# Fuzzy Identity-Based Encryption Data Service with Security Auditing in Clouds

[1]Vemuri Jayamanasa, [2]Chalasani Srinivas, [3]Gadi Nirmala
*[1]M.Tech Student, Department of CSE, Sir C R Reddy College of Engineering,*
*[2]Assistant Professor Department of CSE, Sir C R Reddy College of Engineering,*
*[3]Associate Professor, Department of CSE, Sir C R Reddy College of Engineering,*
*([1]vemuri.jayamanasa@gmail.com)*

***Abstract***-Cloud computing is a form of distributed computing wherein resources and application platforms are distributed over the Internet through on demand and pay on utilization basis. There are many issues that counter data stored in the cloud starting from virtual machine which is the mean to share resources in cloud and ending on cloud storage itself issues. Cloud computing structure allows access to information as long as an electronic device has access to the web. In this technology users have to entrust their data to cloud providers, there are several security and privacy concerns on outsourced data. The cipher text will only be decrypted if each the time instant is within the allowed quantity and also the attributes related to the cipher text satisfy the key's access structure. The proposed scheme provides security and convenience for mobile users to access multiple mobile cloud computing services from multiple service providers using only a single private key. Set Based Encryption, Fuzzy Identity-Based Encryption, Hierarchical Identity-Based Encryption, Hierarchical Attribute-Based Encryption and Hierarchical Attribute-Set Based Encryption for access control of outsourced data are discussed. Once User specified expiration, time the info are securely, self-destructed scheme is secure beneath the choice l-bilinear Diffie Hellman inversion assumption. From system implementation point of view, verification tables are not required for the trusted smart card generator (SCG) service and cloud computing service providers when adopting the proposed scheme.

***Index Terms****-Identity-based cryptography;Proxy public key; Remote data integrity checking; Sensitive data; secure self-destructing; Fine Grained Access Control.*

## I. INTRODUCTION

Cloud refers to the network that provides services to network through internet. It is a model that enables the characteristics like on demand self-service, pay-as-you-use-service. National Institute of Standards and Technology defines cloud computing as a convenient, on-demand computing resources for storage services [1]. In addition, memory, processor, bandwidth and storage are visualized and can be accessed by a client using the Internet [2]. Cloud computing is composed of many technologies such as service oriented architecture, virtualization, web 2.0 and more. A cloud can be private or public. In public, cloud service can be sold to anyone on the Internet [3]. In private, cloud act as a proprietary network or hosted services are supplied to limited people through Data Centre. It may be Private or public the ultimate goal of cloud computing is to provide easy, scalable access to computing resources [4]. To fulfill this challenge, it is necessary to style a comprehensive resolution to support user-defined authorization amount and to produce fine-grained access management throughout to shared information to be self-destroyed once the user outlined expiration time [5]. As a result of the possession of the knowledge is separated from the administration of them, the cloud servers may migrate user's data to completely different cloud servers in outsourcing or share them in cloud wanting [6]. To check whether or not the outsourced files are kept intact, the file owner or an auditor can challenge the cloud server with low communication overheads and computation costs. If some part of the file has been altered or deleted [7]. The model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [8].

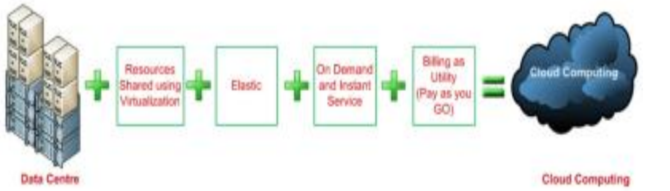
Resources Shared using Virtualization
Elastic
On Demand and Instant Service
Billing as Utility (Pay as you GO)
Cloud Computing
Data Centre
Cloud Computing

*Fig. 1: Schematic definition of cloud computing*

## II. RELATED WORK

Traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations and how to prove data freshness. Batch Auditing can be used to distinguish who is the signer on each block [9]. Currently employed a coverage graph to elucidate the connection among attributes and therefore the protection class and projected a coverage-based secure statistics deletion theme [10]. Reardon et al. leveraged the graph idea, Btree form and key wrapping and projected a novel approach to the planning and analysis of comfy deletion for persistent storage devices [11]. The principle plan of the above-noted schemes is that they severally integrate specific crypto logic techniques with the DHT network to supply fine-grained info get admission to regulate throughout the lifecycle of the enclosed records and to place into result records self-destruction when expiration [12]. To support multi-keyword search and result significance positioning, to receive Vector Space Model (VSM) to construct the searchable file to accomplish precise list items. To enhance search productivity outline a tree-based record structure which supports parallel search to exploit the intense processing limit and assets of the cloud server [13].

