Volume 7, Issue 3, March 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Proposing a Secure Cloud Database Storage [SCDS] Model

Dr. Amit Chaturvedi
Govt. Engineering College, Ajmer, Rajasthan, India

Akanksha Kapoor
M.Tech. Scholar, Bhagwant University, Ajmer, Rajasthan, India

Harish Chandra Morya
Assistant Prof., Bhagwant University, Ajmer, Rajasthan, India

Abstract: ***The benefits of using cloud storage technology for unstructured data are compelling, starting with lower overall storage costs. Being service based, there's no storage hardware to buy, manage and maintain, and depending on the service, it can greatly reduce, if not eliminate, data center and storage administrator costs. Cloud storage eliminates expensive technology refreshes that usually kick in three years to five years after the initial purchase, needed to either get state-of-the-art technology or simply to get around purchasing expensive support contracts for older arrays. Here in this paper we have proposed a Secure Cloud Database Storage [SCDS] Model for improving the customer's satisfaction in third party cloud servers for database storage.***

Keywords: Cloud, database, SCDS, encryption, decryption, secured, server.

I. INTRODUCTION

Cloud computing is emerging as a key computing platform for sharing resources that include infrastructure, software, applications, and business processes. Cloud Service Provider (CSP) maintains database and applications for the users on a remote server and provide independence of accessing them from any place through a network. There are three major cloud service categories: software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS).

Cloud computing security includes a number of issues like multi tenancy, data loss and leakage, easy accessibility of cloud, identity management, unsafe API's, service level agreement inconsistencies, patch management, internal threats etc. It is not easy to enforce all the security measures that meet the security needs of all the users, because different users may have different security demands based upon their objective of using the cloud services.

Here, in this paper, a Secure Cloud Database Storage [SCDS] Model is proposed. In this model an encryption method is applied to the client's database before it is shifted to the third party cloud storage. The primary use of cloud storage today is for unstructured data, which is the fastest growing and most voluminous content, causing the most administrative pains. Cloud storage is less suitable for structured data, which continues to live on traditional enterprise data storage.

The benefits of using cloud storage technology for unstructured data are compelling, starting with lower overall storage costs. Being service based, there's no storage hardware to buy, manage and maintain, and depending on the service, it can greatly reduce, if not eliminate, data center and storage administrator costs. Cloud storage eliminates expensive technology refreshes that usually kick in three years to five years after the initial purchase, needed to either get state-of-the-art technology or simply to get around purchasing expensive support contracts for older arrays.

The technology can provide close to 100% storage utilization by eliminating the massive amounts of unused storage that are needed with traditional data storage for anticipated growth and peak loads. Besides the overall cost savings, scalability of cloud storage and its ability to transparently support base and peak loads are its most appealing characteristics.

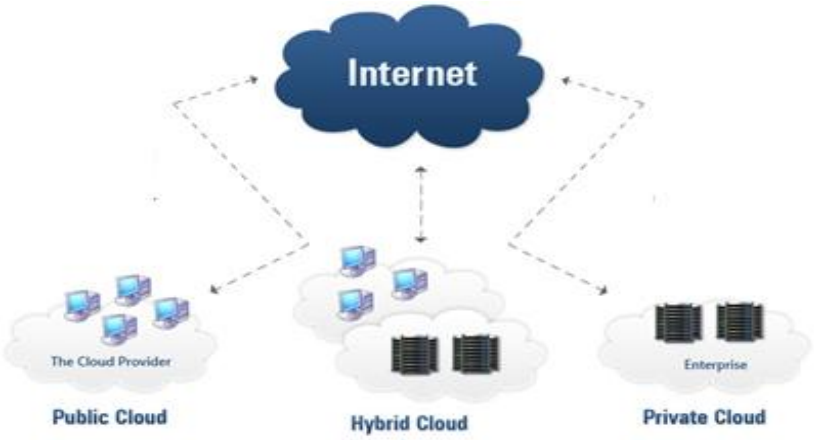

Figure : Basic architecture of Cloud Computing

Everything in the nature is not complete, hence there are also some disadvantages of cloud computing like it requires constant Internet connection and does not work well with low- speed connections, features might be limited, slow, stored data can be lost, stored data might not be secure at it is stored with third party.

II. STUDY ON THE RELATED WORK

A number of cloud storage gateway products have recently appeared to ease the transition between conventional and cloud storage interfaces. Each product focuses on a unique touch point between applications and their storage. Cloud gateways can make cloud storage appear to be a NAS filer, a block storage array, a backup target or even an extension of the application itself.

