JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-6, Issue-3 E-ISSN: 2347-2693

Enhancing Secure and Efficient Online Data Storage over Cloud Using Homomorphic with Probabilistic Encryption

.Mehak Gandhi[1*], Kiranbir Kaur[2]

[1*]Dept. CET, Guru Nanak Dev University, Amritsar, India
[2] Dept. CET, Guru Nanak Dev University, Amritsar, India

[*]Corresponding Author: mehakgandhi06@gmail.com, Tel.: +91-9888124723

Available online at: www.ijcseonline.org

Received: 20/Feb//2018, Revised: 26/Feb2018, Accepted: 19/Mar/2018, Published: 30/Mar/2018

***Abstract*—** Cloud computing is the paradigm used to provide resource on share basis to multiple machines. Due to availability of resources this mechanism becoming extremely popular for accessing resources as and when desired by machines. Reliability however is the issue associated with cloud computing. Data transferred and stored over the cloud will be under siege due to the malicious access or attacks. This paper present the comprehensive survey of techniques used in order to encrypt the data and enhance reliability of cloud. Cloud reliability enhancement is ensured using the encryption algorithms which are researched over the past era. Efficient parameters are extracted and qualitative comparison is presented to depict the efficient encryption mechanism that can be used in future works.

***Keywords*—**Cloud Computing, Reliability, Encryption.

I. INTRODUCTION

In today's era cloud computing becomes the hottest topic due to its ability to reduce the cost associated with computing. Cloud computing provides the on demand services like storage, servers, resources etc. to the users without physically acquiring them and the payment is according to pay per use. Since cloud provides the storage, reduces the managing cost and time for organization to the user but security and confidentiality becomes the one of the biggest obstacle in front of us. The major problem with cloud environment is, the number of user is uploading their data on cloud storage so sometimes due to lack of security there may be chances of loss of confidentiality. To overcome these obstacles a third party is required to prevent data, data encryption, and integrity and control unauthorized access for data storage to the cloud.

With the rapid development of hardware and software cloud computing brings the revolution in the business industry[1]. It provides resources like computational power, storage, computation platform ad applications to user on demand through internet. Some of the cloud providers are Amazon, IBM, Google, Salesforce, Microsoft etc. Cloud computing features included resource sharing, multi-tenancy, remote data storage etc. but it challenges the security system to secure, protect and process the data which is the property of the individual, enterprises and governments. Even though, there is no requirement of knowledge or expertise to control the infrastructure of clouds; it is abstract to the user. It is a service of an Internet with high scalability, quality of service, higher throughput and high computing power[2]. Cloud computing providers deploy common online business applications which are accessed from servers through web browser. Data security is the biggest issue in cloud computing and it is not easy to resolve it.

I.I SECURITY ISSUES IN CLOUD COMPUTING

In cloud environment usual data transmission occurs between client and server using third party. So the confidentiality of your data becomes the primary problem. Security issues for a significant number of these frameworks and innovations are pertinent to distributed computing[3]. For instance, the system that interconnects the frameworks in a cloud must be secure and mapping the virtual machines to the physical machines must be completed safely. Information security includes encoding the information and additionally guaranteeing that suitable strategies are implemented for information sharing[4]. Cloud security isn't to be mistaken for "cloud-based" security benefit over the conventional danger. This security administration can be upgraded with the distributed computing, ensuring against DDOS, Trojan, Virus and Spam and so on more viably than any other time in recent memory[5].

