INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING AND TECHNOLOGY (IRJET) E-ISSN: 2395-0056
VOLUME: 06 ISSUE: 05 | MAY 2019 WWW.IRJET.NET P-ISSN: 2395-0072

# Secure Database Management and Privacy Preserving in Cloud Server

**Laxmi Kurmi[1] and Dr. R.K. Pateriya[2]**

*[1]M.Tech Scholar MANIT Bhopal, India*
*[2]Associate Professor, MANIT Bhopal, India*

---

**Abstract**— As a vital application in distributed computing, distributed storage offers client versatile, adaptable and superb information stockpiling and calculation administrations. A developing number of information proprietors outsource information documents to the cloud. Because of the lack of complete reliability of distributed storage servers, proprietors of information require a tried and true intention to check the possession of their records externalized to remote cloud servers. There are still worries that frustrate the expansion of cloud, and information security/protection is the best worry for information proprietors wishing to move their applications into the cloud environment. Here provide a solution to with cryptosom generation to secure communication with multiple servers (Cloud ).

**Index Terms** — Cloud Storage, Secure Database, DPC(Data Possession Checking), Homomorphic, CyptoSom, Secure Communication.

———————————— ◆ ————————————

## 1.INTRODUCTION

Recent innovative advances ease the dangerous development of computerized sub-stance. The US International Data Corporation (IDC) announces that the computerized universe will develop by a factor of 300, up to 40 trillion gigabytes of imitated information by 2020. This multiplication of computerized universe keeps on raising the interest for new capacity and system utilities, alongside an expanding requirement for more financially savvy utilization of capacity limits and system transmission capacity for information exchange. Accordingly, the utilization of remote stockpiling frameworks is picking up an extending interest, to be specific the Cloud stockpiling based administrations, since they give gainful designs[1]. These designs bolster the transmission, storage, and escalated calculation of outsourced information in compensation for every utilization plan of action. This broad enthusiasm for distributed storage benefits primarily exudes from business associations and government organizations looking for stronger and practical frameworks. That is, the advantages of cloud adoption are extremely unmistakable in another time of responsiveness, and effectiveness in Information Technology service delivery. Cloud Computing (CC) is another means of communication that makes distributed computing and grid computing technologically evolve. Over a certain undefined time frame, CC has evolved and many companies find it interesting to use it. The improvement of ARPANET (Advanced Research Projects Agency Network) by J.C.R. Licklider in the 1960s and number of different experts who sought to improve frameworks connectivity, CC may never have appeared. The arrival of ARPANET, which associated a group of computer systems (for exchanging, sharing and so on), provoking the emergence of the Internet (where it turned out to be simple to cross any barrier between frameworks)[2 ]. This Internet has accelerated various exercises, such as human association (texting, web-based social networking, etc.), an organization's business needs (web-based shopping, money-related administrations, etc.).

In addition, the advancement of Applications Service Provision (ASP), framework and utility registration and distributed computing led to further progress around the Internet. CC presented another worldview that transformed the conventional frame-works interconnection into a pool of joint assets that can be accessed via the web.

### I.1 Privacy and Security Concerns in Cloud

Privacy and Security is one of the major Cloud Computing(CC) usage concerns. As information is not anymore under the clients' immediate control, clients are hesitant to move their important information onto the cloud - particularly general society cloud with its high combination and multi-occupancy. Likewise, from an effectiveness viewpoint, questioning and recovering from cloud servers require significantly more exertion than it does in neighborhood servers[3].

Amongst the many technological aspects, the three main dimensions of data security research are confidentiality, integrity, and availability. The power, optimization, and cloud computing flexibility generate security challenge. It is also a concern for the new user also their accessibility.

In this field, A non-thorough hunt demonstrates few problems. They are Service Level Agreements (SLA), movements, security, etc. Cloud Computing has a programmed refresh element that implies a single change to an application by a head that would consider each of its customers. This also leads to the end that any problems in the product can be noticed very soon, which is a notable hazard for any association with little safety[5]. Numerous scientists also agree that security is a huge concern for the appropriation of distributed computing. Additionally, an IDC overview of 263 officials shows that security is placed first among cloud computing challenges. Although an organization is gloating to have top class security and does not refresh its approaches to security every now and then, in not so distant future it will be inclined to breaks in security. Through this nitty-gritty examination, we propose to refresh and respond to security challenges for perusers with different qualifications (sorts of). We also include real-time challenge mitigation practices, including the solutions proposed by enhanced researchers to demonstrate which areas of cloud computing need more attention.

