# KEY ISSUES IN CLOUD COMPUTING SECURITY: A REVIEW

[1.]Prakash H. Unki, [2.]Suvarna L. Kattimani, [3.]Kirankumar B.G*
[1,2,3] BLDEA'S V.P. Dr. P.G. Halakatti College of Engineering & Technology ,Vijayapur,
[1,2,3] VTU Belagavi

***Abstract— Mobile Cloud computing applications are the new extensions of cloud technologies. Nowadays, these clouds technologies have rapid growth in IT Industry.using cloud, mobile devices can store and retrieve any kind of data from cloud networks. Despite the many benefits of these technologies, there are some issues such as security and privacy that degrade the efficiency of mobile cloud computing. In the first part, we discussed data sharing in mobile cloud computing. In the second part, we discussed the detailed literature review of various algorithms and methodologies. The purpose of the review is considering the problems and limitations of previous research gaps in terms of secure optimal data sharing with limited resources security paradigms such as using public key cryptographic systems***

**Index Terms—*AES* algorithm, *DES algorithm, Proxy-Re-encryption***

## I. INTRODUCTION

The recent development in cloud computing and smart mobile devices makes people share their data stored in the cloud. Typically, mobile devices are having less computational resources compared to cloud computing. In these situations, it is important to use resources more optimal to share and store the data.

Nowadays, a variety of cloud mobile applications are widely available in the market to share the people data in the form of a photo, video, audio documents. most of the mobile cloud applications provide data management functionalities for data owners and data users. These applications are not sufficiently handling the sensitive data in the cloud. And they do not meet the needs of the data owners.to solve these problems the following methods have to be adopted.

First, encrypting personal or sensitive data before uploading the cloud. Second, providing the access control mechanism through cipher text description, third user authentication is achieved through the efficient distribution of encryption /decryption keys.

## II. LITERATURE REVIEW

In [1], the authors have discussed the problem of data disclosure risk during data transfer in cloud computing. To solve this problem implemented the homomorphic scheme with symmetric keys. Ample of the emphasis is on communicating the capabilities to public key cryptosystems and these applications handle the symmetric keys to access the private data efficiently in cloud computing.

In [2], the authors have addressed the issues related to data privacy during data sharing in mobile cloud computing. Data privacy is one of the key challenges when users outsource their data in the cloud, to overcome this issue they have implemented Advanced Encryption Standard on JPEG encoders for providing the data privacy for mobile computing.

In [3], the authors have proposed the new methodology to solve the problems of revocation and re-encryption of data in cloud computing. Whenever the data owner revoke data from one cloud service provider (CSP) to another CSP, data has to re-encrypt with a new key, it makes more cost.to avoid these they have applied the attribute-based proxy re-encryption method.it decreases the communication cost between the data owner and cloud storage. An experimental result shows that the proposed method reduces the communication cost.

In [4], the authors have discussed various lightweight secure data sharing access control policies available in cloud computing, they have mainly focused on challenges of storing and sharing the data in mobile cloud computing. And adopted the cipher text-based attribute encryption algorithm which holds the data confidentiality of outsourced data in the

cloud and meanwhile it also gives efficient access control in the mobile cloud.

In [5], the authors have explained most important security issues like integrity, availability, confidentiality, and in cloud computing and also suggested the suitable measures to handle these challenges, they are Identity Based Encryption, and attribute-based encryption and proxy re-encryption these algorithms are used to share documents in public cloud environment with great security measures. In these algorithms a pair of private and public keys, distribution gives flexibility in access control.

In [6], the authors have discussed privacy issues and access control in collaborative cloud organizations. They have implemented the "Federation as a Services "(FAAS) to adopt the attribute-based access control guidelines for data privacy. Users can access the coalesced data when their identity attributes match the guidelines without see-through the attributes in clear. all members of the federation have complete access control on data.

In [7], the authors have discussed the data security issues for public cloud service.in public cloud environment is having more crowded with heterogeneous users, among them, some of them are legitimate users, and some are fake or malicious users. Testing each user's authenticity cost more and it also increases the communication cost. To solve this problem, they have adopted half a decryption scheme.it diminishes the computing and data communication cost.

In [8], the authors have presented various data modification problems in Electronic Health Records. due to a large amount of stored in EHR records, it is difficult to avoid the integrity and modification attack in cloud computing. There are various algorithms are available to ensure these kinds of attacks but they have some limitations. Attribute-Based Encryption is more suitable for EHR storage, it provides a secure and less computational overhead mechanism to medical organizations and gives cloud-based access to medical providers.

In [9], the authors have discussed the various cloud-based key management issues, distributing a key in public mobile clouds is a tedious task. Because of the crowded users.to face these issues, they have adopted the efficient Key management policies.it provides encrypted keys are stored in the cloud and automatically shared and distributed. These are valid only one time, so it achieves greater efficiency in key management and saves the user time.

In [10], the authors have addressed the problems of an efficient solution for distribution of resources among cloud users. Whenever the data belonging to multiple people in the cloud, it is very difficult to share in groups. Any modification done by single owner creates imbalances in data access.to solve this they have implemented a concept called MONA (Multi-owner data sharing) it offers any cloud users can share the data with others. Meanwhile, data access and computation cost are independent with a number of revoked users.