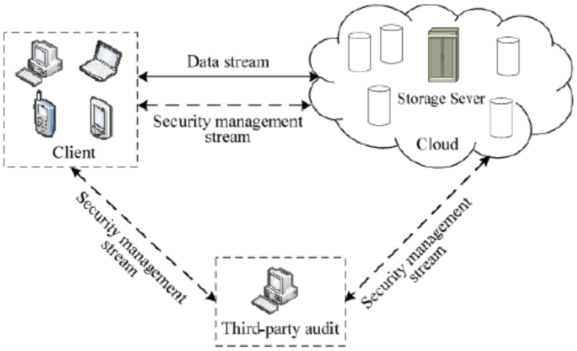
Data stream
Security management stream
Client
Storage Sever
Cloud
Security management stream
Security management stream
Third-party audit

Figure 1: Data storage structure of Cloud Computing

However, the qualities of distributed storage make clients' information looked with numerous security dangers, incorporates: (1) the conventional security district parcel is invalid. On account of the distributed storage benefit must be adaptable, security limits and assurance hardware can't be unmistakably characterized, which builds some trouble for the usage of particular assurance measures; [6](2) the distributed storage transmits information through the system. The benefit interferences, information devastation, data stolen furthermore, altered caused by the noxious assaults in the organize represent a serious test to the security of information correspondences, get to confirmation and classification; [7](3) from the client's view, the distributed storage of information makes distributed computing specialist co-op gets the information get to control, and the client's information is looked with protection security dangers. Individuals stress over that the touchy individual information will be exposure, abuse or missing by putting the information in cloud condition[8]. To tackle the above issues, as of late, scientists made a parcel of research work in the information security to control systems, information respectability, confirmation, cipher text to recover and information encryption system of cloud figuring condition[9].

There are lots of security issues with cloud computing because of technologies utilization including networks, operating systems, databases, resource scheduling, virtualization, load balancing, transaction management, memory management and concurrency control. For example, the network should be secure on cloud so that mapping the virtual machines to the physical machines has to be carried out securely[10]. Data security not only involves encrypting the data but also gives surety of appropriate policies. Cloud computing suffers from some various security concerns which are given below.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

I.I.I CLOUD SECURITY CHALLENGES

Some of the cloud security challenges that come in front of users are given below:

a. Authentication: The data on the internet is available to all the unauthorized users. Therefore the confidentiality of the data can be lost.
b. Access Control: To give access to only legalized users some control policies are used. These services must be adjustable, well planned, and their allocation is overseeing conveniently[11].
c. Policy Integration: There are many cloud providers they use their own policies and approaches. Some of them are Amazon, Google who provides services to end users.
d. Service Management: In this different cloud providers such as Amazon, Google, comprise together to provide services to meet their customers need.
e. Trust Management: The trust management approach must be developed so that trust remains between both parties such as user and provide.

The main contribution of this paper is to enhance cloud security and increase space efficiency by minimizing the amount of space required for redundant data. To optimize better results we will review some paper and find the better results to remove the security barriers. Rest of the paper is organised as follows: Section I provide the security concerns in cloud, Section II provide the related work of existing techniques to derive the best possible technique for future enhancements, since security is low in existing system. Section III present the comparison table of existing methodology for generating decision about technique to be used in future, Section IV gives research gaps which indicates things that would be incorporated and missing in existing system, Section V enhances the problem definition, Section VI defines the main objective of the paper, Section VII focuses on methodology and Section VIII concludes the research work with future direction.

II. RELATED WORK

The cloud security is always a concern and researchers are working towards this issue to enhance security of cloud using optimal strategies. This section present the comprehensive literature survey of most efficient encryption strategies used to enhance security concerns.

In [12] reviewed strategies used to enhance cloud security. Security requirements and objectives of cloud security is discussed in this literature. Accessing resources of the cloud and securely allocating it for effective utilization of cloud is suggested. The problem with this literature is qualitative analysis. Parameters are not extracted and compared using this literature.

In [13] proposed hybrid symmetric encryption mechanism for cloud security. Secure and protected data storage is presented using this literature. In this model, sender outsourced the data towards the destination and decryption key is hidden from the intruder. The authorization is required in order to access the key. The key is used to decrypt the data. Use of hybrid encryption makes the data more secure and less prone to attacks.

In [14] proposed order preserving encryption mechanism. Differential attacks were conducted to judge the security of order preserving encryption mechanism. Estimated distribution can be calculated by the sender in order to determine the attack. The attack is limited due to encryption mechanism employed within order preserving encryption.