- Asigra Inc. produces an integrated backup solution for public and private cloud storage services with integration both on-site and at the service provider location.
- Cirtas Systems produces the Bluejet cloud storage controller, which allows public cloud storage services to be accessed as if they were on-site block storage arrays.
- Nasuni Corp. produces a virtual appliance that acts as a file server, complete with snapshots, caching and encryption.
- StorSimple Inc. produces a storage appliance with caching and provisioning, deduplication, encryption and WAN optimization targeted at SharePoint implementations.
- The TwinStrata Inc. CloudArray is a data protection and disaster recovery appliance integrated with public cloud storage.
- Other companies, like CommVault Technologies Inc. and Symantec Corp., have integrated cloud storage as a backup target on par with tape and disk.

The common theme for all these products, beyond bridging local applications to remote cloud storage, is the value-added features they introduce. Most include encryption technology to safeguard data stored off-site, as well as compression, deduplication and WAN optimization technology to accelerate performance. Many also take advantage of the scalability of cloud storage for features like snapshots, version control and data protection. And in nearly every case, local storage is used as a cache for improved performance.

A. Sachdev, M. Bhansali presented "Enhancing Cloud Computing Security using AES Algorithm". With the tremendous growth of sensitive information on cloud, cloud security is getting more important than even before. The cloud data and services reside in massively scalable data centers and can be accessed everywhere. The growth of the cloud users has unfortunately been accompanied with a growth in malicious activity in the cloud. More and more vulnerabilities are discovered, and nearly every day, new security advisories are published. Millions of users are surfing the Cloud for various purposes, therefore they need highly safe and persistent services. The future of cloud, especially in expanding the range of applications, involves a much deeper degree of privacy, and authentication. We propose a simple data protection model where data is encrypted using Advanced Encryption Standard (AES) before it is launched in the cloud, thus ensuring data confidentiality and security.

K. Handa, U. Singh discussed "Data Security in Cloud Computing using Encryption and Steganography". Cloud Computing is a technology that readily makes available resources that otherwise may require huge amount of investment. Besides, it increases the availability of resources since anyone can access the data using web. But this advantage comes at a cost. Firstly, the data is uploaded unsecurely which has a high risk of being hacked by some malicious people. Secondly, the data saved at remote servers is under the surveillance of unknown people who can do anything with our data. So, these data security risks are causing a hindrance in the development of the field of cloud computing. Thus, this paper has designed a scheme that can help, solve this issue.

B.K. Mohanta, D. Gountia stated that As the data storage challenge continues to grow for insurers and everyone else, one of the obvious solutions is cloud technology. Storing data on remote servers rather than in-house is definitely a money-saver, but in insurance circles, the worry has been that having critical data reside outside the physical and virtual walls of the insurance enterprise is a risky situation. As the IT field is rapidly moving towards Cloud Computing, software industry's focus is shifting from developing applications for PCs to Data Centers and Clouds that enable millions of users to make use of software simultaneously.

S. Bajpai and P. Srivastava presented that Cloud Computing has been the most promising innovation in the computing world in past decade. Its usage is still hindered by the security concerns related with critical data. The encryption of remotely stored data has been the most widely used technique to bridge this security gap. The speculated vast usage of Cloud Computing solutions for data storage and with Big Data Analytics gaining strong foothold; the security on cloud is still at big risk. Fully Homomorphic Encryption is a good basis to enhance the security measures of un-trusted systems or applications that stores and manipulates sensitive data. The model is proposed on cloud computing which accepts encrypted inputs and then perform blind processing to satisfy the user query without being aware of its content, whereby the retrieved encrypted data can only be decrypted by the user who initiates the request. This allows clients to rely on the services offered by remote applications without risking their privacy.

D. Dave,R. Thakkar proposed that Cloud computing is the most important parameter of distributed computing. Cloud computing ore use and its easily available services at low cost. Cloud computing provide data security. Now a day's data security and confidentiality is the major issues. In this paper focus on solve the security and confidentiality

problem. Homomorphic encryption is the best solution of this problem. In this paper new technique homomorphic apply and solve the security and confidentiality problem.

K. Benzekki, A. E. Fergougui, and A. E. B. E. Alaoui presented that The Purpose of homomorphic encryption is to ensure privacy of data in communication, storage or in use by processes with mechanisms similar to conventional cryptography, but with added capabilities of computing over encrypted data, searching an encrypted data, etc. Homomorphism is a property by which a problem in one algebraic system can be converted to a problem in another algebraic system, be solved and the solution later can also be translated back effectively. Thus, homomorphism makes secure delegation of computation to a third party possible. Many conventional encryption schemes possess either multiplicative or additive homomorphic property and are currently in use for respective applications. Yet, a Fully Homomorphic Encryption (FHE) scheme which could perform any arbitrary computation over encrypted data appeared in 2009 as Gentry's work. In this paper, we propose a multi-cloud architecture of N distributed servers to repartition the data and to nearly allow achieving an FHE.