In [11], the authors have addressed the problem of malicious users present in multi-cloud environments in health record sharing organization. Malicious users easily revoke access without generating fresh encryption keys.it makes the data in the cloud become open to all public users in the multi-cloud environment and causes security attacks by malicious users.to overcome this problem they have adopted the revocable key policy-based encryption scheme.

In [12], the authors have discussed the issues related to secure data sharing in cloud computing. usually in cloud environment increased file transfer taken place.at the same time it increases the more power consumption and communication cost, there are chances of security violations during the file transfer.to solve this problem they have proposed aggregate key forward security key encryption and re-encryption standard.

In [13], the authors have discussed the various security and cryptographic techniques in cloud computing to confirm the security of the data in cloud computing. Employed the fully homomorphic encryption cloud managed key encryption, identity-based encryption to resolve the limitation of attribute-based encryption in real-time applications.

In [14], the authors have presented the various methologies which are available in the encryption and decryption during the data transfer between the sender and receiver. Implemented the key policy-based attribute encryption. recognized the problem during the decryption of encrypted data is not decided by encryptor.

In [15], the authors have conducted a literature survey on secure data sharing in clouds. Mainly focused on multiple

security issues occurs due to different users in the group.to solve this issue they have adopted Symmetric encryption using multiple key management.it allows multiple users to access data at the same time.

## CONCLUSION

In this research, various security issues like privacy, Integrity, data availability has been clearly discussed with the appropriate solutions. Data sharing in the mobile cloud will deliver efficient secure data storage, It can use various cryptographic techniques like AES, DES, symmetric AES, multiple key AES,ECC provides less security whereas Proxy Re-encryption, homomorphic, asymmetric algorithm can provide better security in mobile communication with cloud data sharing.

## REFERENCES


[1] C. P. Gupta and I. Sharma, "A fully homomorphic encryption scheme with symmetric keys with application to private data processing in clouds," 2013 Fourth International Conference on the Network of the Future (NoF), Pohang, 2013, pp. 1-4.

[2] M. Bahrami and M. Singhal, "A Light-Weight Permutation Based Method for Data Privacy in Mobile Cloud Computing," *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, San Francisco, CA, 2015, pp. 189-198.

[3] Y. Jin, C. Tian, H. He and F. Wang, "A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing," *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*, Dalian, 2015, pp. 172-179.

[4] Y. Yasumura, H. Imabayashi and H. Yamana, "Attribute-based proxy re-encryption method for revocation in cloud storage: Reduction of communication cost at re-encryption," *2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA)*, Shanghai, 2018, pp. 312-318.

[5] S. Alansari, F. Paci, A. Margheri and V. Sassone, "Privacy-Preserving Access Control in Cloud Federations," *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, Honolulu, CA, 2017, pp. 757-760.

[6] C. Wise, C. Friedrich, S. Nepal, S. Chen and R. O. Sinnott, "Cloud Docs: Secure Scalable Document Sharing on Public Clouds," *2015 IEEE 8th International Conference on Cloud Computing*, New York, NY, 2015, pp. 532-539.

[7] Y. Zhou and L. Wang, "SDS2: Secure Data-Sharing Scheme for Crowd Owners in Public Cloud Service," *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, Shenzhen, 2017, pp. 22-29.

[8] M. Joshi, K. Joshi and T. Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems," *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, 2018, pp. 932-935.

[9] P. K. Tysowski and M. A. Hasan, "Cloud-hosted key sharing towards secure and scalable mobile applications in clouds," *2013 International Conference on Computing, Networking and Communications (ICNC)*, San Diego, CA, 2013, pp. 449-455

[10] X. Liu, Y. Zhang, B. Wang and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1182-1191, June 2015

[11] Cheng - Kang Chu , Sherman S. M. Chow , Wen - Guey Tzeng, Jianying Zhou, and Rober H Deng,"Key- Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage ," IEEE Transactions on Parallel and Distributed Systems,vol. 25,no. 2, pp.468 - 477, Feb 2014. Huijun Zhu , Licheng Wang , Haseeb Ahmad , Xinxin Niu," Key Policy Attribute - Based Encryption with Equality Test in Cloud Computing ", IEEE Access , vol.5 , pp . 20428 –20439, Sep.2017.

[12] Parmar Vipul Kumar J., RajaniKanth Aluvalu ," Key Policy Attribute Based Encryption ( KP- ABE ) : A Review, International Journal of Innovative and Emerging Research in Engineering ,vol. 2, no. 2,pp. 49- 52,2015.

[13] Mansoor Ebrahim , Shujaat Khan , Umer Bin Khalid ," Symmetric Algorithm Survey : A Comparative Analysis , " International Journal of Computer Applications ,vol. 61, no.20,pp.12-19 , Jan 2013.

[14] Anmin Fu , Shui Yu, Yuqing Zhang ,Huaqun Wang and Chanying Huang , " NPP : A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users," IEEE , vol . PP,no. 99,pp.1-1,May 2017.

[15] Swati V . Thakre, K.K.Chhajed,V.B.Bhagat,"Review on Key Based Encryption Scheme for Secure Data Sharing on Cloud ," International Research Journal of Engineering and Technology.