In [15] suggested and reviewed the techniques used within cloud to ensure integrity of data stored within cloud computing. Risk and advantages associated with encryption algorithms such as RSA was analysed. Qualitative analysis of parameters is not done in this literature.

In [16] proposed a data access mechanism using authorization in multi authority cloud system. Concept of update and secret key are used in order to encrypt and decrypt the information. Encryption and decryption mechanisms are securely performed by the use of secret keys. Reliability is enhanced by the application of data access mechanism. Data access mechanism distributes data access controls to the users. Users can access only that part of the cloud to which they have authority. Security and protection of data stored within the cloud is greatly enhanced using this mechanism.

In [17] proposed block level encryption standards. The mechanism first of all fetches the similar blocks from the files stored within the cloud. The fetched blocks are encrypted and stored back over the cloud. The similar blocks are indexed and hence less storage requirements exist in this case. In cloud cost is encountered on the pay per use basis. Hence cost is significantly reduced.

In [18] proposed query based homomorphic encryption slandered in cloud. This type of encryption performs computation on cipher text. This computation generates a encrypted result. During decryption, the generated plain text exhibits same computation as on cipher text. This encryption is one of the most secure mechanism for securing and protecting data stored within cloud computing.

Literature survey suggest that there is a room for improvement in the security concern within cloud computing. The most secure cloud security mechanism is homomorphic encryption that can be extended by including block level redundancy handling mechanism to save space and subsequently cost associated with storage.

III. COMPARISON TABLE

Table 1. Comparison Table for Security in Cloud Computing

Title	Technique	Parameters	Merits	Demerits
Query based computation on encrypted data through homomorphic encryption in cloud computing security [18]	Homo-morphic Encryption	Availability Execution Time	Execution time is decreased and availability is enhanced	Space conservation is poor
Cloud Computing security: From Single Cloud to Multi-	Digital Signature	Execution time	Security is enhanced and execution time is decreased	Block level security enhanceme-nt is missing.

Clouds using Digital Signature [19]				
Security transparency:the next frontier for security security research in the cloud Moussa Ouedraogo1*, Severine Mignon1, Herve Cholez1, Steven Furnell2 and Eric Dubois1 [20]	Security Transparency between cloud service providers and users	No parameters specified	Transparency is suggested to ensure better security	No quantitative analysis of security parameters
An Efficient Protocol with Bidirectional Verification for Storage Security in Cloud Computing[21]	Bidirectional verification for storage security in cloud	Computational overhead	Computation overhead is reduced	Space utilization is high so cost and space must be optimised
Secure Algorithm for Cloud Computing and Its Applications [22]	HE-RSA	Execution time	Execution time is reduced	Space complexity is high due to redundancy
Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors[23]	Security algorithm for Cloud radio Channels	Execution time	Execution time is reduced by the application of this technique	Space and redundant parameters are not considered
BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication[24]	Block level message locked deduplication	Execution time Space utilization	Execution time is reduced and space utilization is reduced	Bit level redundancy handling mechanism can increase the performance of this approach
Optimal Scheduling In Cloud Computing Environment Using the Bee Algorithm [25]	Optimised scheduling of resources in cloud for security enhancement	Makespan	Makespan is reduced	Security parameters can be enhanced further considering encryption within allocation
Modern Applications of QR-Code for Security [26]	QR based Security	Execution time	Execution time is reduced	Generating QR code is exceedingly difficult
Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review [27]	Review of security mechanisms are presented	No parameters specified	Different security techniques are analysed which can be used for future enhancement	Qualitative analysis of parameters is missing

IV. RESEARCH GAP

The techniques analysed worked on execution time reduction and safely storage if information over the cloud. The space conservation however is not considered. In other words there could be multiple keys which are generated for same information. In cloud cost is encountered on the basis of pay per use. This cost can be minimised by the use of space conservation mechanism. Redundancy handling mechanism along with homomorphic encryption can ensure efficient storage and space conservation mechanism.

V. PROBLEM DEFINITION

Cloud computing is the need of the hour and used heavily now days by almost every organization due to practically infinite resources provided by it. As the users of cloud increase so does the threats. Malicious users can corrupt the data. Also cloud is vulnerable to attacks like DDOS. In order to tackle the issue space conservation and encryption could be a solution that is partially handled in existing literature using homomorphic encryption. Redundancy handling mechanism however is missing. Problems formulated from existing literature is listed as under

1. Encryption process becomes weekend through the application of redundancy.
2. Space conservation mechanism is missing
3. Cost of storage enhanced greatly by the use of existing literature.

VI. OBJECTIVE OF THE STUDY

Cloud security is of prime concern and enhancement procedure is suggested in the proposed literature. Our objective is to introduce redundancy handling to minimise storage requirement and to enhance efficiency of homomorphic encryption. Cost associated with the overall system can be further reduced as storage requirement is minimised.

Parameter Consideration for optimization

- Space Utilization

Equation used for this purpose

Space Utilization= Task Size/Task Space (1)

- Execution time

This is the time required to execute entire task over the cloud

Execution Time= Finish Time-End Time (2)

- Reliability

  This parameter is obtained from the execution time observed in case of existing and proposed literature. Since reliability is an indirect metric hence it will be evaluated from the above two factors.

VII. METHODOLOGY

The methodology describes the steps to be followed in order to enhance the existing literature

Input: Cloudlets

Output: Space Utilized, Execution Time

a. Initialize Cloud, datacenters, VMs and Brokers
b. Restructure Cloudlet
   Perform Redundancy check and replace it with index value
c. Submit cloudlet for encryption (homomorphic)
d. Encrypted Cloudlets are submitted for execution
e. Generate Result in terms of space utilization and execution time

VIII. CONCLUSION AND FUTURE WORK

Cloud computing not only provides the resources to the users but also give a big challenge of security. There are securities requirements for both users and cloud providers but sometimes it may conflict in some way. Security of the cloud depends upon trusted computing and cryptography. In our review paper some issues related to data location, security, storage, availability and integrity. Establishing trust in the cloud security is the biggest requirement. These issues mentioned above will be the research hotspot of cloud computing. The homomorphic encryption with redundancy handling mechanism can be future scope for this literature. The result would be better and may enhance security of the information over the cloud.

REFERENCES

[1] X. Yu, “Intelligent Urban Traffic Management System Based on Cloud Computing and Internet of Things,” pp. 2169–2172, 2012.

[2] B. Mills, T. Znati, and R. Melhem, “Shadow Computing: An energy-aware fault tolerant computing model,” *2014 Int. Conf. Comput. Netw. Commun.*, pp. 73–77, 2014.

[3] C. A. Chen, M. Won, R. Stoleru, and G. G. Xie, “Energy-efficient fault-tolerant data storage and processing in mobile cloud,” *IEEE Trans. Cloud Comput.*, vol. 3, no. 1, pp. 28–41, 2015.

[4] S. S. Lakshmi, “Fault Tolerance in Cloud Computing,” vol. 04, no. 01, pp. 1285–1288, 2013.

[5] R. Buyya, C. S. Yeo, and S. Venugopal, “Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities,” *Proc. - 10th IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2008*, pp. 5–13, 2008.

[6] Z. Xiao, W. Song, and Q. Chen, “Dynamic Resource Allocation Using Virtual Machines for Cloud Computing Environment,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1107–1117, Jun. 2013.

[7] U. Wajid, C. Cappiello, P. Plebani, B. Pernici, N. Mehandjiev, M. Vitali, M. Gienger, K. Kavoussanakis, D. Margery, D. G. Perez, and P. Sampaio, “On Achieving Energy Efficiency and Reducing CO 2 Footprint in Cloud Computing,” vol. 7161, no. c, 2015.

