A COST-EFFECTIVE PARADIGM FOR MULTIPLE INTERMEDIATE DATASETS USING UPPER-BOUND CONSTRAINT APPROACH

[1]Rama Lakshmi Boyapati
[1]*Asst prof Department Of Computer Science Engineering ,*
Sir C R Reddy College Of Engineering, Eluru, W.G.Dist

Abstract-Cloud computing is an unique aspects of complicated security and privacy assert. In cloud providing security to the data is critical task, to overcome from this problem security principle is used to secure data, its applications and framework associated within the cloud computing automation. Without any infrastructure investment the intensive data applications generate more number of intermediate datasets, so that it saves the cost of computing. Now a day's privacy preserving of intermediate datasets is a demanding problem , so this problems may recover by analyzing multiple intermediate datasets from privacy-sensitive information. The data sets in cloud must be conserve privacy by using encryption and anonymization from the Existing approaches. Encrypted data on data sets is efficiently a difficult task, as most unencrypted data sets are running on existing systems. A proposed practical upper-bound searching algorithm is used to point out which data needs to be enciphered for preserving privacy while other datasets need not be enciphered. This approach can naturally decreases privacy-preserving cost over other approaches, which is favorable for the cloud users who employ services in a pay-at-sight.

Key words –*Cloud Computing; Data Sets; Privacy Preserving; multiple Intermediate Dataset ;Enciphered.*

I. INTRODUCTION

Cloud Computing is one of the important and useful technology compared to existing technologies, collected within a new framework hierarchy that offers improved extensibility, flexibility, business techniques, increased startup time , low administration costs, and at the last minute availability of resources. In Cloud computing storage users has more capacity to store and process the data in third force data centers. The benefactor must establish the framework secure and that their users data and applications are also protected. Cloud Computing specify to manage, construct and uses the hardware and software sources from anywhere. It offers online data storage, infrastructure and application.Security and privacy is a big challenging task in cloud computing. Data management and infrastructure managing in cloud is done by third-party, to handover sensitive information to the cloud user is always a critical job. Security structure is more only when the correct defensive executions are in the project. Fully homomorphism encryption and Searchable enciphered are used in encryption algorithm

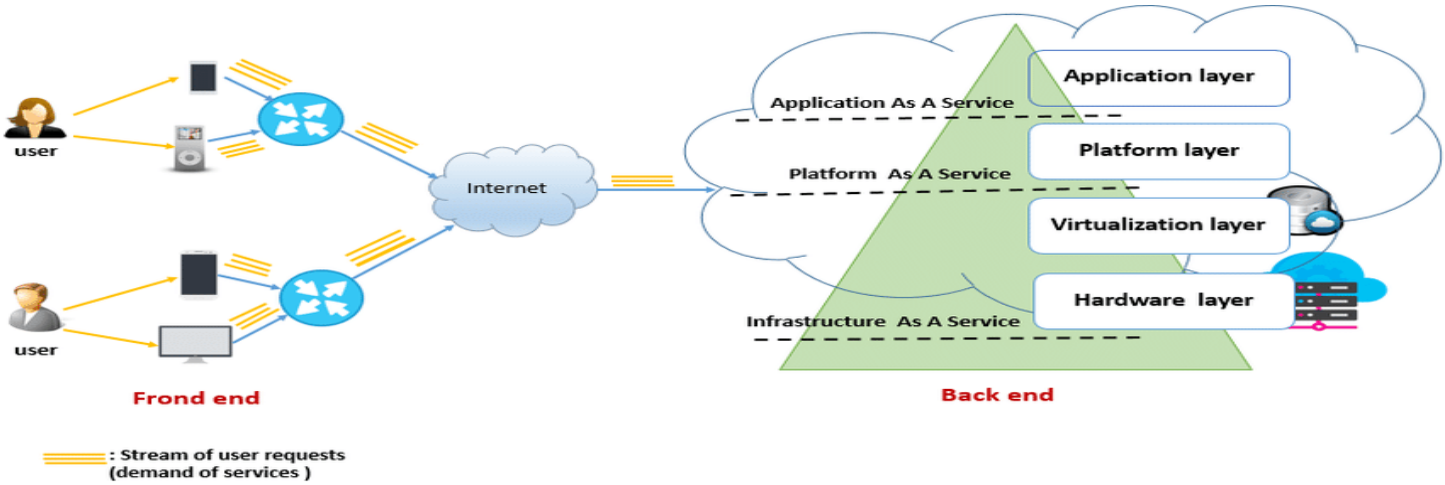

Fig.1: Cloud Computing Architecture

The users can manage or uses files in online by using Cloud computing, so that they can access them from any location through the Internet. Examples of cloud services include online file storage, social networking sites & webmail etc. Advantages of cloud computing are accessibility, almost unlimited storage, backup and recovery, cost saving and collaboration. File management in cloud computing is the most cost efficient method The data delivery in cloud computing is a technique, by using internet. There are three types of cloud computing models: software as a service, platform as a service and infrastructure as a service.