## III. SYSTEM MODEL

Cloud Computing provides many technologies for security issues like Service Oriented Architecture (SOA) [14]. Virtualization allows multiple users to share a physical server. In virtualization environment storage strengthening at the file system is desirable because it enables data sharing, administration efficiency and performance optimization the security requirements in multitenant file systems are analyzed [15]. High Availability and Integrity Layer (HAIL) [9] model helps in developing a tool to improve the security and efficiency. HAIL helps in managing the file integrity and helps in availability of file across the set of servers or independent storage device [16]. It is a time reference server without any interaction with other entities involved in the system. It is responsible for a precise release time specification [17].

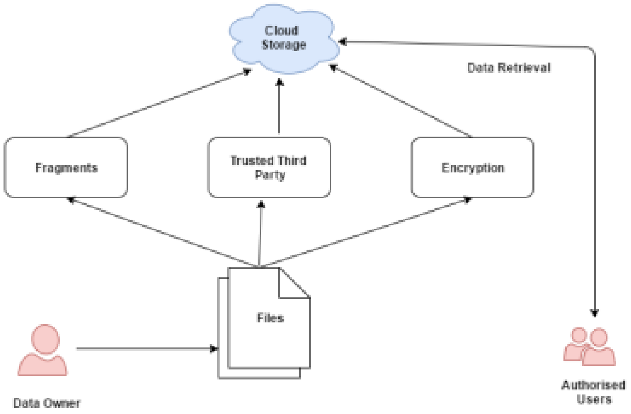

*Fig .2: The Architecture of Data Storing Security and Privacy.*

## IV. PROSED SYSTEM

The HAIL works when there is corruption. It is detect the corruption but it remedies it by avoiding this corruption in a subset of storage providers by using the data in the other service provider storage [18]. The proposed uses many clouds to build a cloud-of-clouds to address two security requirements in their storage system, which are confidentiality and availability of data. They combined the byzantine quorum protocol is well secret sharing cryptographic and erasure codes [19]. It is an aggregate key where each part of it can decrypt part of the cipher text key can decrypt the whole cipher text. Therefore, this cryptosystem helps in sharing data among a group of users with fine grain access control and without giving them a key that can decrypt all that data [20]. In public cloud to concentrates on the identity-based proxy oriented information uploading and remote information integrity checking.

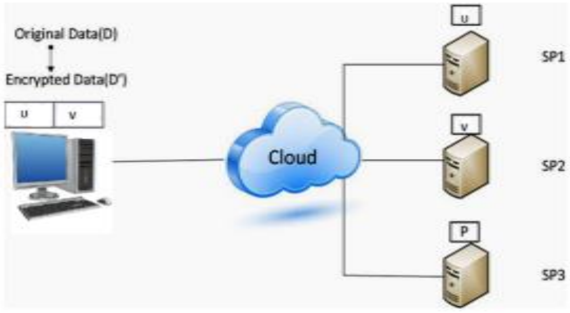

*Fig. 3: The proposed parity scheme*

*A.* Ciphertext-Policy Attribute Based Encryption In CP-ABE schemes attribute policies are associated with data and attributes are associated with keys. Decryption is enabled only same keys is associated with attributes satisfy the policy associated with the data. Our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC) [21]. The CP-ABE users can use all possible combinations of attributes issued in their keys to satisfy policies. This scheme is support user attributes and organized logically single set. CP-ABE schemes that support numerical attributes are limited to assigning only one value to any given numerical attribute within a key [22]. Data Owner to get key from key generator Encrypt the file. Encryption is the modify data is called a cipher text that cannot be easily understood by unauthorized people.

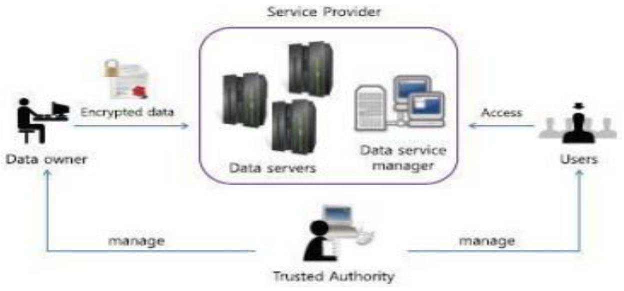

*Fig .4 :Architecture of Data sharing System*

*B. Fuzzy Identity-Based Encryption*

The Fuzzy Identity-Based Encryption views an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for Fuzzy-IBE gives rise to two interesting new applications. The first is an Identity-Based Encryption system that uses biometric identities. Since biometric measurements are noisy, we cannot use existing IBE systems [23]. Secondly Fuzzy IBE is used for an application that we call “attribute-based encryption”. In this application a party will wish to encrypt a document to all users that have a certain set of attributes. Set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then he will be able to decrypt the cipher text and obtain the data [24].