## 2. CLOUD COMPUTING: SERVICE MODELS

Cloud Computing can be easily accessible via a set of server or service modal. This services is design to provide easy accessibility and security of user. It is provide big data storage and controlling. Cloud computing is combination of multiple server, that is provide global reach of data without limitation.

CC has different type of service modal, namely-
1.Infrastructure-as-a-Service (IaaS).
2.Platform-as-a-Service (PaaS).
3. Software-as-a-Service (SaaS).

All three services work in layered. The model is shown in figure below. All layer is depending each other first work start of visualization then work on infrastructure. infrastructure is basically work on application requirement. After infrastructure we need to design its application module then its go to end used module to complete task.

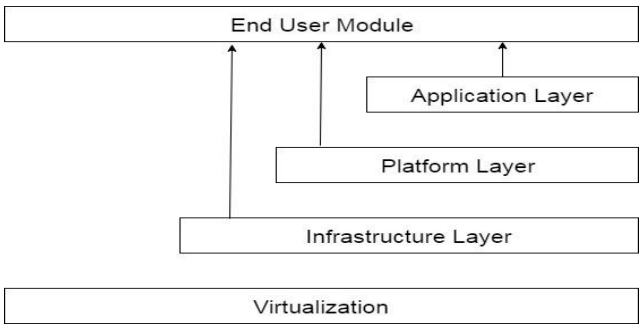



Fig. 1 Structure of service model

## 3. PROPOSED METHODOLOGY

In this proposed work, present Efficient Data send and Management in cloud and outsourcing calculation into IBE (Identity Based Encryption) renouncement, and formalize the security importance of outsourced revocable IBE (Identity Based Encryption) suddenly to the best of our understanding Here is a proposed plan to create key , for enhanced security in cloud to hide identity and assign key through the encryption process. The second part to develop the proposed methodology to increase data and secure communication in the minimum time period.

The proposed system, likewise with the recommendation, we understand disavowal through refreshing the private keys of the unrevoked clients. Yet, However, not under any condition like that work which inconsequentially links day and age with personality for key age/refresh and requires that the entire private key be reissued for unwanted customers, We propose a new configuration safe key issuing method: for each customer, we use creamer private key, which includes an AND door interface and links two sub-sections, in particular, the character segment and time segment.

At first, the client can acquire from the essential server a default time segment and the character part (i.e., for the present era) as its private key in key issue. A little time later, with a specific end goal to keep up decode capacity, the need for unrevoked clients to intermittently request key refresh for the time part of an optional service that has recently been presented.

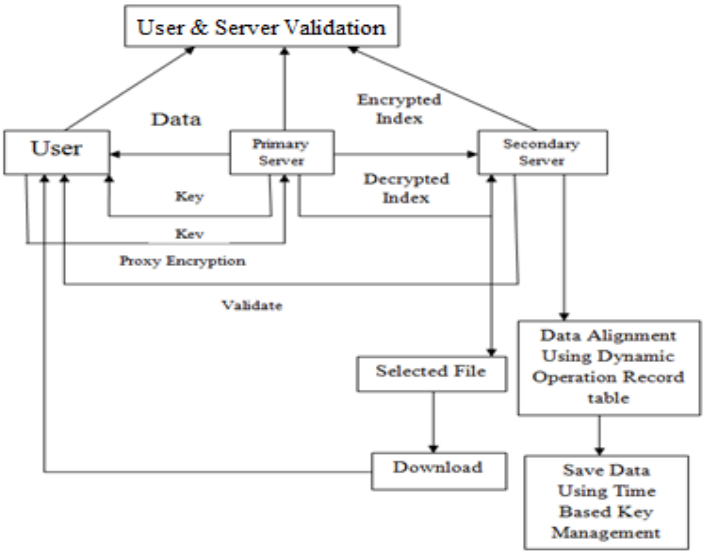



Fig.2 Stream chart of proposed framework

## 4 PROXY RE-ENCRYPTION

Proxy re-encryption plans are cryptosystems which permit outsiders (intermediaries) to modify a ciphertext which hosts been scrambled for one get-together, with the goal that it might be unscrambled by another. Anyway, the outsiders can't get the mystery esteem [10]. Blast introduces the BBS, Elgamal-based plan working more than two gathering _ of prime request q with a bilinear map. The system parameters are random generators $g \in G_1$ and $Z = e(g, g) \in G_2$.

- **Key Generation (KG).** The user A select random x. A's key pair is the form.
- **Re-Encryption Key Generation (RG).** A user A delegates to B by publishing the re-encryption key, computed from B's public key.
- **First-Level Encryption ( $E_1$ ).** To encrypt a message under in such a way that it can only be the holder of, output.
- **Second-level Encryption ( $E_2$ ).**To encrypt a message $m \in G_2$ under $pk_a$ in such a way that it can be decrypted by user A and his delegates, output $c = (g^{ak}, mZ^k)$.
- **Re-Encryption(R).** Anybody can change a second-level ciphertext for A into a first level ciphertext for B with $rk_{A \to B}$. From $c_a = (g^{ak}, mZ^k)$, compute $e(g^{ak}, g^{b/a}) = Z^{bk}$ and publish $c_b = (Z^{bk}, mZ^k)$.

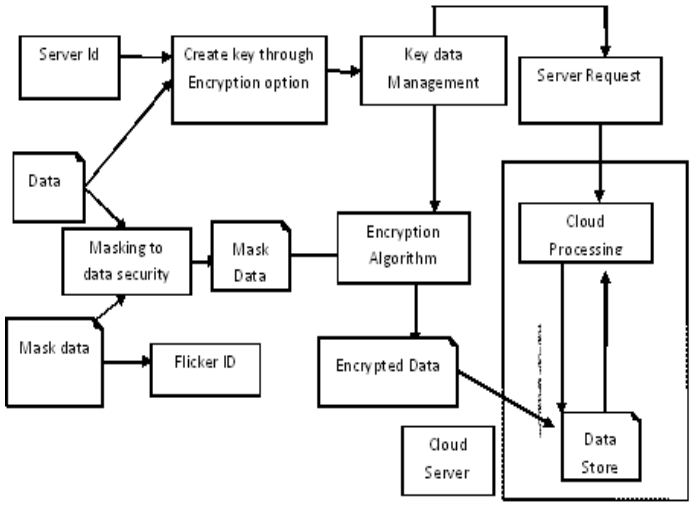



Fig3: Structure of Encryption Process

- **Decryption ( $D_1$ , $D_2$ ).** To decrypt a first-level ciphertext $c_a = (\alpha, \beta)$ with secret key $sk = a$, compute $m = \beta / \alpha^{1/a}$. To decrypt a second-level ciphertext $c_a = (\alpha, \beta)$ with secret key $sk = a$, compute $m = \beta / e(\alpha, g)^{1/a}$.
- **Step 1 :**Calculate Data dimension
- **Step 2 :**Create server id using fomula *flk_ID = $h_2(x,y,h_1(I))$* (1) *$h_1(I) = mod(M \times N, E)$* (2) *where I = original Data M, N = dimension datax & y = coefficient of correlation of adjacent of data and E = entropy of data*
- **Step 3 :**XOR data from Original and mask
- **Step 4 :** Then Data is divided into 8 sub data by using the Logistic Map and random permutation$x_{n+1} = rx_n(1-x_n)$, (3)
- **Step 5:** for *b = 1 to 8 do*
- Data block shuffling
  *Dimension of a block : $B_m \times B_n$*

## 5 RESULT & DISSCUSSION

To work acknowledge renouncement through refreshing the private keys of the unrevoked clients. Be that as it may, different from the work that inconsistently connects day and age with key age/refresh personality and requires the reissue of the entire private key for unrevoked customers. The proposed research work results are shown below figure.Our system basically works on two cloud structure first that is user interact and second work on data security. For this basically design one system that follow some steps:

1. Server identity
2. Server Key Encryption
3. Server User Validation
4. User and Input Data
5. Ker Encryption and URL Design
6. Data Store in Cloud
7. Verification of Key
8. Decryption of Key
9. Verify Identity

10. Download Data
11. Analyze accuracy

In figure 3 take basic information of Server to validate the identity of the server and verify for secure communication.

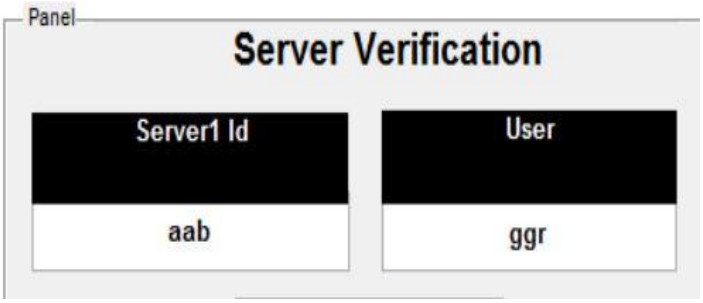
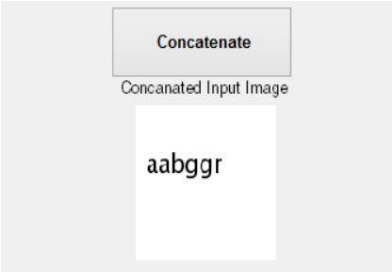



Fig.3 Server Identity



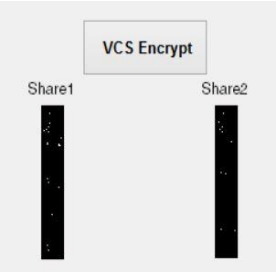




Fig.4 Merge Server Identity Fig.5 Key design based on server

Figure 4- and 5 show process to merge identity of server and design key using personal information. This is generate more security in cloud architecture

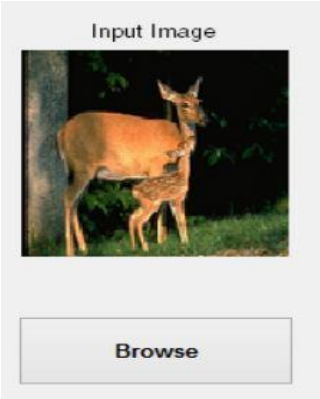




Fig.6 User Data Fig.7 User data Masked

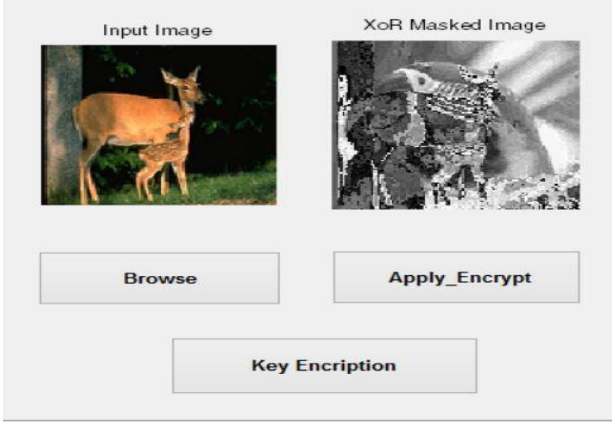



Fig.8 Key Design and URL

In figure 6 and 7 is show user utility, here user is interacting with server and store data in the cloud. Before is store data in the cloud we process and secure it by using the hash algorithm I masked input data to secure basic information of data.

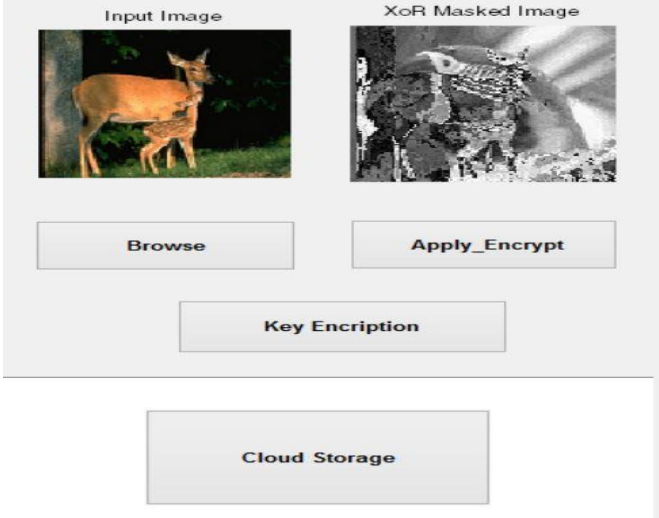
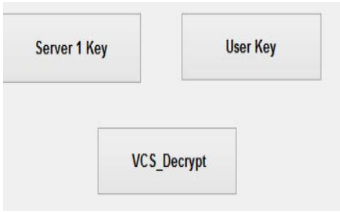



Fig.9 Store Data in Cloud

Figure 9 and 10 is shown masking of input data to secure data information and then design key URL(Index) of data to store content in cloud URL.



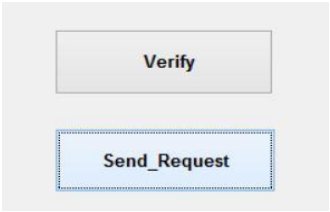




Fig.10 Verify Server Ownership Fig.11 Send Request

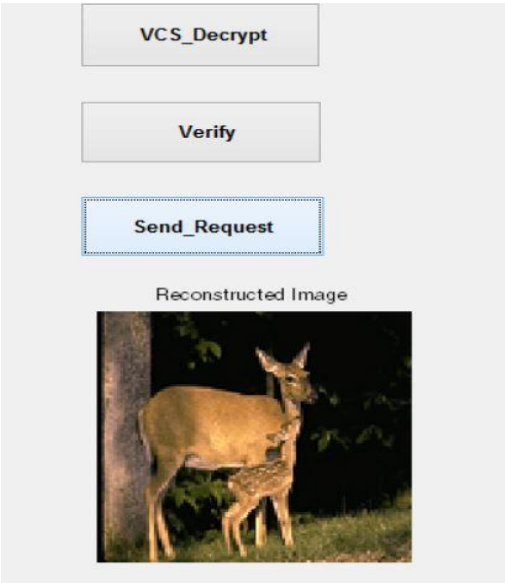



Fig.12 Data Retrieval and Accuracy Measure

Figure 10 to 12 is the process which is proved communication between server and user and show the accuracy of data.

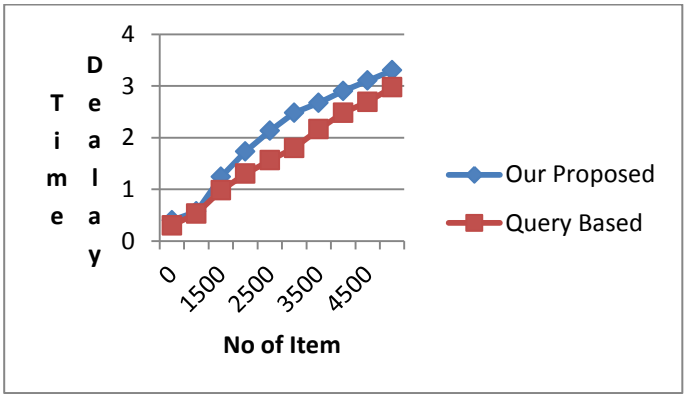



Fig.13 Efficiency for Item Select in Single Process

## 5 CONCLUSION

This study proposed to propose a privacy-preserving protocol for data security in cloud architecture. In this research proposed a methodology to address the efficiency problems big data in the cloud server. The system we work multiple server encryption data and identity, design key encryption utility to verify and secure transition of communication. This system is basically designed secured key address through the encryption process and enhanced cloud security.

## REFERENCES

1. AKaipingXue, Shaohua Li, Jianan Hong, YingjieXue, Nenghai Yu, and Peilin Hong "Two-Cloud Secure Database for Numeric-Related SQL Range Queries With Privacy Preserving" IEEE Transactions On Information Forensics And Security, Vol. 12, No. 7, July 2017.
2. 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.

3. A 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.
4. A 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.
5. Yan, Hao, et al. "A novel efficient remote data possession check protocol IEEE Trans. on Info. Forensics and Security 12.1 (2017): 78-88.
6. 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.
7. 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.
8. 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.
9. Haifeng, Ma, GaoZhenguo, and Yao Nianmin. "Hierarchical Enhanced Remote Data Possession Checking in Cloud Storage" BoletínTécnico 55.3 (2017): 145-154.
10. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur.PrivacyCommun.Netw.(SecureComm), 2008, Art.no. 9.
11. 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.
12. 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).
13. 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.
14. 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.
15. G. Ateniese et al., "Provable data possession at untrusted stores" in Proc. 14th ACM Conf. Comput. Commun.Secur.(CCS), 2007, pp. 598–609.
16. 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.