Multi Owner Multi User Privacy

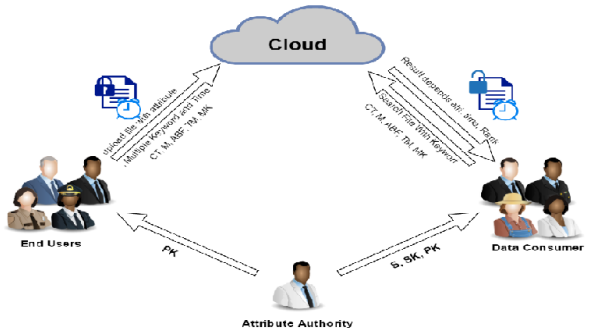
Prof Anuja Dombe[1], Prajakta Thorat [2], Surbhi Bhat A[3], Rohini Ahirrao[4]
[1,2,3,4] Jspm's RSCOE , Tathawade

Abstract- *In the realm of web of Things, sensitive information is distributed among many information homeowners, whereas multiple information users would like to access totally different aspects of this info. This paper presents a review of few recently implemented techniques to preserve privacy of multi-owner multi-user (MOMU) system. It also proposes a technique Cipher text Policy Attribute primarily based cryptography (CP-ABE) to preserve the privacy of a system where each owner has different privacy needs against each user, and different users may seek to collaborate in order to violate owner's privacy. Cipher text Policy Attribute primarily based cryptography (CP-ABE) may be a promising cryptography technique that allows end-users to encipher their information underneath the access policies outlined over some attributes of information shoppers and only permits information shoppers whose attributes satisfy the access policies to rewrite the information. Existing ways solely part hide the attribute values within the access policies, while the attribute names are still unprotected. In this paper we propose an efficient big data access control scheme with privacy-preserving policy. Specifically, we tend to hide the entire attribute (rather than solely its values) within the access policies. To assist data decryption, we also design a novel Attribute to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy.*

I. INTRODUCTION

In the era of big data, a huge amount of data can be generated quickly from various sources (e.g., smart phones, sensors, machines, social networks, etc.).Towards these big data, conventional computer systems are not store and process these data. Due to the flexible and elastic computing re-sources, cloud computing is a natural for storing and processing big data. With cloud computing, end-users store their data into the cloud, and rely on the cloud server to share their data to other users (data consumers). In order to only share end-users data to authorized users, it is necessary to design access control mechanisms according to the requirements of end-users. When out sourcing data into the cloud, end-users lose the physical control of their data. Moreover, cloud service providers are not fully-trusted by end-users, which make the access control more challenging. For example, if the traditional access control mechanisms (e.g., Access Control Lists) are applied, the cloud server becomes the judge to evaluate the access policy and make access decision. Thus, end-users may worry that the cloud server may make wrong access decision intentionally or unintentionally, and disclose their data to some unauthorized users. In order to enable end-users to control the access of their own data, some attribute-based access control schemes are proposed by leveraging attribute-based encryption. In attribute-based access control, end-users gain access policies for their data and encrypt the data under these access policies. Only the users whose attributes can satisfy the access policy are eligible to decrypt the data. Cloud computing is an alternative traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. Cloud service providers e.g. Amazon, are deliver various services to cloud users with the help of powerful data centers. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant in-vestments on their local infrastructures. It is one of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its stats in the same group or department to store and share in the cloud. By utilizing the cloud, the stats can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored _les. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data, and then upload the encrypted data.

II. ARCHITECTURE DIAGRAM



III. LITERATURE SURVEY

1. Paper Name: Multi-Owner Multi-User Privacy.
This paper focuses on the development of the system for a multi-owner multi-user (MOMU) system where data owners

require privacy guarantees before offering their private data. In such a setting each owner has different privacy needs against each user, whereas, users may seek to collaborate in order to violate owners' privacy. Using approximate differential privacy, we focus on the case where n data owners possess a real-valued private data and m data users wish to learn a linear query of this data. We consider a Gaussian mechanism, derive the constraints on the covariance matrix for the mechanism to be multi-owner multi-user private, and propose a convex semi-definite relaxation to design the covariance. Finally, we illustrate our approach to a synthetic scenario where n agents act both as data owners and data users and we evaluate the privacy and the accuracy of the resulted mechanism.

