "multi-tenancy", this is curse in ecstasy for the cloud, because several organizations share the identical infrastructure provided by a different organization. As a result safety of the outsourced data lies solely under the management of a different organization. This is one of the major reasons behind data vulnerability in cloud and poses many new security and privacy challenges (Singh, 2012). International Data Corporation (IDC) had conducted a survey in the year 2008 and 2009 on cloud services, 74% IT CIOs and managers believed that security issues are the vital issue that cease users from using cloud services in cloud computing (Parsi, 2015).This survey concludes that for smooth and sustained implementation of cloud, there is much need for strong security mechanisms. In this section authors have recognized few security issues as shown by the International Standards Organization (ISO) 7498-2 (IEC, 1989).Some of the security issues like Data loss, Insufficient due diligence etc have already been brought up by us only (Kaur,2015). The security

requirements are described below in context of cloud data security.

A. Identification and Authentication

This phenomenon (IEC, 1989) ensures the ingress control of the cloud by authenticating cloud users. The authentication can be done by MAC address, User-id, password, firewalls, IP address or any other mechanism.

B. Confidentiality

Confidentiality provides that only authorized clients have permission to access and manipulate data. It guarantees that data which resides with in the cloud cannot be disclosed to unapproved persons. It plays a major role primarily in maintaining organization's data spread across multiple distributed databases. Multi-tenancy plays a major role in introducing a number of confidentiality threats. In breaching confidentiality, data remanence also plays a vital role. Data remanence is the ability to retain the stored data that have been removed in some ways. As client works on single infrastructure separated virtually, this retention leads to disclosure of private data. Confidentiality can be achieved when clients and servers encrypt their exchanges in proper way (Tianfield, 2012).

C. Integrity

Integrity is one of the decisive components in any system. It guarantees that data locale in a scheme is a suitable delineation of the data expected and that it can only be modified by authorized person. Usually it refers to protect data from illegitimate alteration or deletion. Data Integrity in Cloud Computing is maintained via database ACID properties. Data Integrity can be achieved by various techniques such as Digital Signatures, RAID etc. At the point when any application is running on a server, to make it safe in case of information loss episode reinforcement routine is designed. Ordinarily, the data will reinforcement to any compact media on a consistent premise which will then be put away in outer area (Tianfield, 2012).

D. Non-Repudiation

Non-repudiation (IEC, 1989) provides security against deny of communication between two communicating parties. Repudiating interactions are generally thwarted by some authorizing protocols. These systems are in this way utilized for access control. Amongst others, trade of public keys, digital signatures are likewise included.

E. Availability

Availability refers to the property of any system that is available and accessible on demand at all times. Accessibility can be influenced shortly or permanently. Network failures, Natural Disasters, Hard disk failure, Active attacks etc leads to breach availability. This concern is usually key element for mission basic frameworks. As organizations have business continuity plans (BCP's), hence accessibility for these frameworks is essential (Tianfield, 2012).

III. BACKGROUND

The main cloud computing providers individually appeared various accidents. On March 10, 2009, Google announced that a flaw in Google Docs had permitted unexpected access to some private records. Even in February and July 2009, Amazon's Storage Service was also interrupted twice. To lessen these worries, a cloud provider must assure that customers can keep on having the comparative protection and security controls over their applications, for they are the ones who will shoulder the responsibility if things go wrong (Subashini, 2011).

In recent days, it has been seen that data mining has been used by cloud providers to provide better service to its users (Liu, 2004). Also many profitable approaches in data mining has been reported from various areas such as medical, marketing, finance etc but apart from the benefits data mining results in revealing of valuable knowledge or the personal information of individuals without their permission. If cloud providers too misuse the personal information of users' then client privacy is jeopardize. Basically, the intent of implementing data mining techniques through cloud is to extract structured information from an unstructured data but the issue lying at the place as data mining works by assessing individual's data. And this leads to privacy loss and also information loss (Modak, 2014). Techniques are summarized as below (Lindell, 2002;Verykios, 2004;Aggarwal, 2008; Nayak, 2011; Qi, 2012):

A. Anonymization Technique

While releasing micro data, disclosure risks must be limited and maximize the data utilization (Malik, 2012). To achieve this, *k*-anonymity privacy model was introduced by Sweeney (Sweeney, 2002). This model was achieved using suppression and generalization according to which each record in anonymized table must be identical with at least k-1 other records with respect to quasi-identifier attribute in the anonymized dataset(Sweeney, 2002;Samarati, 1998). Anonymization is a technique in which record owner's identity or sensitive data remain hidden (Agrawal, 2000;Aggarwal, 2008). Table II shows a set of Patient's record. Table III represents registration list of Voter's. Table IV represents an instance of 2-anonymized data set for Table II.