[8] Y. Xie, H. Wen, B. Wu, Y. Jiang, and J. Meng, “Transactions on Cloud Computing,” vol. 13, no. 9, 2015.

[9] D. Ardagna, G. Casale, M. Ciavotta, J. F. Pérez, and W. Wang, “Quality-of-service in cloud computing : modeling techniques and their applications,” pp. 1–17, 2014.

[10] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, “A view of cloud computing,” *Commun. ACM*, vol. 53, no. 4, p. 50, 2010.

[11] S. Saha, S. Pal, and P. K. Pattnaik, “A Novel Scheduling Algorithm for Cloud Computing Environment,” vol. 1, 2016.

[12] P. You, Y. Peng, W. Liu, and S. Xue, “Security Issues and Solutions in Cloud Computing,” 2012.

[13] S. Kaushik, “Cloud data security with hybrid symmetric

encryption," pp. 0–4, 2016.

[14] K. Li, W. Zhang, C. Yang, and N. Yu, "Security Analysis on One-to-Many Order Preserving Encryption Based Cloud data Search," vol. 6013, no. c, pp. 1–9, 2015.

[15] F. Sabahi, "Cloud Computing Security Threats and Responses," pp. 245–249, 2011.

[16] X. Wu, R. Jiang, and B. Bhargava, "On the Security of Data Access Control for Multiauthority Cloud Storage Systems," pp. 1–14, 2015.

[17] Y. Zhao and S. S. M. Chow, "Updatable Block-Level Message-Locked Encryption," pp. 449–460, 2017.

[18] V. Biksham, "Query based computations on encrypted data through homomorphic encryption in cloud computing security," pp. 3820–3825, 2016.

[19] G. A. Prajapati, S. S. Satav, S. Dahiphale, S. More, and P. N. Bogiri, "Cloud Computing Security : From Single to Multi-Clouds using digital signature," vol. 2, no. 6, pp. 204–213, 2014.

[20] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, and E. Dubois, "Security transparency : the next frontier for security research in the cloud," *J. Cloud Comput.*, 2015.

[21] B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu, T. Qiu, and S. Member, "An Efficient Protocol with Bidirectional Verification for Storage," vol. 3536, no. c, pp. 1–13, 2016.

[22] A. Bhandari, "Secure Algorithm for Cloud Computing and Its Applications," pp. 188–192, 2016.

[23] J. I. A. You, Z. Zhong, G. Wang, B. O. Ai, and S. Member, "Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors," vol. 2, 2014.

[24] R. Chen, Y. Mu, G. Yang, and F. Guo, "BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 12, pp. 2643–2652, Dec. 2015.

[25] N. Hesabian, H. Haj, and S. Javadi, "Optimal Scheduling In Cloud Computing Environment Using the Bee Algorithm," vol. 3, no. 6, pp. 253–258, 2015.

[26] K. Saranya and A. Professor-i, "Modern Applications of QR-Code for Security," no. March, pp. 1–5, 2016.

[27] O. Harfoushi, B. Alfawwaz, N. a. Ghatasheh, R. Obiedat, M. M. Abu-Faraj, and H. Faris, "Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review," *Commun. Netw.*, vol. 06, no. 01, pp. 15–21, 2014.

Authors Profile

Mehak Gandhi pursued BTech in Computer Science from DAV Institute of Engineering and Technology,Jalandhar in year 2016. She is currently pursuing Mtech in Computer Science from Guru Nanak Dev University,Amritsar and currently working as Research Scholar in Department of Computer Science. Her main research work focuses on Cryptography Algorithms, Cloud Security and Privacy.

Kiranbir Kaur pursued BTech in Computer Science and MTech from Guru Nanak Dev University, Amritsar in year 2008. She is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science,Guru Nanak Dev University, Amritsar. She has published more than 10 research papers in Ugc approved Conferences.Her main research work focuses on Cloud Computing Interoperability and Portability, Cloud Security and Privacy. She has 6 years of teaching experience.