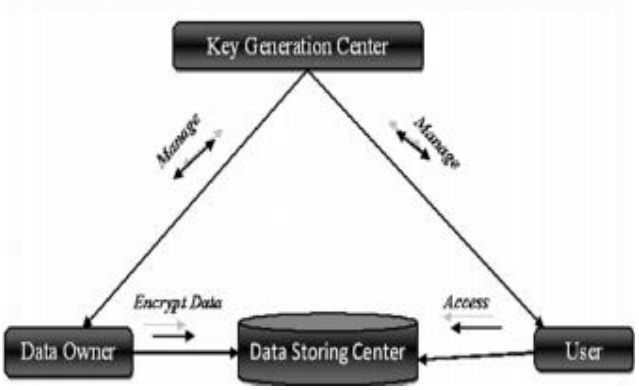

*Fig. 5: Node Structure of a Data Sharing System*

*C. Mobile Cloud Computing*

The advancement in mobile devices is more processing, storage, memory, sensors and operating system capabilities, there is a limitation of energy resources needed for complex computation. Some of the application in mobile devices is data-intensive or compute-intensive application [25]. Mobile cloud computing is using the mobile as front end and the cloud as back end for the storage and computation. Mobile cloud computing consists of mobile computing, cloud computing, and network. The file is divided to many blocks and each block is divided to many chunks and each chunk in n bits. Each block represents matrix with chunks number as rows and bits as columns. a code victor matrix is created from the entered password. Their proposed method has two requirements: balancing computation overhead with maintaining the security and avoiding offloading the file to the mobile cloud computing for encryption by making the file is meaningless before sending it.

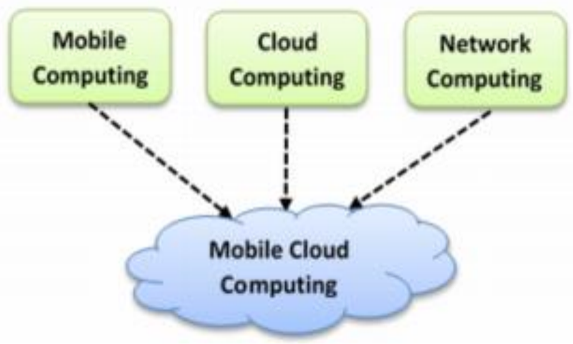

*Fig. 6: Mobile cloud computing*

*D. Third Party Auditor*

Third Party Auditor (TPA) is the person who has the skills and experience to carry out all auditing processes such as in the figure5. TPA scheme is used for checking the data integrity and doubtful actions, users of cloud storage depend on third party auditors [26]. Their proposed scheme attains data integrity and assures the data owner of the data security. The owner is aware of all his resources on the cloud. The data owner validates and modifications lesser than or equal to this threshold data. The data owner is supposed to do surprise auditing.

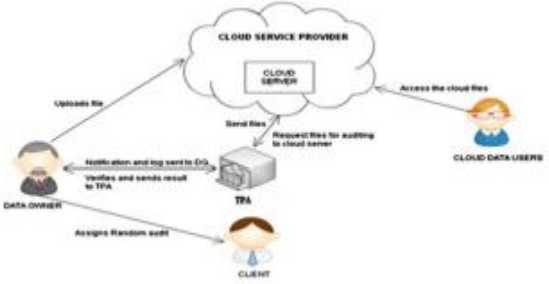

*Fig. 7: Architecture of third-party auditing*

## V. CONCLUSION

Cloud computing gives many advantages like storage security, increase storage space and reduce storage cost and decreases overheads on cloud, users. The cost of attractive when it is compared to building the infrastructure is many security models coming with this technology as happens when every technology matures. The concludes that the Hierarchical attribute-set- based encryption is the advanced encryption scheme for outsourcing data in the cloud service provider.

Only the authorized proxy can process and outsource the file on behalf of the file-owner. Both the file origin and file integrity is verified by a public auditor. Further, these different techniques are used in improving the security of the data stored and also giving privacy to the data. We mentioned new techniques that protect data seen by the cloud service provider while it is shared among many users. Many studies have been conducted to discover the issues that affect confidentiality, integrity, and availability of data to find a solution for them. This mechanism will be able to manage the time for each user to access the cloud data as a result the cloud cost will be dramatically reduces.

## REFERENCES

[1] D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud data protection for the masses,” Computer, IEEE, vol. 45, no. 1, pp. 39–45, Jan 2012.

[2] P. Mell and T.Grance, “The NIST Definition of Cloud Computing”, Natinal Institute of Standards and Techology, vol. 53, no.6, pp. 1-3, 2009.