In proposed system Encrypting all intermediate data sets will lead to high overhead and low efficiency when they are again and again accessed or processed. As such, the propose system encrypts the of intermediate data sets part rather than all, to reduce privacy-preserving cost. In this paper, a tree structure is modeled from generation relationships of data sets to analyze privacy propagation of data sets. As quantifying joint privacy leakage of multiple data sets is efficiently a big task, an upper bound constraint based approach is exploit to confine privacy disclosure. This problem is decomposed into a section of sub-problems by decomposing privacy leakage constraints. Finally, the design was developed by using practical heuristic algorithm to identify the data sets that need to be encrypted.

II. RELATED WORK

Now a days, most previous research to secure privacy of the data in cloud is done by encryption of given intermediate data sets. To outsource the data, clients regularly used servers to reduce the manage the cost. Then the proposed Predicated based fine-grained access control has further been used, where client is a constrained to predefined states. Access control application and conservation strategies have been taken. Notwithstanding, the interface between the two, entrance control systems and the security assurance components has been lost. As of late, Chaudhuri have aimed to access control with protection systems[1][2]. In encryption processwell for privacy of the data approaches in existing, it iscompulsory to encrypt and decrypt datasets repeatedly in so many applications. Encryption is usually collective with other techniques to attain high data usability for cost decrease andprivacy fortification, a proposed an approach that is acombination of data fragmentation and encryption to get aprivacy protection for distributed data storage with encryptingonly some part of data sets. It provides considerable storagespace capacity to the users to deploy their applications without any modification its communications details[9]. The data owner can storevaluable intermediate data sets selectively whenprocessing original data sets in data intensiveapplications, in order to curtail the overall expenses byavoiding frequent re-computation to obtain these datasets. Such scenarios are quite commonbecause data usersoften reanalyze results, conduct new analysis onintermediate data sets, or share some intermediate results with others for collaboration. Usually, intermediate datasets in cloud are penetrate and handled by multiple parties, but rarely controlled by original data set holders[10].

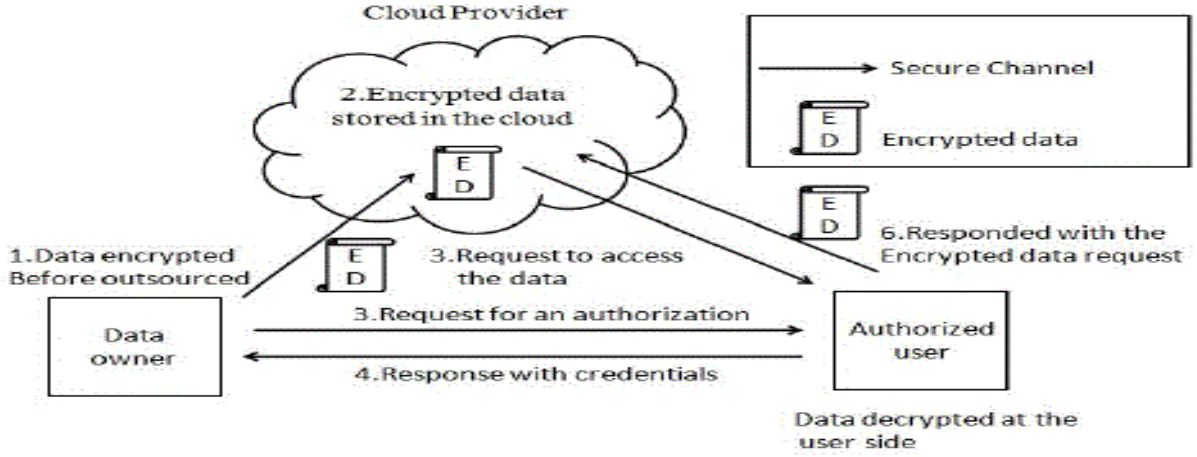

Fig.2: Architecture for privacy preserving intermediate datasets in cloud

III. PROBLEM STATEMENT

Privacy Protection Mechanism (PPM) is used to conquer and conception of relational data to anonymous and amuse privacy needs. In Relational database access control is used for privacy-preserving and to manage framework. Access Control Mechanisms(ACM) give the correct information for the authorized user. Selection predicates is one of the policy used to give privacy requirement and to satisfy the kanonymous Partitioning with Imprecision Bounds or I-diversity. For accuracy and privacy constraints we use kanonymous

Partitioning with Imprecision Bounds (KPIB). Roles in organization for the objects defines the permissions by using Role-based Access Control (RBAC). The Top Down Selection Mondrian (TDSM) algorithm construction is framed by using greedy heuristic and kd-tree model and Query workload-based anonymization is done.