TABLE II PATIENT'S RECORD

ID	AGE	GENDER	ZIP CODE	DISEASE
1	25	MALE	73661	COUGH
2	27	MALE	73634	COUGH
3	31	MALE	63967	FEVER
4	39	FEMALE	63949	TOOTHACHE

TABLE III REGISTRATION LIST OF VOTERS

ID	NAME	AGE	GENDER	ZIP CODE
1	TOM	25	MALE	73661
2	LILY	27	MALE	73634
3	RAM	31	MALE	63967
4	KIM	39	FEMALE	63949

TABLE IV A 2-ANONYMUS DATASET OF TABLE II

ID	AGE	GENDER	ZIP CODE	DISEASE
1	2*	MALE	736*	COUGH
2	2*	MALE	736*	COUGH
3	3*	*	639*	FEVER
4	3*	*	639*	TOOTHACHE

Sensitive data in Patient's data is disease. Quasi identifiers age, gender, zip code are available both in micro-data as well as voter registration list that is publicly available as shown in Table II and Table III. Even with registration list of voters, a foe can deduce that Tom may be the individual entailed in initial two rows of Table II, or correspondingly, the disease of Tom is revealed only with 50% Probability. Hence k-anonymity provides protection against identity disclosure but it does not protect attribute disclosure as limitation of k-anonymity originates from two assumptions. While it ensures that transformed data is true but at the same time it suffers homogeneity and background attack (Malik, 2012). Moreover, linking attack is accomplished by linked outer tables which contain the identities of individuals and the public attributes.

B. Randomisation Technique

Randomisation has been usually used as a part of distorting data by probability distribution for methods such as survey (Warner , 1965).The method of randomization can be described as follows (Agrawal , 2000;Aggarwal, 2008): Consider a set of information represented by P= {p1, p2...pN}. Probability distribution fB (r) is used to obtain a noise component which is being added to record piϵ P. Independent of data, the noise components are produced and are represented as r1,r2....rN. Hence, new distorted information is p1+r1.....pN+rN and can be represented by s1...sN where si ϵ S. Thus the complete relation can be represented by

$$S = P + R$$
$$P = S - R$$

As shown in (Aggarwal, 2008) the noise added is enormously large so that specific values cannot be retrieved and only the distribution is recovered which leads to loss of individual's information.

C. Cryptographic Technique

B. Pinka's*et al.*, (Pinkas, 2002)proposed Cryptographic technique. It develops a well outlined model for privacy that involves ways for quantifying and proving it. However, a huge set of cryptographic algorithms are available which prevent privacy leak, but it doesn't ensure output of computation. Moreover, technique becomes difficult when more than a few parties are involved and hence difficult to deal with. Likewise, it doesn't address the question of whether or not the exposure of the final data mining result could violate the privacy of individual records.

D. Condensation Approach

Charu C. Aggarwal and Philip (Aggarwal, 2004)introduced Condensation approach. Instead, other techniques works with modifications of original data, this approach works with pseudo-data, hence helps in preserving privacy better than other techniques (Aggarwal, 2004). It constructs clusters of similar size and generates pseudo-data. However, it gives information loss.

IV. PROPOSED TECHNIQUE

In this paper we are proposing Tortoise technique. As with tortoise if he perceives himself in jeopardy, he hides into its shell to preserve from outside danger. Similarly, in this we are using an image to compare the dataset with the edge pixels without changes the properties of image data and send the randomized index values in the form of text file on to the cloud.

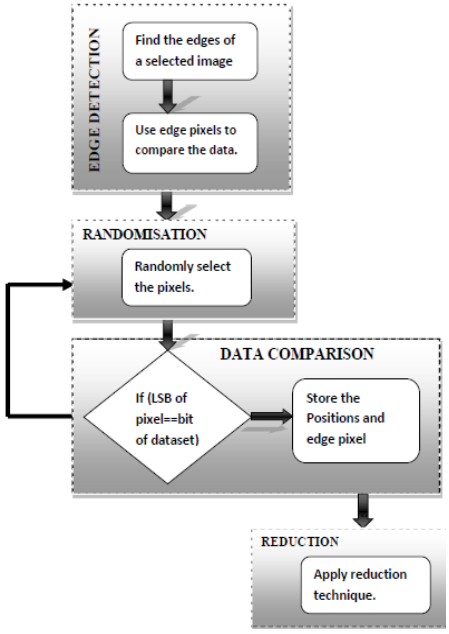

Fig. 2 Flowchart of Proposed Technique

An image which is a collection of numbers that constitutes distinct light intensities in distinct region of the image and this numeric representation forms a grid. Also, the independent points are said to be pixels. This technique is divided into four phases and each phase outputs a result which is to be used as input to next phase.Figure2 describes the flowchart used to explain the Tortoise technique.

