RESEARCH ARTICLE OPEN ACCESS

AIDA Technique for Privacy Protection in Cloud

Kavita Manekar , Prof. A.Bhattacharya, Prof. S.D.Kamble

(Computer Science Department, G. H. Raisoni Institute of Engineering & Technology for Women
Index Terms— Cloud computing, Data sharing, Privacy Preserving. Nagpur, India)
kjmanekar@gmail.com

(Lecturer, Dept. of Computer science & Engineering , G. H. Raisoni College Institute of Engineering &Technology for Women Nagpur, India) antara.bhattacharya@raisoni.net
(Professor, Dept. of Computer science & Engineering, Yeshwantrao Chavan College of Engineering Nagpur, India)

ABSTRACT
Cloud is a relatively new concept and emerging technology. The information assurance, data protection, network security and privacy concerns have yet to be fully resolved. Cloud is offering different services to its users. Data sharing between two organizations is common in many application areas. Current data sharing and integration among various organizations require a central and trusted authority to collect data from all data sources and then integrate the collected data. In today's trend, there is need of data sharing while preserving privacy in cloud. With cloud computing, it is necessary for data to be not only stored in the cloud, but also shared across multiple users. For this purpose many different data sharing techniques are developed in cloud environment.

I. INTRODUCTION

Clouds are the hottest issue in the field of IT from a years now. Introduction of cloud computing has made a revolutionary change in the field of IT. Cloud computing is a most recent area which offers a different model for IT. Cloud computing is emerging technology which consists of existing techniques combined with new technology paradigms. In this technology, we shared different resources like software's, and hardware's also information is provided to its users and other peoples on internet whenever demanded.

Today's world relies on cloud computing to store different data such as their public as well as some personal information which is needed by the user itself or some other persons. Cloud service is any service offered to its users by cloud computing. As cloud computing comes in service there are some drawbacks such as privacy of user's data, security of user data is very important aspects. Cloud computing has been demanded on different shared computing resources. With the continuous development of cloud computing technology, its appliance is more and more widely. Now a days, cloud computing is oftener used with different synonymous like grid, cluster , distributed, autonomic computing.

Privacy is an important issue in cloud computing, whenever user wants to make use of data that involve individual sensitive information. With the rapid development of internet technology, privacy preserving data publication has become one of the most important research topics and become a serious concern in publication of personal data in recent years. However, for data owners who are becoming increasingly concerned about their privacy of the data which contains some personal information about individuals.

II. PROPOSED METHODOLOGY

This work deals with efficient algorithms for assigning identifiers (IDs) to the nodes of a network in such a way that the IDs are anonymous using a distributed computation with no central authority. Given nodes, this assignment has essentially a permutation of the integers with each ID being known only to the node to which it is assigned. Our main algorithm has been based on a method for anonymously sharing simple data and results in methods for efficient sharing of complex data. The IDs are needed in networks for security or for administrative tasks requiring reliability, such as configuration and monitoring of individual nodes. IDs is uniquely generated and which is used for sharing data among nodes. An application where IDs need to be anonymous is grid computing where IDs are anonymous to another, so that no one can access his/her personal data. To distinguish anonymous ID assignment from anonymous communication, consider a situation where number of parties wish to display their data collectively, but anonymously, in slots on a third party site. The ID has been used to assign the slots to users, while anonymous communication can allow the parties to conceal their identities from the third party.

Our network is not anonymous and the participants are identifiable in that they are known to and can be addressed by the others. For anonymous

communication , methods for assigning and using sets of pseudonyms, have been developed in networks. The methods developed in these works generally require a trusted administrator, and their end products generally differ from ours in form and/or in statistical

properties. To be precise, with nodes the algorithms of distribute a computation among the nodes generating a permutation of chosen with a uniform probability of from the set of all permutations of where will know only. The algorithms are more complex and utilize cryptographic methods as players must, in general, be able to proved that they held the winning hand. Throughout this technique, we assume that the participants are, also known as passive and execute their required protocols faithfully. A permutation can also be created using an anonymous routing protocol.. The sharing algorithm will be used at each iteration of the algorithm for anonymous ID assignment (AIDA). This AIDA algorithm can require a variable and unbounded number of iterations. Finitely-bounded algorithms for AIDA will reduce the number of expected rounds.

Given nodes n1…….n_n , use distributed computation (without central authority) to find
an anonymous indexing permutation: s (1…..N) ⟶ (1…..N)

1) Set the number of assigned nodes A=0 .
2) Each unassigned node chooses a random number in the range 1 to N. A node assigned in a previous round chooses r_i=0 .
3) The random numbers are shared anonymously. One method for doing this was given. Denote the shared values by q_1……..q_N.
4) Let q_1……..q_k denote a revised list of shared values with
duplicated and zero values entirely removed where is the number of unique random values. The nodes which drown unique random numbers then determine their index
from the position of their random number in the revised list as it would appear after being sorted:

$s_i = A = Card(q_j : q_j <= r_i)$

5) Update the number of nodes assigned: A= A + k .