M. TEBAA, S.E. HAJJI, A. E. GHAZI discussed that Cloud computing security challenges and it's also an issue to many researchers; first priority was to focus on security which is the biggest concern of organizations that are considering a move to the cloud. The advantages of cloud computing include reduced costs, easy maintenance and re-provisioning of resources, and thereby increased profits. But the adoption and the passage to the Cloud Computing applies only if the security is ensured. How to guaranty a better data security and also how can we keep the client private information confidential? There are two major questions that present a challenge to Cloud Computing providers.

When the data transferred to the Cloud we use standard encryption methods to secure the operations and the storage of the data. But to process data located on a remote server, the Cloud providers need to access the raw data. In this paper we are proposing an application of a method to execute operations on encrypted data without decrypting them which will provide us with the same results after calculations as if we have worked directly on the raw data.

HUANG Qin-long, MA Zhao-feng, YANG Yi-xian, FU Jing-yi, and NIU Xin-xin proposed "Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing". Cloud computing provides a convenient way of content trading and sharing. In this paper, they propose a secure and privacy-preserving digital rights management (DRM) scheme using homomorphic encryption in cloud computing. We present an efficient digital rights management framework in cloud computing, which allows content provider to outsource encrypted contents to centralized content server and allows user to consume contents with the license issued by license server. Further, we provide a secure content key distribution scheme based on additive homomorphic probabilistic public key encryption and proxy re-encryption. The provided scheme prevents malicious employees of license server from issuing the license to unauthorized user. In addition, we achieve privacy preserving by allowing users to stay anonymous towards the key server and service provider. The analysis and comparison results indicate that the proposed scheme has high efficiency and security.

Xiaofen Wang discussed One-round secure fair meeting location determination based on homomorphic encryption. This paper states that determination of optimal meeting location without revealing the locations of participants to the location server is an interesting research problem. A major concern for a location based service is location privacy. However, adding privacy protection to a location service will inevitably introduce computational complexity. To provide location privacy with low computational cost is a challenging task. In this paper, we propose a one-round meeting location determination protocol, where the location service provider makes a decision with a semi-trusted cloud server which works as a computation centres and conducts most of computation. The user location privacy is preserved against the outside and internal attackers including the computation center, the meeting location determination server and participants. In order to study the performance of the protocol, we test its computational efficiency on smartphones. The simulation results and the performance comparison of our protocol with another protocol of the same functionalities demonstrate that our solution is more efficient and practical.

S. Dasgupta, S.K. Pal proposed Design of a polynomial ring based symmetric homomorphic encryption scheme. Security of data, especially in clouds, has become immensely essential for present-day applications. Fully homomorphic encryption (FHE) is a great way to secure data which is used and manipulated by untrusted applications or systems. In this paper, we propose a symmetric FHE scheme based on polynomial over ring of integers. This scheme is somewhat homomorphic due to accumulation of noise after few operations, which is made fully homomorphic using a refresh procedure. After certain amount of homomorphic computations, large ciphertexts are refreshed for proper decryption. The hardness of the scheme is based on the difficulty of factorizing large integers. Also, it requires polynomial addition which is computationally cost effective. Experimental results are shown to support our claim.

III. SECURE CLOUD DATABASE STORAGE [SCDS] MODEL

Many researchers have worked and proposed many algorithms, models and methodologies for securing the database. Here we are also proposing a Secure Cloud Database Storage [SCDS] model. In Cloud computing, the database is stored on the cloud servers, which are basically the shared servers. Hence, if data will be stored on the shared servers after encryption and decryption is done when accessed on the user's or owner's site, then this will definitely secure the data and improves the customer's satisfaction in cloud computing.

The proposed Secured Cloud Database Storage [SCDS] Model is shown in figure 1. First user enters plain data through its system and saved at its site as plain database. Then this plain data will be encrypted through an encryption method and then this plain database will be changed to an encrypted database. Now this encrypted database will be then shifted to Cloud storage servers.

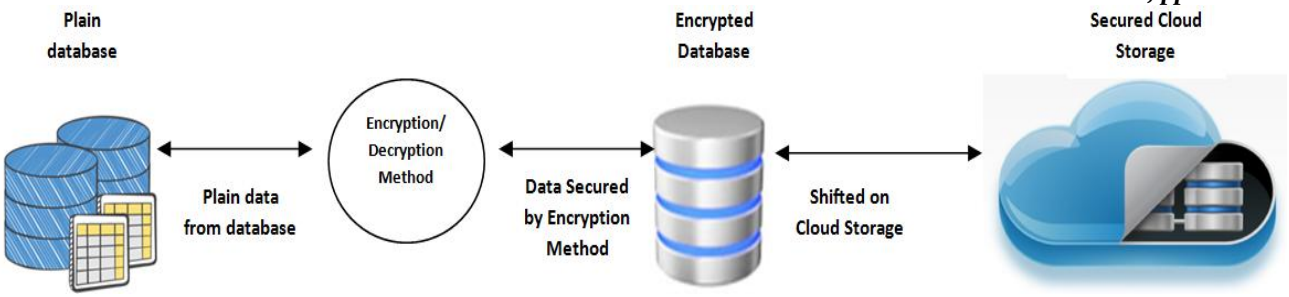

Fig 1 : Secured Cloud Database Storage [SCDS] Model

The data on third party if in original form is under risk. In Multi-tenent environment, multiple users store and access their data on that shared server. So, there are chances of unauthorized access of data. So, one way to secure the data is to store, the data after encrypting it with a strong key, on the shared server.

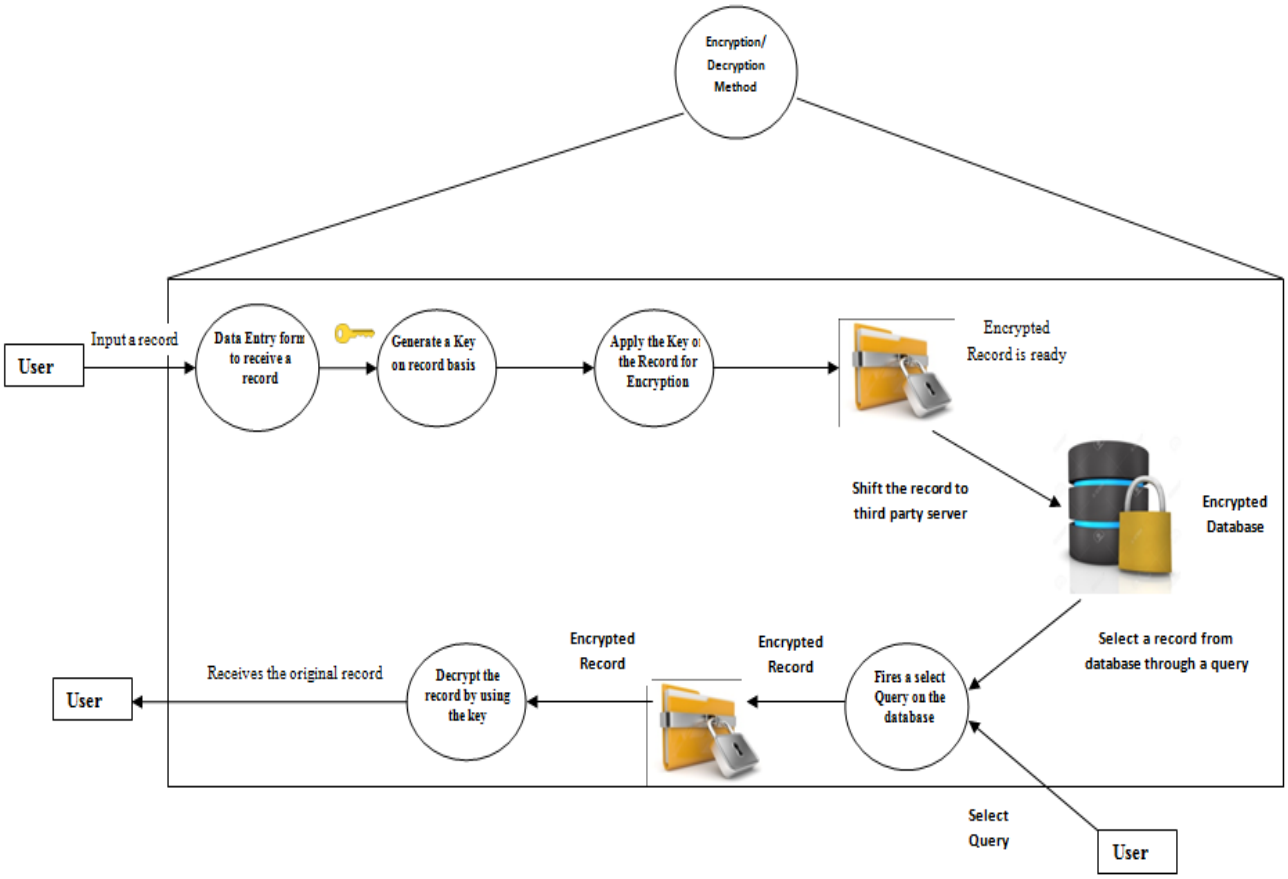

Fig 2: Encryption/ Decryption Method for SCDS Model

The proposed encryption / decryption method shown in fig.2 will improve the customer's satisfaction in cloud data storage and in future cloud computing also. Many of the organizations are moving towards hiring cloud servers for keeping their customer's data.

IV. CONCLUSION

Many researchers are presently working on providing secured cloud data environment. Secured Cloud Database Storage [SCDS] Model is also an effort in this direction. We have explained the concept of encryption and decryption through a model in figure 2. This will definitely increase the customer's satisfaction in cloud data storage.

Future researchers may work on implementation with different methods of key generation and query optimization.

ACKNOWLEDGMENT

We are thankful to all the friends and evaluators for their valuable support for preparing and correcting the matter of this paper. We are thankful to the faculty and staff of Computer Sc Deptt, Bhagwant Univ., Ajmer.

REFERENCES

[1] A. Sachdev, M. Bhansali presented "Enhancing Cloud Computing Security using AES Algorithm", International Journal of computer application, Vol 67, No. 9 April, 2013, pp 19-23

[2] K. Handa, U. Singh discussed "Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing, Vol. 4, Issue 5, May 2015, pp 786-791

[3] B.K. Mohanta, D. Gountia, "Fully homomorphic encryption equating to cloud security: An approach", IOSR Journal of Computer Engineering, e-ISSN 2278-0661 , p-ISSN 2278-8727, vol 9, No. 2 , Feb, 2013, pp 46-50

[4] S. Bajpai and P. Srivastava, " A Fully homomorphic Encryption Implementation on Cloud Computing", International Journal of Information & Computation Technology, ISSN 0974-2239, Vol. 4 No. 8, 2014 pp. 811-816.

[5] D. Dave,R. Thakkar, "HOMOMORPHIC ENCRYPTION IN CLOUD COMPUTING", ijirt, Vol 1 Issue 12, ISSN 2349-6002, 2015, pp. 1352-1357.

[6] K. Benzekki, A. E. Fergougui, and A. E. B. E. Alaoui , "A Secure Cloud Computing Architecture Using Homomorphic Encryption", International Journal of Adv. Computer Sc. and Application", Vol. 7, No. 2, 2016, pp. 294-298.

[7] M. TEBAA, S.E. HAJJI, A. E. GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceeding of the World Congress on Engineering, Jul, 2012, Vol, I,, ISSN: 2078-0958 (Print), ISSN: 2078-0966 (online).

[8] HUANG Qin-long, MA Zhao-feng, YANG Yi-xian, FU Jing-yi, and NIU Xin-xin, "Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing", The Journal of China Universities of Posts and Telecommunications, Science Direct, Dec 2013, pp. 88-95

[9] Xiaofen Wang, "One-round secure fair meeting location determination based on homomorphic encryption", Information Sciences 372 (2016) 758–772, Elsevier, pp 758-771.

[10] S. Dasgupta, S.K. Pal, "proposed Design of a polynomial ring based symmetric homomorphic encryption scheme", Science Direct, Elsevier, Jul, 2016, pp 692—695.

[11] Z. Wang, G. Sun, D. Chen," A new definition of homomorphic signature for identity management in mobile cloud computing", Journal of Computer and System Sciences 80 (2014) 546–553

[12] Saravana K.N., Rajya Lakshmi G.V., Balamurugan B.," Attribute Based Encryption for Cloud Computing", International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science 46 (2015) 689 – 696

[13] Vu Mai, I. Khalil, "Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography", Future Generation Computer Systems, 2016, 0167-739X,

[14] S. Singh, Y.S. Jeong, J.H. Park, "A survey on cloud computing security: Issues, threats, and solutions", Journal of Network and Computer Applications 75 (2016), pp. 200–222

[15] F. Chao, X.Yang, "Fast key generation for Gentry-style homomorphic encryption", The Journal of China Universities of Posts and Telecommunications, December 2014, 21(6): pp. 37–44

[16] S. K. Pasupuleti, S. Ramalingum, R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing", Journal of Network and Computer Applications 64 (2016) pp. 12–22