A. Phases

1. Edge Detection Phase

Edges characterize object boundaries. Edges usually exist on the boundary between two distinct regions in an image.

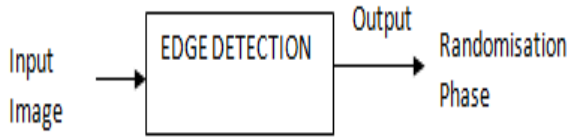

Fig. 3 Edge Detection Phase

Edge detection let user to discover those characteristics of an image where there is a less or more sudden change in texture or gray level representing the end of one region and the beginning of another in the image. Edge detection of an image diminishes notably the amount of data and refines the information that may be considered as less pertinent, preserving the chief structural properties of an image. There are number of edge detectors. In this work we are using Canny Edge Detector as it diminish the probability of identifying false edge, and gives sharp edges.

The Canny edge detection algorithm has the following five stages (Bassil , 2012; Jain, 2012).Moreover, the canny algorithm has two basic adjustable parameters, the size of the Gaussian filter and the threshold. Image is in the form of 2-D matrix or 2-D array. Hence, Store all the edge pixel values with their positions i.e. its row and column into an array named as Position Array.

For example:
P (i, j, x) where P is the pixel with i= i^{th} row, j= jthcolumn and x= value of the pixel on that address.

2. Randomisation Phase

In this phase, after storing the detected edge pixel values and their positions into that Position array provided this array is having one more column named as Index Values representing index of that array, hencerandomly select the index value from Position array by using random function generator.

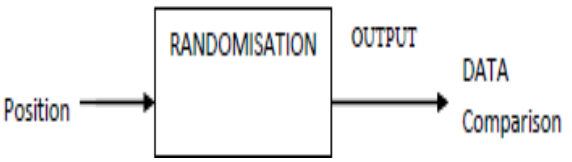

Fig. 4RandomisationPhase

The way the array index is generated randomly means that the pixel values of the image are random and message bits are compared to the randomised pixels. For example: array having values as shown in Table V.

TABLE V POSITION ARRAY

INDEX VALUES	I	J	x
0	89	3	8
1	90	3	17
2	92	3	29
3	95	3	55
4	111	3	1
...	...	...	...

Where I and J are positions stated rows and columns,X is pixel value, Index Values representing index of an array beginning with Zero. After this random function generator is used to select the random index values and correspondingly select the pixel value. For instance: by applying random function generator got the index value 3 and correspondingly pixel value is 55.

3. Data Comparison Phase

This phase describes as

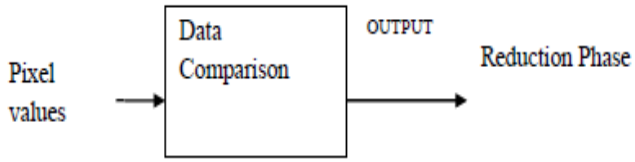

Fig. 5 Data Comparison Phase

This phase is accomplished using following steps

a. After pixel value is selected using randomisation, LSB (Least Significant Bit) comparison is done. This is described as below and shown in Figure 6.
   1. If the LSB of the pixel value P (i, j) is equal to the message bit m, store the positions and pixel values. Else
   2. Again choose another pixel value using randomisation and repeat the process.

$$Ls(i,j)= \begin{cases} \text{LSB } (P(i,j)=1) \text{ and } m=0, \text{ ignore that LSB} \\ \text{LSB } (P(i,j)=0) \text{ and } m=1, \text{ ignore that LSB} \\ \text{LSB } (P(i,j)=0) \text{ and } m=0, \text{ then,} \\ \quad ((\text{binary value of Pixel} \,\&\, 0xFE) \mid m) \\ \text{LSB } (P(i,j)=1) \text{ and } m=1, \text{ then,} \\ \quad ((\text{binary value of Pixel} \,\&\, 0xFE) \mid m) \end{cases}$$

Fig. 6 LSB Comparison Procedure

For example: let the pixel value be 55 with binary representation 0110111. This pixel value is having LSB 1 and if message bit is also 1 store the positions and corresponding pixel values, otherwise again find another pixel value using randomisation.

b. This procedure works until all message bits of the dataset are not compared with LSB.