The above proposed method having many different advantages such as No brute force attacks , more secure and limited time period to access data.

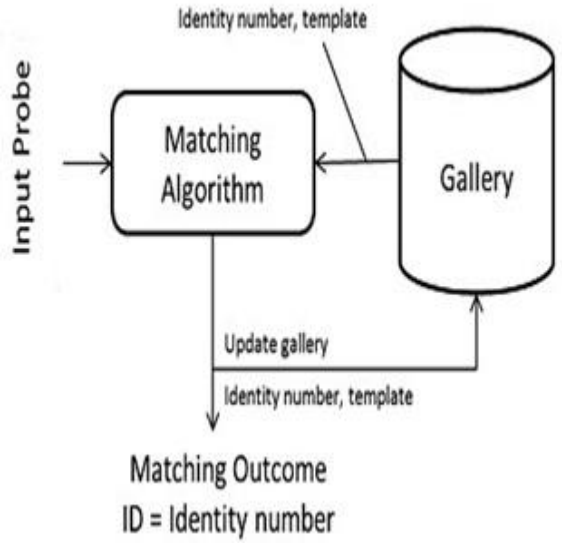
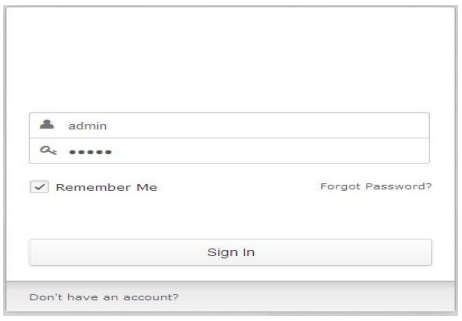
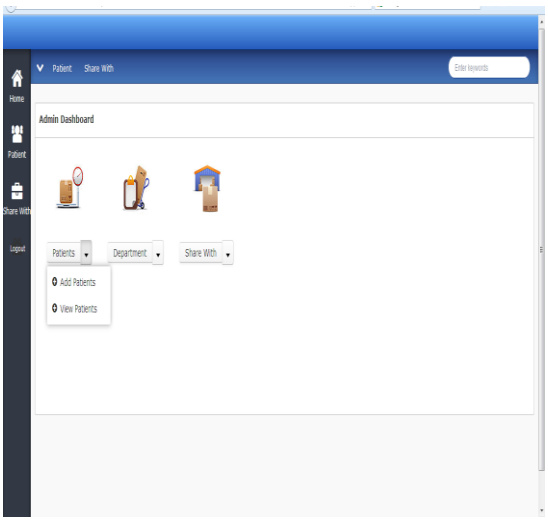