2. Paper Name: An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy.

This paper developed the system using Cipher text-policy attribute-based encryption (CP-ABE), which is a promising encryption technique that enables end-users to encrypt their data under the access policies defined over some attributes of the data consumers and allows only those data consumers whose attributes satisfy the access policies to decrypt the data. In CP-ABE, the access policy is attached to the cipher text in plaintext form, which may also leak some private information about end-users. In the Existing methods only partially hide the attribute values in the access policies, while the attribute names are still unprotected. Specifically, this technique hides the whole attribute (rather than only its values) in the access policies.

3. PaperName: Expressive, efficient, and revocable data access control for Multi-authority cloud storage.

This paper focuses on the development of the system for an expressive, efficient and Changing data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. This technique proposes a multi-authority CP-ABE scheme, and apply it as underlying techniques for designing the data access control scheme. Attribute revocation method can be achieved by both forward security and backward security. It analyses that proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

4. Paper Name: Clustering Sentence-Level Text Using a Novel Fuzzy Relational Clustering Algorithm

This paper focuses on the development of the system by a novel fuzzy clustering algorithm that operates on relational input data; i.e., data in the form of a square matrix of pair wise similarities between data objects.In this algorithm a graph representation of the data is used. It operates in an Expectation-Maximization framework in which the graph centrality of an object in the graph is interpreted as likelihood. It also include results of applying the algorithm to benchmark data sets in several other domains.

5. Paper Name: "Enabling _ne-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data."

This paper focuses on the development of the system by fine-grained multi-keyword search schemes over encrypted cloud data. Its original contributions are three-fold.Initialy, it introduces the relevance scores and preference factors upon keywords which enable the precise keyword search and personalized user experience. Second, it developed a practical and very efficient multi-keyword search scheme. This scheme can support complicated logic search the mixed “AND”, “OR” and “NO” operations of keywords. Third, it further employs the classified sub-dictionaries technique to achieve better efficiency on index building, trapdoor generating and query. Lastly, it analyzes the security of the proposed schemes in terms of confidentiality of documents, privacy protection of index and trapdoor.

6. Paper Name: Efficient privacy-preserving keyword search method for retrieving data from cloud.

This paper focuses on the development of the system with secure multi keyword ranked search method which is implemented for providing additional privacy and efficiency. It has accessible operations such as updating, deletion, insertion of words. These operations are used to get the files from cloud server with minimum retrieval time. Data owners gather up large volumes of data and store it in cloud servers for future purpose; later users make use of those data. Data owners are allowed into the cloud server only after they are authenticated successfully and are also permitted to create their own web pages. For the storage and retrieval of data from cloud server, Blowfish algorithm is generally used in encryption and decryption purpose. Sub linear search time and efficiency is increased.

7. Paper Name: Privacy Protection based Access Control Scheme in Cloud-based Services.

This paper focuses on the development of the system access control with privilege separation based on privacy protection (PS-ACS). In the PS-ACS scheme, it divides users into private

domain (PRD) and public domain (PUD) logically. In PRD, to achieve read access permission and write access permission, it adopts the Key-Aggregate Encryption (KAE) and the Improved Attribute-based Signature (IABS) respectively. In PUD, new multi-authority cipher text policy attribute-based encryption (CP-ABE) scheme is constructed with efficient decryption to avoid the issues of single point of failure and complicated key distribution. The analysis and simulation result show that this scheme is feasible and superior to protect users' privacy in cloud-based services.

8. Paper Name: Topic model for graph mining.

This paper focuses on the development of the system which uses Bernoulli distributions to model the edges between nodes in a graph. The edges in a graph contribute to latent topic discovery and improve the Correctness of the supervised and unsupervised learning of graphs. The results display that proposed GTM outperforms the latent Dirichlet allocation on classification by using the unveiled topics of these two models to represent graphs

9. Paper Name: A soft similarity measure for k-means based high dimensional document clustering.

This paper focuses on the development of the system with Feature dimensionality that has always been one of the key challenges in text mining as it increases complexity when mining documents with high dimensionality. High dimensionality introduces sparseness, noise, and boosts the computational and space complexities. Reduction in dimensionality is usually addressed by implementing either feature reduction or feature selection techniques. In this work, the problem of dimensionality reduction is addressed using singular value decomposition and the results are compared to information gain approach through retaining top-k features. High dimensional clustering is carried by using k-means algorithm with Gaussian function. The proposed dimensionality reduction and clustering approaches are compared to conventional approaches and results prove the importance of this approach.

