Assessing the Security Benefits of Cloud Computing on Security Guidance for Critical Areas of Focus in Cloud Computing

Ms. Sana Parveen[1], Prof. Sarwesh Site[2]

[1]Research Scholar, [2]Assistant Professor

CSE, All Saints College of Technology

Abstract: Cloud computing hides the complexity of framework usage from users. User need not to worry about the storage details of information and data. Maintenance and testing is also not the concern of user.

I. INTRODUCTION

There are many definitions given for cloud computing. The US National Institute of Standards and technologies (NIST) has given a standard definition of cloud computing. According to this definition "Cloud computing is a model for on-request access to a mutual pool of configurable resources (e.g., network, servers, applications, storage and administrations) that can be quickly provisioned and discharged with minimal administration effort and service provider interaction" [2][3].In other words we can say cloud computing is a sort of outsourcing of PC programs. Utilizing cloud computing, clients can get access to programming and applications from wherever they are; the PC programs are being facilitated by an outside get-together and live in the cloud. This implies clients don't need to stress over things, for example storage and power, they can just appreciate the final product. Cloud makes significance to two basic thoughts:

Virtualization: Virtualization is a method, which permits to share a solitary physical occurrence of a resource or an application among different clients and associations [4]. It does by appointing a consistent name to a physical storage and giving a pointer to that physical asset when requested. For better understanding of cloud computing, we have layout the cloud computing in two distinct sets i.e. service models and deployment models.