[3] Leonard Heilig and Stefan Vob, “A Scientometric Analysis of Cloud Computing Literature”, IEEE Transactions on Cloud Comouting, vol. 2, no. 3, pp. 266- 278, July-September 2014.

[4] Cohen, Reuven, Rebello and Jagdish, “The State of Cloud Storage: A Benchmark Comparison of Speed, Availability and Scalability”, White paper, Nausni, 2015.

[5] J. J.Wylie, M. Bakkaloglu, V. Pandurangan, M.W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla, “Selecting the Right Data Distribution Scheme for a Survivable Storage System”,

[6] M. AlZain, E. Pardede, B. Soh, and J. Thom, “Cloud computing security: From single to multi-clouds,” in System Science (HICSS), 2012 45th Hawaii International Conference on, Jan 2012, pp. 5490–5499.

[7] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, “A review on remote data auditing in single cloud server: Taxonomy and open issues,” Journal of Network and Computer Applications, vol. 43, pp. 121–141, 2014.

[8] E. Aguiar, Y. Zhang, and M. Blanton, “An overview of issues and recent developments in cloud computing and storage security,” in High Performance Cloud Auditing and Applications. Springer, 2014, pp. 3–33.

[9] I. Gul, M. Islam et al., “Cloud computing security auditing,” in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on. IEEE, 2011, pp. 143–148.

[10] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, “Enhanced data security model for cloud computing,” in Informatics and Systems (INFOS), 2012 8th International Conference on. IEEE, 2012, pp. CC– 12.

[11] S.Yu,C.Wang,K.Ren,and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. IEEE INFOCOM 2010, 2010, pp. 534– 542.

[12] Beimel. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technology, Technion , Haifa, Israel, 1996.

[13] L. Cheung and C. Newport. Provably secure ciphertext policy abe. In CCS ’07:Proceedings of the 14th ACM conference on Computer and communications security, pages 456–465, New York, NY, USA, 2007. ACM.

[14] Adi Shamir. Identity-based cryptosystems and Signature schemes.In Proceedings of CRYPTO 84 on Advances in cryptology,pages 47–53. Springer-Verlag New York, Inc.,1985.

[15] L. Cheung and C. C. Newport, “Provably secure ciphertext policy abe,” in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 456– 465.

[16] Waters, “Ciphertext-policy attribute based encryption: An expressive, efficient, and provably secure realization,” Public Key Cryptography–PKC 2011, pp. 53–70, 2011.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM conference on Computer and Communications Security. ACM, 2006, pp. 89–98.

[18] A. F. Chan and I. F. Blake, “Scalable, server-passive, user anonymous timed release cryptography,” in Proceedings of the International Conference on Distributed Computing Systems. IEEE, 2005, pp. 504– 513.

[19] K. G. Paterson and E. A. Quaglia, “Time-specific encryption,” in Security and Cryptography for Networks. Springer, 2010, pp. 1–16.

[20] Q. Li, J. Ma, R. Li, J. Xiong, and X. Liu, “Large universe decentralized key-policy attribute-based encryption,” Security and Communication Networks, 2014.

[21] S. H. Islam and G. Biswas, “Design of improved password authentication and update scheme based on elliptic curve cryptography,” Math. Comput. Modelling, vol. 57, no. 11, pp. 2703–2717, 2013.

[22] S. H. Islam and G. Biswas, “Dynamic ID-based remote user mutual authentication scheme with smartcard using elliptic curve cryptography,” J Electron., vol. 31, no. 5, pp. 473–488, 2014.

[23] C.-L. Hsu, Y.-H. Chuang, and C.-l. Kuo, “A novel remote user authentication scheme from bilinear pairings via internet,” wireless Pers. Commun., vol. 83, no. 1, pp. 163–174, 2015.

[24] Matthew Malensek, Sangmi Pallickara, and Shrideep Pallickara, “MINERVA : Proactive Disk Scheduling for Qos in Multi-tier, Multi-tenant Cloud Environments”, IEEE Transactions on Internet Computing, vol. 20, no. 3, pp. 19-27, ISSN: 1089-7801, May-June 2016.

[25] Xu, Lei and Wu, Xiaoxin and Zhang, Xinwen, “CL-PRE: A Certificateless Proxy Re-encryption Scheme for Secure Data Sharing with Public Cloud”, In the Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 87-88, 2012.

[26] Kaitai Liang and Willy Susilo, “Searchable AttributeBased Mechanism With Efficient Data Sharing for Secure Cloud

Storage", IEEE Transaction on Informations Forensics and Security, vol. 10, no. 9, pp.1981-1992, September 2015