10. Paper Name: Label Correlation Mixture Model: A Supervised Generative Approach to Multi-label Spoken Document Categorization.

This paper focuses on the development of the system of a novel probabilistic generative model, label correlation mixture model (LCMM), to depict the multiply labeled documents, which can be used for multilabel spoken document categorization as well as multilabel text categorization.. The LCMM consists of two important components: 1) a label correlation model and 2) a multilabel conditioned document model. The label correlation model formulates the generating process of labels where the dependences between the labels are taken into account. An efficient algorithm for calculating the probability of generating an arbitrary subset of labels is also proposed. The multilabel conditioned document model can be regarded as a supervised label mixture model, in which labels for a document are known. Each label is characterized by distributions over words

IV. PROPOSED SYSTEM

The Proposed System can hide the whole attribute (rather than its values) in the access policies. Data is Stored in Encrypted format (Cipher Text) and downloaded in Decrypted format (Plain Text). In this proposed System, an efficient and fine-grained big data access control scheme is used with privacy-preserving policy.

V. CONCLUSION

The access policy does not allow to leak any privacy information. It can hide the whole attribute in the access policies. All end users (Data Owner) can store their data in encrypted format with ABF, time server and also multiple keywords. All the information is stored securely and data is secured efficiently.

REFERENCES

[1] FragkiskosKoufogiannis and George J. Pappas,"Multi-Owner Multi-User Privacy", 2016.
[2] P. Mell and T. Grance, The NIST definition of cloud computing, [Recommendations of the National Institute of Standards and Technology- Special Publication 800-145], 2011.
[3] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, toward efficient and privacy-preserving computing in big data era, IEEE Network, vol. 28, no. 4, pp. 4650, 2014.
[4] K. Yang and X. Jia, Expressive, efficient, and revocable data access control for multi-authority cloud storage, IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 17351744, July 2014.
[5] H. Li, D. Liu, K. Alharbi, S. Zhang, and X. Lin, Enabling fine-grained access6. Control with ancient attribute revocation and policy updating in smart grid, KSII Transactions on Internet and Information Systems (TIIS), vol. 9, no. 4, pp. 14041423, 2015.
[6] K. Yang, Z. Liu, X. Jia, and X. S. Shen, Time-domain attribute-based access control for cloud-based video

content sharing: Cryptographic approach, IEEE Trans. on Multimedia (to appear), February 2016.

[7] Atzori, A Iera, and G Morabito. The internet of things: A survey. Computer networks, 54(15):2787–2805, 2010.

[8] C Dwork, M Naor, T Pitassi, and GN Rothblum. Differential privacy Under continual observation. In Proceedings of the 42nd ACM Symposium on Theory of computing , pages 715–724. ACM, 2010.

[9] J Le Ny and GJ Pappas. Differentially private filtering. Automatic Control, IEEE Transactions on, 2014.

[10] J Hsu, Z Huang, A Roth, and ZS Wu. Jointly private convex Programming. Arrive preprint arXiv:1411.0998 , 2014.

[11] Z Huang, S Mitra, and N Vaidya. Differentially private distributed Optimization. In Arrive preprint arXiv:1401.2596 , 2014.

[12] H Ebadi, D Sands, and G Schneider. Differential privacy: Now it's getting personal. In Proceedings of the 42nd Annual ACM SIGPLAN- SIGACT Symposium on Principles of Programming Languages , 2015.

[13] M Alaggan, S Gambs, and AM Kermarrec. Heterogeneous differential Privacy. arXiv preprint arXiv:1504.06998, 2015.

[14] F Koufogiannis and G Pappas. Diffusing private data over networks. arXiv preprint arXiv:1511.06253 , 2015