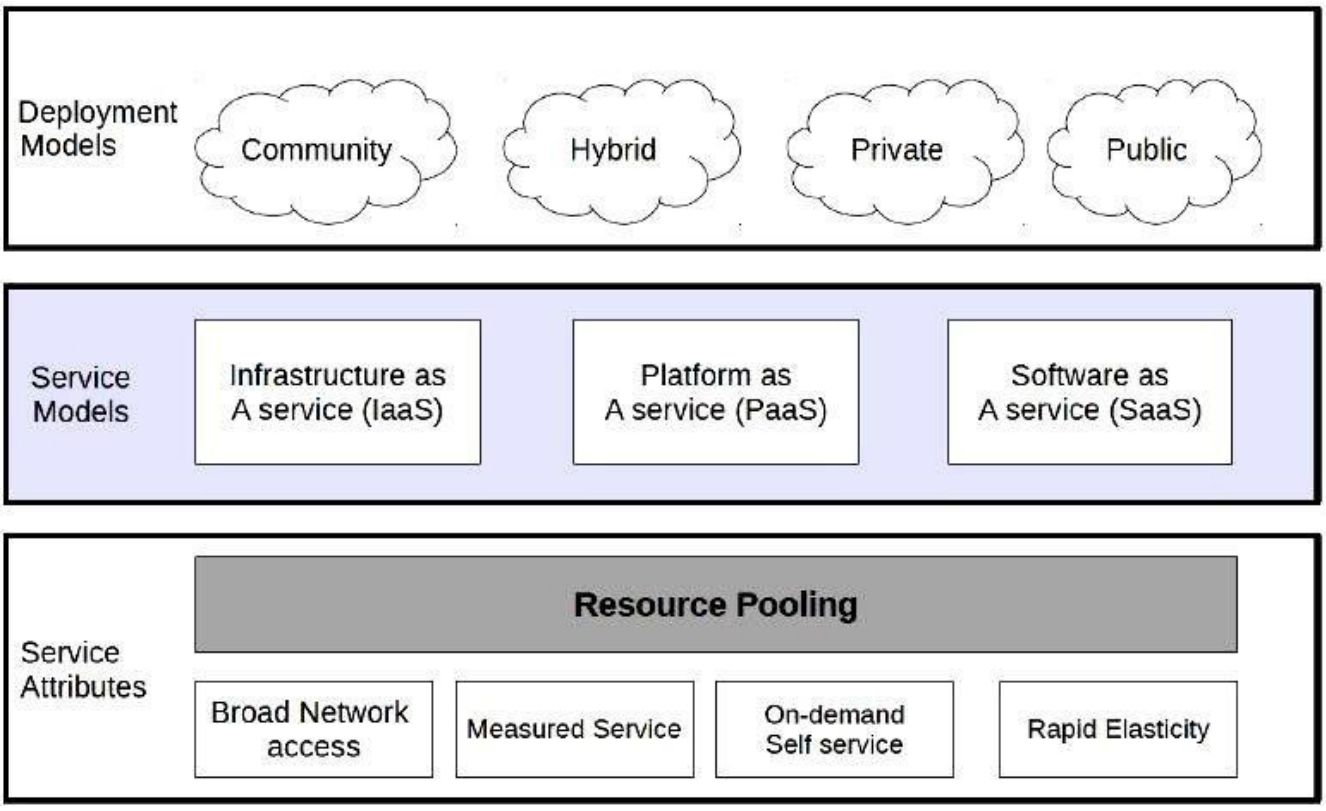

Fig 1.1 NIST Model of Cloud Computing

Service Models of Clouds

These models describe variety of services that user can get through cloud computing.There are various kind of service model in cloud computing. Three main type of service models are covered in this section [5]. They are asfollow:

- Infrastructure as aservice
- Platform as aservice
- Software as aservice

Deployments Models of Clouds

Deployments model signifies the arrangements and executives of the clouds. Deployment models of cloud [6]. There are four deployment models for cloud:

- PrivateCloud
- PublicCloud
- CommunityCloud
- HybridCloud

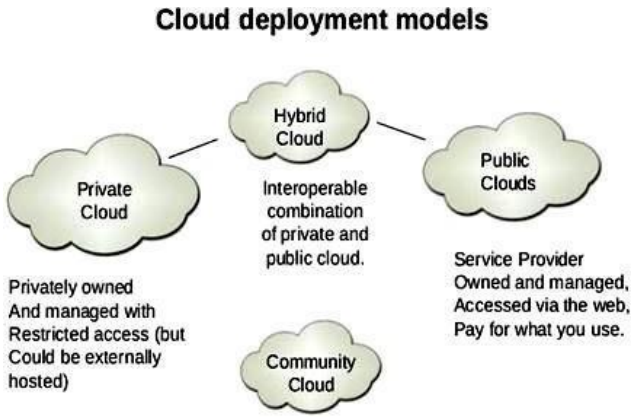

Fig1.2 Deployment Models in Cloud

II. REVIEW OF LITERATURE

KaipingXue et al.[1] " Two-Cloud Secure Database for Numeric-Related SQL Range Queries With Privacy Preserving ", In this paper, Authors tend to examine the issue for uprightness checking of data records redistributed to remote server In this paper, we presented a two-cloud architecture with a series of interaction protocols for outsourced database service, which ensures the privacy preservation of data contents, statistical properties and query pattern. At the same time, with the support of range queries, it not only protects the confidentiality of static data, but also addresses potential privacy leakage in statistical properties or after large number of query processes. Security analysis shows that our scheme can meet the privacy-preservation requirements. Furthermore, performance evaluation result shows that our proposed scheme is efficient. Utilizing our new association, the data proprietor will perform embed, alter or erase task on record hinders with high productivity. The given plan is demonstrated secure in existing security display. Creators tend to gauge the execution in term of network value, calculation cost and capacity cost. The examinations results demonstrate that our plan is commonsense in distributed storage.

FahadPolash, et al., [2] The Cloud Computing (CC) as a field is advancing significantly. So as to sort out the information on this recently thriving field, various scientific categorizations have been proposed throughout the most recent couple of years. A well- created cloud scientific classification plans to help specialists and experts from the scholarly community and industry by sorting out cloud computing-ideas and wording. It gives scientists a device to concentrate on the angles that dispense with research holes. This paper introduces a review of the current cloud computing scientific categorizations for different purposes. We plan to empower the perusers to more readily comprehend the cutting edge of cloud computing and order the current cloud computing related scientific classifications into three classes: theoretical, execution and security scientific classifications. This characterization will assist perusers with finding out alternate points of view in cloud computing scientific categorizations. We derive that present undertakings in CC scientific classification have not yet broadly investigated all parts of the developing field.

Josef Spillner [4] " Stealth Databases: Ensuring User-Controlled Queries in Untrusted Cloud Environments " In this author proposed Stealth databases represent a novel distributed data management design targeted at maintaining data security in untrusted environments with low capacity but rather high performance overheads. Our prototype StealthDB, while currently only implementing a subset of SQL, allows for a thorough evaluation of stealth database concepts. The results of our experiments show that for smaller workloads such as sensitive private data, the system performs reasonably well. In the future, we intend to tackle the performance issues with optimised calculation modules.