Disadvantages of existing system-

A. Ineffective cost for providing privacy to large intermediate data sets.

B. The time exhausting is important for encrypting the part of intermediate datasets

C. Encrypted data sets is an efficient and big task, as most other applications only run on unencrypted data sets.

IV. UPPER-BOUND CONSTRAINT IN HEURISTIC ALGORITHM

Privacy-preserving for multiple datasets is a big problem and generalization technique can be used to solve the attacks on one single datasets.The knapsack problem:

A. Stages = items, states = how much weight capacity to use at this and all preceding stages, i.e. for this an all preceding items (0,1,2,3,4,5).

B. Cost of initial state, Ignore the integrality constraint of an IP.

C. Recursive relation:

$$f_i(y_i) = max_{k_i \le \left\lfloor \frac{y_i}{w_i} \right\rfloor} \{u_i k_i + f_{i+1}(y_i - w_i k_i)\}$$

Y be an extended basic feasible solution that satisfies the upper-bound maximal j = 0 and isαconditions. For a non-basic variable xj = 0, (2) is satisfied automatically. Set y≤j = 0, cj α 0 and ≤also satisfied. With j c T j, which is dual feasible. For a non-basicαj + ·A j = .j c Then is also satisfied byαvariable xj = uj, is satisfied automatically. Take 0, a condition induced from satisfying the≥j = j c αconstruction; and the dual variable upper-bound maximal conditions. For a basic variable taking xj such that 0 < xj < uj, j c = cj – y T x = 0, then (3) is satisfied·j = 0 satisfies. If bi - Aiαj. = 0. Setting ·A x·automatically; else, for bi - Ai > 0, the dual variable yi = 0 is guaranteed by the complementary slackness condition of the Simplex method. Thus, we have successfully Tαconstructed a dual feasible solution (y,) T that together with x satisfies the complementary slackness condition. This shows that x is primal optimal.

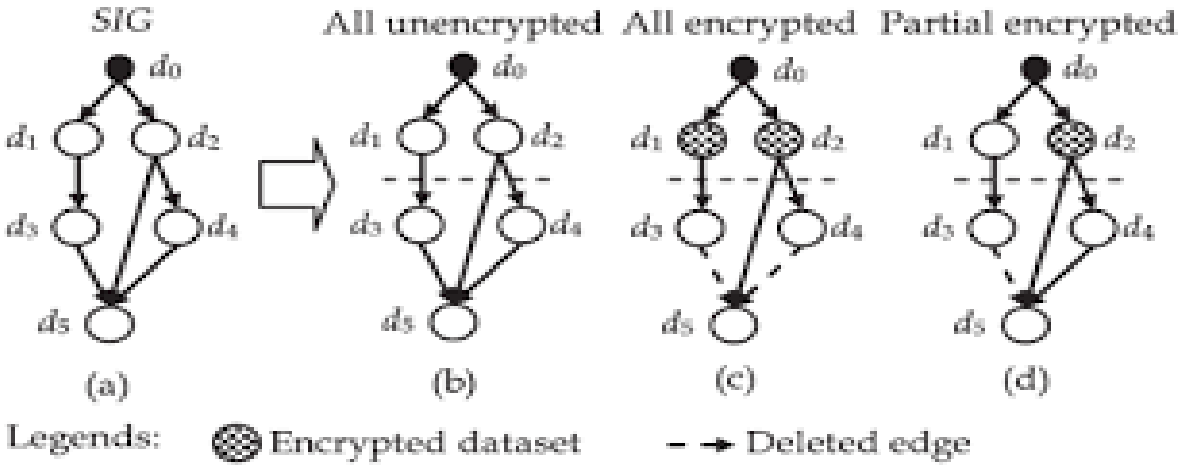

Fig.3: Unencrypted, encrypted and partially encrypted data sets

Privacy quantification is defined by single data sets. To fix the necessary subset of intermediate datasets i propose an upper-bound constraint based approach that needs to be encrypted for minimizing privacy-preserving cost. The privacy leakage upper-bound constraint is divided into number of layers.