4. Reduction Phase

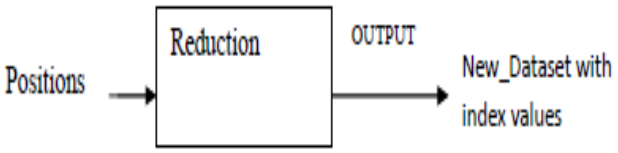

Fig. 7 Reduction Phase

Reduction is done in the way that instead of storing the positions and corresponding edge pixel values of Position Array with which our message bit is compared, we will store the corresponding index values of that array into a text file and send this text file to cloud. And at our local end store that array containing edge pixels and their positions.

V. ALGORITHM FOR ENCODING TEXT DATA

Inputs: Dataset, RGB image
*Output:*New_Dataset with Indexes

Begin
Step1: Take the RGB image as input.
Step2: Detect the edges by applying canny edge detection method.
Step3: The pixels constitute the edges are denoted by X. I, J constitute the positions of the edge pixel such thatP (i, j, X). Put them into a Position Array.
Step4: Read character from Dataset that is to be compared and convert the ASCII value of the character into equivalent binary value of 8 bits.
Step5: For each message bit m initialize random function generator and randomly select index value of Position Array.
Step6: Extract the pixel value from that index and check it's LSB; if LSB matched with the message bit then store the positions corresponding to that pixel value, otherwise ignore and find the index value again by random method.
Step7: Instead of sending the positions and edge pixel value, Store the randomly generated index values corresponding to pixel values into a text file i.e. New_Dataset with indexes and send that file to cloud.
End;

VI. ALGORITHM FOR DECODING TEXT DATA

Inputs: New Data set with indexes, Position Array as a key**.**
*Output:*Original Dataset.

Begin
Step 1: Fetch the New_Dataset with indexes from the cloud.
Step 2: Take Position Array which stores at local end and act as a key.
Step 3: Match the index value with the Position Array index value which is stored at the local end.
Step 4: Corresponding to that index value in Position Array, check the pixel value.
Step 5: Extract the LSB of that pixel value and store them into an array B.
Step 6: Repeat this process for every index value which is fetched from the cloud.
Step 7: Convert the array B into characters and the resultant forms the original dataset.
End

Hence, this technique concludes with a new dataset in an unreadable format which is sent on to the cloud. Intruders or third parties didn't get the actual dataset. And hence privacy of an individual should be maintained. To read the data, download the file from cloud and get the original records back without the loss of information.

VII. CONCLUSION

Cloud Computing is envisaged as the next unruly wave. But besides its advantages, preserving privacy is one of the major issues that become an impediment in the escalation of Cloud Computing. One of the most popular techniques of PPDM was used in Cloud Computing to preserve privacy but none of the techniques addresses the issues properly. Hence, the key conclusion of this thesis is that, in above techniques linking attack is achieved from Public available data. Moreover, instead of Original data only distribution was constructed which leads to information loss. A proposed technique called The Tortoise technique in Cloud Computing Environment which aims to provide privacy without any loss of information. By this the sensitive information of individual remains preserve. As in this technique randomly generated index values corresponds to the pixel values of picked image is sent on the cloud instead of actual data therefore it becomes very difficult to restore actual data without recognizing that what these bits and bytes actually point to.

REFERENCES

[1] J. Heiser, "What you need to know about cloud computing security and compliance", *Gartner, Researc*h, ID Number: G00168345, 2009.
[2] Peter Mell and Tim Granc, "The NIST definition of cloud computing", 2011.
[3] Dikaiakos, D. Marios, Dimitrios Katsaros, Pankaj Mehra, George Pallis and Athena
[4] H. A. Y. E. S. Brian, T. Brunschwiler, H. Dill, H. Christ, B. Falsafi, M. Fischer and M. Kaiserswerth, "Cloud Computing", *Communications of the ACM*, Vol. 517, pp. 9-112008.
[5] GTSI Group, "Cloud computing-building a framework for successful transition", *White Paper, GTSI Corporation*,Vol. 2, No. 9, 2009.
[6] Krutz, L. Ronald and Russell Dean Vines, "Cloud security: A comprehensive guide to secure cloud computing", Wiley Publishing, 2010.
[7] R. B. Bohn, J. Messina, F. Liu, J. Tong and J. Mao, "NISTcloudcomputingreferencearchitecture",*IEEE*, pp. 594–596. 2011.
[8] Ramgovind, Sumant, Mariki M. Eloff and Elme Smith, "The management of security in cloud computing", *In Information Security for South Africa ISSA,IEEE*, pp. 1-7, 2010.
[9] Peng, Junjie, Xuejun Zhang, Zhou Lei, Bofeng Zhang, Wu Zhang and Qing Li, "Comparison of several cloud computing platforms", In *Information Science and Engineering ISISE, Second International Symposium, IEEE*, pp. 23-27, 2009.