Fig: System Architecture

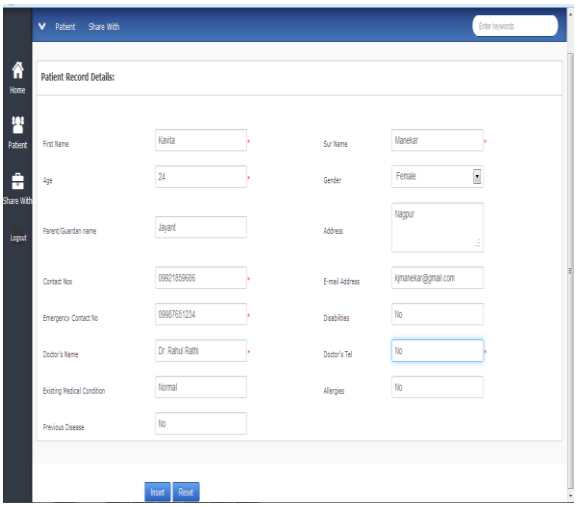
III. Result and Future Work



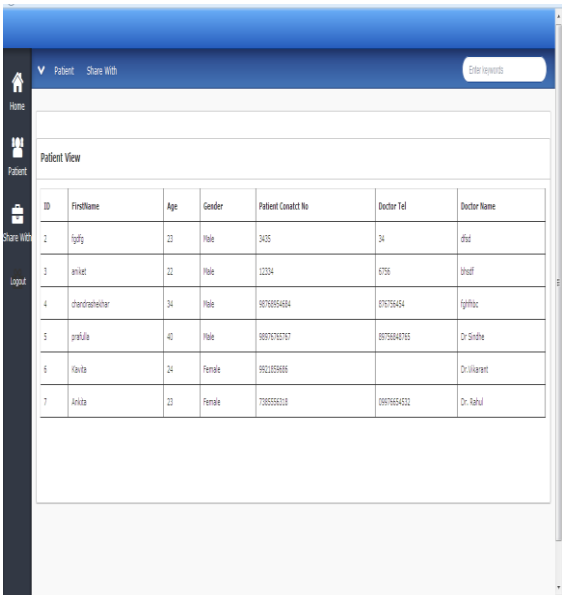
Admin Login Page



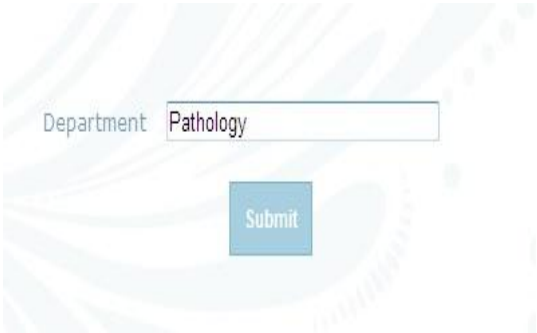
Home Screen



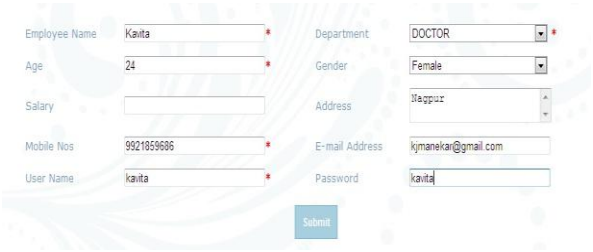
Patient Registration



Registered Patients



Add Department



User Creation

Sharing Database

In above snapshots, first admin login then patients registration should be done by filling patient registration form. After that we can view patients data in database. After creating a database, we can create user creation to patients database with different departments. Once user creation is done after that online token generation could be done by using algorithm in future.

IV. CONCLUSION

The identification of security challenges and mitigation techniques in Cloud Computing is challenged by considering the large number of services. There are many applications that require dynamic unique IDs for network nodes. Such IDs can be used as part of schemes for sharing/dividing communications bandwidth, data storage, and other resources anonymously and without conflict. The working reported in this paper explores the connection between sharing secrets in an anonymous manner, distributed secure multiparty computation and anonymous ID assignment. In the process of identification from the research methods AIDA and Survey, we will found that satisfactorily number of challenges and mitigation techniques in current and future Cloud Computing.

REFERENCES

[1] Debasish Jana , Amritava Chaudhuri and Bijan Bihari Bhaumik "Privacy Protection In Anonymous Computational Grid Services" 2012 IEEE International Conference on Computing

[2] Maria E. Skarkala, Manolis Maragoudakis Hannu Toivonen and Pirjo Moen "Privacy Preservation by *k*-Anonymization of Weighted

Social Networks"2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining

[3] Benjamin C.M. Fung, Ke Wang, and Philip S. Yu, Fellow, IEEE "Anonymizing Classification Data for Privacy Preservation" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 19, NO. 5, MAY 2007

[4] Savita Lohiya Lata Ragha "Privacy Preserving in Data Mining Using Hybrid Approach" 2012 Fourth International Conference on Computational Intelligence and Communication Networks

[5] Boyang Wang ,Baochun Li and Hui Li "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" 2012 IEEE Fifth International Conference on Cloud Computing

[6] Mingxuan Yuan, Lei Chen, Member, IEEE, Philip S. Yu, Fellow, IEEE, and Ting Yu "Protecting Sensitive Labels in Social Network Data Anonymization" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 3, MARCH 2013

[7] Yi Lu, *Member, IEEE*, Weichao Wang, *Member, IEEE*, Bharat Bhargava, *Fellow, IEEE*, and Dongyan Xu, *Member, IEEE "*Trust-Based Privacy Preservation for Peer-to-Peer Data Sharing*"* IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 36, NO. 3, MAY 2006

[8] Stephen S. Yau, Fellow, IEEE, and Yin Yin "A Privacy Preserving Repository for Data Integration across Data Sharing Services" IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 1, NO. 3, JULY-SEPTEMBER 2008

[9] Wang Yan, Le Jiajin, Huang Dongmei "A Method for Privacy Preserving Mining of Association Rules based on Web Usage Mining" 2010 International Conference on Web Information Systems and Mining

[10] Philip J. Riesch, Xiaojiang Du "Audit Based Privacy Preservation for the OpenID Authentication Protocol" 2012 IEEE

[11] Anita A. Parmar, Udai Pratap Rao, "Blocking Based approach for Classification Rule Hiding to Preserve the Privacy in Database", International Symposium on Computer Science and Society (ISCCS) , pp.323-326, 2011

[12] Savita Lohiya, Lata Ragha, "Privacy Preserving in Data Mining Using Hybrid Approach" 2012 Fourth International Conference on Computational Intelligence and Communication Networks