V. EXPERIMENTAL EVALUATION

The system is developed in JAVA/J2EE and MYSQL is used as back end database.Andnetbeans 8.0 is used as Integrated development environment (IDE) In this the experimental evaluation is done by using patient datasets. The experimental results are shown by using two access control models i.e., privacy access control model and multiple datasets access

control. In Home page, it shows all the operations in the project i.e., Health service provider, login page, cloud storage. In patient original data up loader form all the data about patients will be uploaded. After uploading the patient details, we can View all patients details .Original data from privacy preserving option and in this privacy preserving it consist of 5layers.This 5layers are used for privacy preserving of datasets. Security layer1 details will be shown from either security layer 1 or from PP original data and this layer1 consists of layer2 in it. Details of layer2 can get from layer1 and it continues with layer3,this will be continued till layer 5.

Registration form for different users. Like Government, Pharmaceutical Company, research centre . Login page to search patients for government users. Searching patient details with their age wise through government users. Login page to search patients for pharmaceutical company users. Searching patient details with their disease through research centre. Login page to search patients for Adversary users. In welcome page it consists of view health details option,from that it shows health dataset. In welcome page it consists of view profile details option, from that it shows profile of at particular person. And to take permission from the cloud we should register the Cloud Registration form.

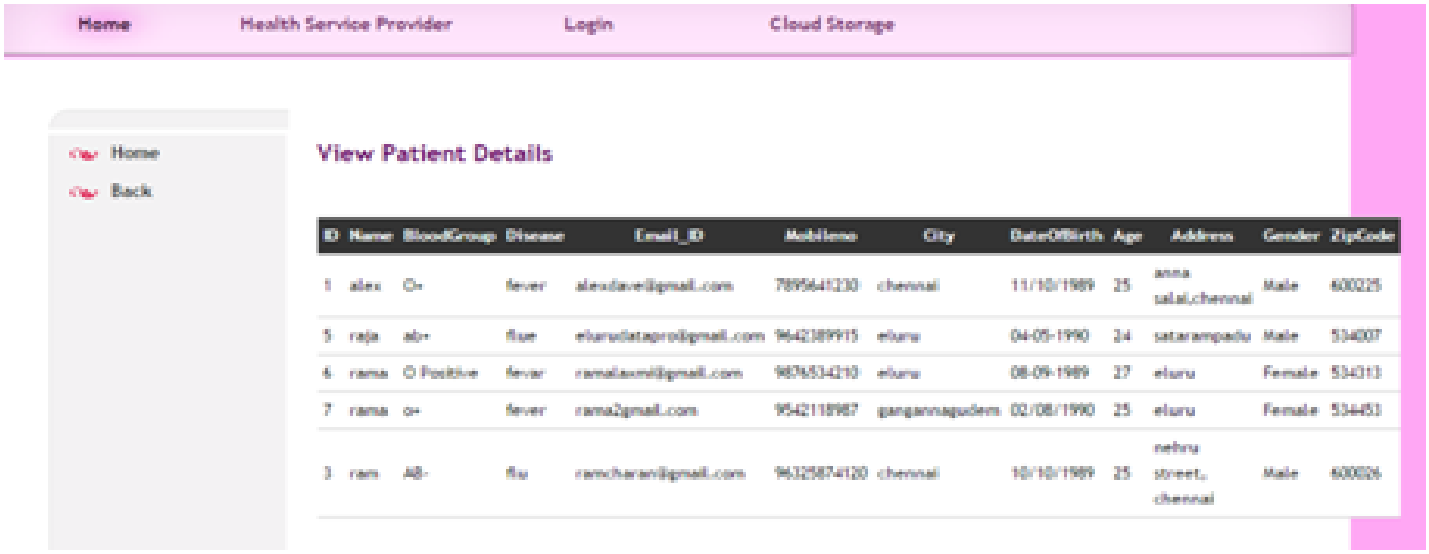

Fig.4: Patients Details

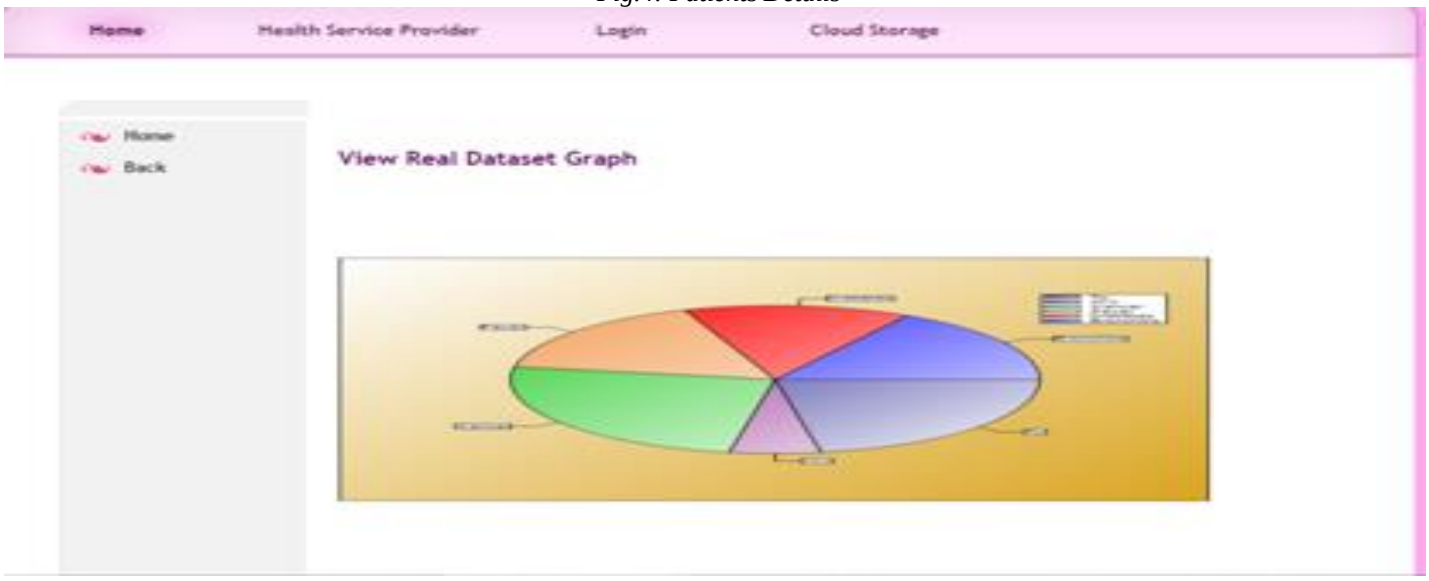

Fig.5: Data Set Graph.

VI. CONCLUSION