[10] Zoho. [Online]. Available: http://www.zoho.com
[11] Google Docs. [Online]. Available: http://docs.google.com
[12] Vmware. [Online]. Available: http://www.vmware.com
[13] IDC.2017. [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS42321417
[14] R. Singh, S. Kumar and S. K. Agrahari, "Ensuring data storage security in cloud computing", *IOSR Journal of Engineering*, Vol. 212, 17-21.2012
[15] K. Parsi, "Security Concerns of Data in Cloud Environments", 2015
[16] International Electrotechnical Commission, *Information Processing Systems, Open Systems Interconnection: Basic Reference Model. Part 4, Management Framework*, [Geneva]: ISO/IEC, 1989.
[17] Kaur, Jagpreet, Sunny Singh and AmitKam, "Analysis of security issues and management standards in cloud computing", In *Computing for Sustainable Global Development INDIACom, 2nd International Conference, IEEE*, pp. 1474-1478, 2015.
[18] H. Tianfield, "Security issues in cloud computing", *In Systems, Man, and Cybernetics SMC, IEEE International Conference*, pp. 1082-1089, Oct. 2012.
[19] Subashini, Subashini and VeerarunaKavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, Vol. 341, pp. 1-11 2011.
[20] Liu, Ying, JayaprakashPisharath, Wei Keng Liao, GokhanMemik, AlokChoudhary and PradeepDubey, "Performance evaluation and characterization of scalable data mining algorithms", In *Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems*, ACTA Press, Vol. 16, pp. 620-62, 2004.
[21] Modak, Masooda M. Aslam and M. Vijayalakshmi. "Privacy preserving data mining techniques in the cloud: A comparative analysis", *In VESIT, International Technological Conference, I-TechCON*, 2014.
[22] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin and Y. Theodoridis, "State-of-the-art in privacy preserving data mining", *ACM Sigmod Record*,Vol. 331, pp. 50-57. 2004
[23] Y. Lindell and B. Pinkas, "Privacy preserving data mining", *Journal of Cryptology*,Vol. 153, 2002
[24] Aggarwal, C. Charu and S. Yu Philip, "A general survey of privacy-preserving data mining models and algorithms", *InPrivacy-Preserving Data Mining, Springer*, Boston, MA, pp. 11-52, 2008.
[25] Nayak, Gayatri and Swagatika Devi, "A survey on privacy preserving data mining: approaches and techniques", *International Journal of Engineering Science and Technology*,Vol. 3, No. 3, 2011.
[26] Qi, Xinjun and MingkuiZong, "An overview of privacy preserving data mining", *Procedia Environmental Sciences*,Vol. 12, pp. 1341-1347, 2012.
[27] M. B. Malik, M. A. Ghazi and R. Ali, "Privacy preserving data mining techniques: current scenario and future prospects", In *Computer and Communication Technology ICCCT, 2012 Third International Conference on* pp. 26-32. IEEE, Nov. 2012.
[28] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression", *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 1005, pp. 571-588, 2002.
[29] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression", Technical report, SRI International, pp. 101-132, 1998.
[30] R. Agrawal and R. Srikant, "Privacy-preserving data mining", *In ACM Sigmod Record*, Vol. 29, No. 2, pp. 439-450. ACM.2000.
[31] S. L. Warner, "Randomized response: A survey technique for eliminating evasive answer bias", *Journal of the American Statistical Association*, Vol. 60309, pp. 63-69. 1965.
[32] B. Pinkas, "Cryptographic techniques for privacy-preserving data mining", *ACM Sigkdd Explorations Newsletter*, Vol. 42, pp. 12-19, 2002.
[33] C. C. Aggarwal and S. Y. A. Philip, "Condensation approach to privacy preserving data mining", *In International Conference on Extending Database Technology, Springer*, Berlin Heidelberg. pp. 183-199, 2004
[34] Y. Bassil, "Image steganography based on a parameterized canny edge detection algorithm", *ArXiv preprint ar Xiv: 1212.6259*. 2012.
[35] N. Jain, S. Meshram and S. Dubey, "Image steganography using LSB and edge–detection technique", *International Journal of Soft Computing and Engineering (IJSCE) ISSN*, Vol. 223, 2012.