III. IMPORTANCE OF SECURITY IN CLOUD COMPUTING

The strength, usability and ability to adopt of cloud computing accompany packet of security challenges. Although CC is another instinctive technique for getting to applications and making job easy, there are different problems / challenges that can affect its reception. In this field, a non-thorough quest uncovers a few problems. They are: Service Level Agreements, relocation, safety, etc. Cloud computing does have a programmed refresh component that means a chairman's solitary shift to an implementation that would think of its customers as a

whole [7]. This also prompts the end that any problems in the product are evident to innumerable immediately or, in other words, opportunity for any association with less safety. Numerous experts also agree that safety is a major concern for the appropriation of distributed computing. Likewise, an IDC analysis of 263 authorities shows that safety is placed first among CC problems. Despite the reality that an organization is glad to have top- class safety and is not refreshing its safety policies over and over again, in not so remote future this will be prone to safety breakdowns. Through this nitty gritty inquiry, we suggest that perusers with different skills (types of) be refreshed in safety problems and their responses [8]. We also integrate ongoing procedures to mitigate difficulties, integrate improved agreements suggested by experts to show which distributed computing regions need to be given more concern.

IV. SECURITY AND PRIVACY CONCERNS IN CLOUD

Security/protection is one of the real worries as far as the use of distributed computing. As information is not any more under the clients' immediate control, clients are hesitant to move their important information onto the cloud - particularly general society cloud with its high union and multi-tenure. Additionally, from a proficiency point of view, questioning and recovering from cloud servers require significantly more exertion than it does in nearby servers. Among the numerous mechanical perspectives, the three fundamental measurements of information security inquire about are classification, respectability and accessibility [9]. Security risk is a composition of frequency of security threat event and magnitude of its result or effect, using their product. There are various security risks associated with Cloud Computing such as

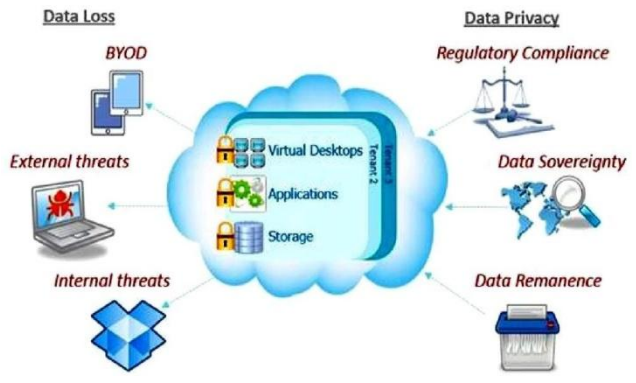

Fig. 1.7 Types of security threats.

V. HASH FUNCTION

A few calculations fulfill the homomorphism for increase, for example, RSA. A few calculations fulfill the homomorphism for expansion, for example, Paillier. On the off chance that a few calculations fulfill homomorphism for expansion and duplication, at that point they known as complete homomorphism calculations. There are no honest to goodness full homomorphic encryption calculations accessible. Homomorphic hash work implies that the hash work has the normal for homomorphism. The homomorphic hash work utilised during this work [10]. A homomorphic hash perform (Krohn, Freeman, &Mazieres, 2004) consists of two sub-algorithms, namely, homomorphic key generation and hash generation. In the primary part, it takes as input four security parameters wherever and ar separate log security parameters, m is that the variety of sectors in per hash message, S may be a random seed which might be generated by hashing file name, and outputs the homomorphic key wherever and ar random primes satisfying , and is 1 × m row vector of order q in Zp. In hash generation, a message F is split into n blocks, say,, and every block is any metameric into m sectors . The homomorphic hash price of F is, and every is computed as:

The reason for proven data ownership is to enable the customer to check that information is properly contained on the unsafe stockpiling server. There are two gatherings for the most portion: client and capacity server. The plan of provable information ownership base upon homomorphic hash work is made out of five stages:

(1) Setup;

(2) TagBlock;

(3) Challenge;

(4) ProofGen;

(5) ProofVerify.

First, we have to split the F file into n blocks. In the following phases such as TagBlock phase and Proof Verify phase, all the calculations are based on the file blocks,

$Setup(\lambda_p, \lambda_q, m, s) \rightarrow G = (p, q, g)$
Seed PRNG R with s.
do
  q ← qGen(λ_q)
  p ← pGen(q, λ_p)
while p=0 **done**
for(i=1 **to** m) **do**
  do
    x ← R(p − 1) + 1
    $g_i \leftarrow x^{(p-1)/q} \pmod p$
  while $g_i = 1$ **done**
done
return (p,q,g)

$qGen(q, \lambda_q)$
do
  q ← R(2^{λ_q})
while q is not prime **done**
return q

$pGen(q, \lambda_p)$
for(i=1 to $4\lambda_p$) **do**
  X ← R(2^{λ_p})
  c ← X(mod 2q)
  p ← X − c + 1
  if p is prime **then return** p
done
return 0

Fig.1.4 Algorithm

Setup Phase: In this phase, the I/P value is (, , m, s), and output value is G = (p, q, g). G is hash parameters that are used to generate hash value in the homomorphic hash function. Setup phase is described in Algorithm.

VI. PROPOSED FLOW CHART

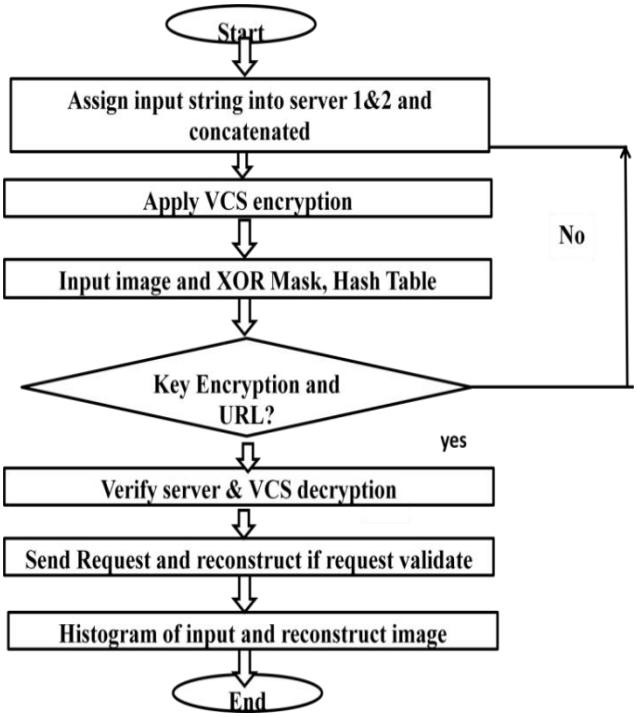

Figure 1.5 showing proposed flow chart in which each step is mention according to proposed work. The explanation of flow chart is discussed in following algorithm.

VII. VISUAL CRYPTOGRAPHY (VCS)

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. In this a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image [11]. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlayed, the original image would appear.

Figure 1.6: A demonstration of visual cryptography

Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the ciphertext.

In this example, the cipher key has been split into two shares. Each white pixel in the original key is split into two of the same small blocks that have half black and white pixels. When these two blocks are overlayed, they line up exactly, and the result is a light-colored block (with half black and half white pixels). Each black pixel in the original logo is split into two complementary small blocks. When these two blocks are overlayed, the result is a completely black box. If each pixel in the original image is split randomly as described above, then each individual share is a totally random collection of blocks. Only when the shares are combined is any information revealed about the original image [12].

VIII. RESULTS

Simulation Software

MATLAB (**mat**rix **lab**oratory) is a numerical computing environment and fourth-generationprogramming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java,and Fortran.

Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPADsymbolic engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems [13].

In 2004, MATLAB had around one million users across industry and academia. MATLAB users come from various backgrounds of engineering, science, and economics. MATLAB is widely used in academic and research institutions as well as industrial enterprises

The term “MATLAB” is familiar to every Engineering graduate. MATLAB is a scientific computational package that has been widely in use ever since its inception in the early nineties. In the beginning it was limited to the research arena but later it gained a prominent place in the Engineering course syllabus, especially the Electrical and Electronics branches [14].

MATLAB is a mathematical and graphical software package; it has numerical, graphical, and programming capabilities. It has built-in functions to do many operations, and there are toolboxes that can be added to augment these functions (e.g., for signal processing). There are versions available for different hardware platforms, and there are both professional and student editions. When the MATLAB software is started, a window is opened: the main part is the

Command Window. In the Command Window, there is a statement that says:

In the Command Window, you should see:

>>

The >> is called the prompt. In the Student Edition, the prompt appears as: EDU>>

In the Command Window, MATLAB can be used interactively. At the prompt, any MATLAB command or expression can be entered, and MATLAB will immediately respond with the result. It is also possible to write ***programs*** in MATLAB, which are contained in ***script files*** or M-files.

There are several commands that can serve as an introduction to MATLAB and allow you to get help:

- **info** will display contact information for theproduct
- **demo** has demos of several options inMATLAB
- **help** will explain any command; **help, help** will explain how helpworks
- **help browser** opens a HelpWindow

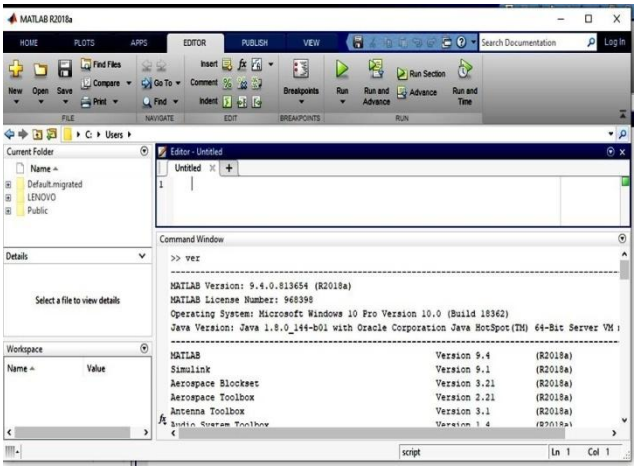

Figure 1.7: Snap shot of MATLAB

Figure 1.8 is the process which is proved communication between server and user and show the accuracy of data.

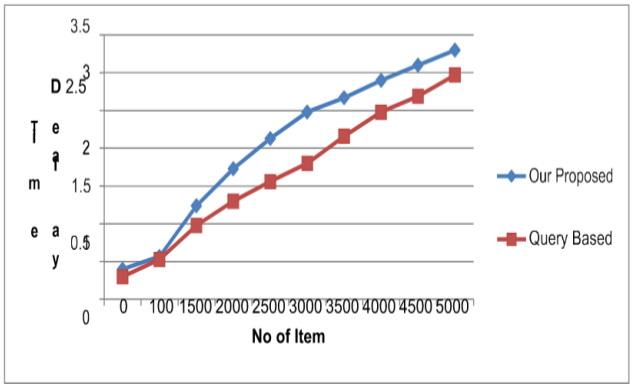

Fig. 1.8 Efficiency for Item Select in Single Process

Fig 1.9 Input and reconstructed image

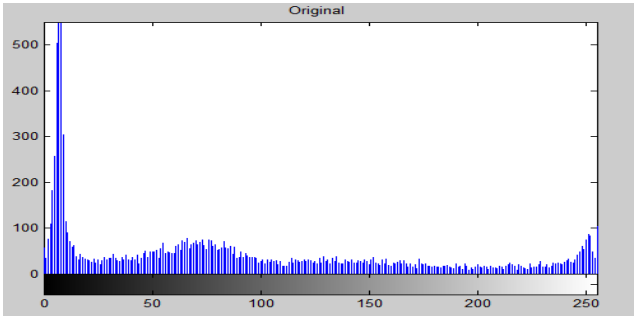

Fig 1.10 Histogram of original data/image

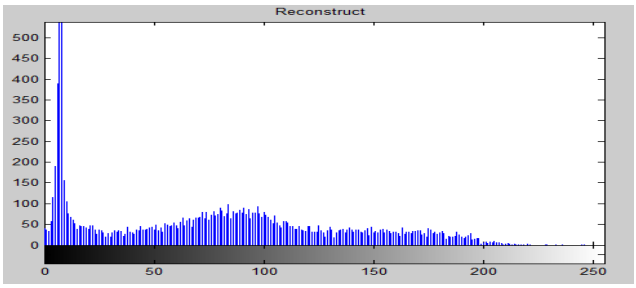

Fig 1.11 Histogram of original and reconstruct data/image

Table 5.1 Comparison of proposed work with previous comparison

Sr.No.	Parameter	Previous Work	Proposed Work
1	Proposed Method	Paillier Cryptographic Algorithm	VCS Cryptographic Algorithm & Hash Function
2	No of Cloud server	2	2
3	Complexity	More	Less
4	latency	50ms	20ms
5	Cost	High	Low
6	Efficiency	Decrease	Increase

IX. CONCLUSION

Security issues in the area of cloud computing are active area of research and experimentation. Various issues are identified one of which is the security of user data and

applications. In this dissertation proposed security algorithm based on VCS encryption, hash function and proxy re- encryption for data storage in cloud server. In proposed System we work multiple server encryption data and identity, design key encryption utility to verify and secure transition of communication. This system is basically design secured key address through encryption process and enhanced cloud security [19].

REFERENCES

[1] KaipingXue, Shaohua Li, Jianan Hong, YingjieXue, Nenghai Yu, and PeilinHong "Two-Cloud Secure Database for Numeric-Related SQL Range Queries With Privacy Preserving" IEEE Transactions On Information Forensics And Security, Vol. 12, No. 7, July2017.

[2] FahadPolash, Abdullah Abuhussein and Sajjan Shiva, "A Survey of Cloud Computing Taxonomies:Rationale and Overview",The 9th International Conference for Internet Technology and Secured Transactions(ICITST-2014)

[3] Marek Moravcik, Pavel Segec and Martin Kontsek, "Overview of Cloud Computing standards ICETA 2018 16th IEEE International Conference on Emerging eLearningTechnologies and Applications November 15-16, 2018, StaryRo

[4] bert B. Bohn, John Messina,Fang Liu, Jin Tong and Jian Mao, "NIST Cloud Computing Reference Architecture",2011 IEEE World Congress on Services Smokovec, The High Tatras,Slovakia

[5] Deepika Tenepalli and NARAYANA RAO Appini, "Active Resource Provision In Cloud Computing Through Virtualization", 2014 IEEE Conference "Cloud Service and Deployment Models", Cloud Strategy Partners, LLC Sponsored by: IEEE Educational Activities and IEEE Cloud Computing

[6] Fu, Zhangjie, et al. "Enabling personalized search over encrypted outsourced data with efficiency improvement" IEEE trans. on parallel and distributed systems 27.9 (2016): 2546-2559.

[7] Xia, Zhihua, et al. "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data" IEEE trans. on parallel and distributed systems 27.2 (2016): 340-352.

[8] Li, Jiguo, et al. "Flexible and fine-grained attribute-based data storage in cloud computing" IEEE Trans. on Services Computing 10.5 (2017): 785-796.

[9] Yan, Hao, et al. "A novel efficient remote data possession check protocol IEEE Trans. on Info. Forensics and Security 12.1 (2017): 78-88.

[10] Qian, Huiling, et al. "Privacy-preserving personal health record using multi- authority attribute-based encryption with revocation" Intern. Jou.of Information Security 14.6 (2015): 487-497.

[11] Li, Jiguo, et al. "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage" IEEE Trans. on Services Computing 10.5 (2017): 715-725.

[12] Yu, Yong, et al. "Improved security of a dynamic remote data possession checking protocol for cloud storage" Expert systems withapplications 41.17 (2014): 7789- 7796.

[13] Haifeng, Ma, GaoZhenguo, and Yao Nianmin. "Hierarchical Enhanced Remote Data Possession Checking in Cloud Storage" BoletínTécnico 55.3 (2017): 145-154.

[14] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun.Netw. (SecureComm), 2008, Art.no. 9.

[15] F. Sebé, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034–1038, Aug. 2008.

[16] Nalini, Dr T., Dr K. Manivannan, and VaishnaviMoorthy. "Efficient Remote Data Possession Checking in Critical Information Infrastructures Ensuring Data Storage Security in Cloud Computing" International Journal of Innovative Research in Computer and Communication Engineering 1.1 (2013).

[17] Y. Deswarte, J.-J.Quisquater, and A. Saïdane, "Remote integrity checking, in Proc. 6th Work. Conf. Integr. Int. Control Inf. Syst. (IICIS), 2003, pp. 1–11.

[18] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Trans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432–1437, Sep. 2011.

[19] G. Ateniese et al., "Provable data possession at untrusted stores" in Proc. 14th ACM Conf. Comput. Commun.Secur.(CCS), 2007, pp. 598–609.

[20] Y.-J. Ren, J. Shen, J. Wang, J. Han, and S.-Y.Lee, "Mutual verifiable provable data auditing in public cloud storage" J. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.