In this paper, the proposed system proposes the technique that can show where data need to be enciphered for privacy and other data should not be enciphered. Leakage problem is also solved by admitting the problem of saving cost to store data . Specific anonymization is used to propose the applications. Experimental results on real world datasets have determine the price of storing data secure in cloud can be minimized automatically with the algorithm previous research where all datasets are encrypted.

REFERENCES

[1] Xuyun Zhang, Chang Liu, Surya Nepal, Suraj Pandey, and Jinjun Chen, Member , "A Privacy Leakage Upper Bound Constraint-Based Approach for Cost-Effective Privacy Preserving ofIntermediate Data Sets in Cloud," IEEE Transactions On Parallel And Distributed Systems, VOL. 24, NO. 6, (2013 JUNE).

[2] Ramalakshmi B and Y.Leela Sandhya Rani (2015) A Privacy Preserving Cost-Effective Heuristic For Multiple Intermediate Datasets In Cloud",IJMCA, Vol 3, Issue 5(2015 JUNE).

[3] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic ," Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility"Elsevier Volume 25, Issue 6(June 2009).

[4] S.Y. Ko, I. Hoque, B. Cho and I. Gupta, "Making Cloud Intermediate Data Fault-Tolerant," Proc. 1st ACM Symp. Cloud Computing (SoCC'10), pp. 181-192, 2010.

[5] N. Cao, C. Wang, M. Li, K. Ren and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. 31st Annual IEEE Int'l Conf. Computer Communications (INFOCOM'11), pp. 829-837, 2011.

[6] M. Li, S. Yu, N. Cao and W. Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS'11), pp. 383-392, 2011.

[7] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Annual ACM Symp. Theory of Computing (STOC'09), pp. 169-178, 2009.

[8] B.C.M. Fung, K. Wang, R. Chen and P.S. Yu, "Privacy-Preserving Data Publishing: A Survey of Recent Developments," ACM Comput. Surv., vol. 42, no. 4, pp. 1-53, 2010.

[9] X. Zhang, C. Liu, J. Chen and W. Dou, "An Upper-Bound Control Approach for Cost-Effective Privacy Protection of Intermediate Dataset Storage in Cloud," Proc. 9th IEEE Int'l Conf. Dependable, Autonomic and Secure Computing (DASC'11), pp. 518-525, 2011.

[10] K.P.N. Puttaswamy, C. Kruegel, and B.Y. Zhao" Toward Data Confidentiality in Storage-Intensive Cloud Applications", 2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing.