International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 10 153 – 156

# A Novel Architecture for Privacy Preserving Using obfuscated Attribute In e-Health Cloud

[1]Patel Switi, [2]Jayesh Mevada, [2] Krunal Suthar
[1]M.Tech Student, [2]Assistant Professor, [3]Assistant Professor
[2]Department of Computer Engineering, MEC , Basna , India
[2]Department of Computer Engineering, SPCE , Visnagar , India

**ABSTRACT**: Cloud computing now a days provides numerous number of benefits to their users. As the Cloud infrastructure is not directly under control of user its seems to be difficult for user to have a better security. Other side as the number of user grow even it become more difficult to manage a data such a way that user needs for any data are satisfied efficiently. There are lots of chances to misuse the data of user. So, here Cloud providers need to balance this two fundamental of Privacy handling and efficient analysis of data together is become very important In this research we aim is to provide the solution of both of this issue using a novel techniques. When we talk about the health records of patient or medical firm and available on remote machine issue of privacy of record provided by the anonymization fundamental. Here we provided a technique T- Closeness to achieve this goal. We also aim is to provide the security of stored data using obfuscation mechanism. Some time full obfuscation of file consume more time so here we provided scheme of attribute based obfuscation which lessen the burden of Cloud server by providing adequate security and also help to execute user query faster. We also aim in this research to reduce the burden of the Cloud by proposing third party based approach.So, together we tried to achieve better throughput securely by increase the trust of user toward Cloud.

***KEYWORDS***: Cloud Computing, Access Control ,E- Health, Privacy Preserving, Attribute Based Encryption, Obfuscation, Anonymization, Attribute Based Obfuscation.

*****

## I. INTRODUCTION

Security is one of the most important factors that everyone thinks before uploading data's in the cloud. That's way Required Security in health records of patient in medical firm. Fast and Secure data stored and access using obfuscation. Attribute Based obfuscated used for Save time and reduce cost for retrieve Information on cloud by maintaining privacy. Efficient Technique in Anonymization used for Privacy Preserving using Enhance Performance of existing solution. Group based and Agent Based Accessing facility helps user to provides better outcome, fast Access and reduce load in cloud.

## II. RELATED WORK

Authors of [1] A Cloud-Based E-Health Architecture for Privacy Preserving Data Integration, Building an anonymized medical database from multiple sources. Proposed, Architecture of a secure and scalable Privacy preserving in E-health cloud system. Algorithm that allows building a database with patient's data for the research purposes.In this proposed solution defines how to achieve data integration in a heterogeneous network of many clinical institutions, while preserving data utility and patients' privacy. In future work, Agent based coordination model used For research purposes.
Authors of [2] Cloud – Assisted Mobile-Access of Health Data With Privacy And Auditability, To build privacy into mobile health systems with the help private cloud. Provided a solution for privacy-preserving data storage by integrating a PRF (pseudorandom function) based key management for unlink ability. A search and access pattern hiding scheme based on redundancy. Secure indexing method for privacy-preserving keyword search.Investigated techniques that provide access control (in both normal and emergency cases).Auditability of the authorized parties to prevent misbehavior, by combining ABE-controlled threshold signing with role-based encryption.
Authors of [3] Privacy Preserving System Using Attribute Based Encryption for E-Health Cloud , Privacy preserving and secure sharing patient personal health records in cloud computing.Different techniques based on the attribute- base encryption have been proposed to secure the cloud storage and controlled sharing of patient's health data in cloud computing.Used attribute- base encryption technique to encrypt the personal health records data , so that patient can allow access as the private users, but not accessible by the public users. Authors of [4] Data Obfuscation: Anonymity and Desensitization of Usable Data Sets, Basic fundamental of Obfuscation. Data obfuscation properties: Reversibility, specification, shift. Experiments :Personalization and encryption methods. Data obfuscation examples :Medical records. Billing transaction.Military information.

 ISSN: 2321-8169
153 – 156

| Individual Criteria → Providers ↓ | e-Health Cloud measures | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Cloud Computing | Access Control | E- Health | Privacy Preserving | Attribute Based Encryption | Obfuscation | Anonymization | Attribute Based Obfuscation |
| [1] | √ | √ | √ | √ | × | × | × | × |
| [2] | √ | √ | √ | √ | × | × | × | × |
| [3] | √ | × | √ | √ | √ | × | × | × |
| [4] | √ | √ | × | √ | × | √ | × | × |
| [5] | √ | √ | × | × | × | √ | × | √ |
| [6] | √ | √ | √ | √ | × | × | √ | × |
| [7] | √ | √ | × | √ | √ | × | √ | × |

Table-1: Comparative Study

Authors of [5] Obfuscated Databases and Group Privacy, Introduced a new concept of database privacy, based on permitted queries rather than secrecy of individual records, and realized it using provably secure obfuscation techniques. Investigating the connection between obfuscation and database privacy. define group privacy in terms of a particular ideal functionality, but there may be Proofs in this paper are carried out in the random oracle model. Whether privacy-via-obfuscation can be achieved in the plain model is another research challenge.

Authors of [6] E-Health Care Solutions Using Anonymization , Security is one most important factor that everyone thinks before uploading data's in the cloud. A combination of anonymization and encryption. Anonymization s done using l-diversity techniques, which add more security for present data.Then whole data set is encrypted using DES technique. Then private data is double encrypted. The anonymized data is not accessible to all. Only few users closely related the data can access this private data. Proposed method provides secured health data access.

Authors of [7] provides Privacy Preserving of Data Using K-Anonymisation And T-Closeness , Different techniques such as 1) k-anonymity2) L-diversity 3) T – closeness Are used to preserve privacy of sensitive data.We have show that l-diversity has a number of limitation than proposed another privacy model called t- closeness Take more rating to analyses the data

## III. COMPARISON OF VARIOUS RESEARCH SCHEMES

The table below shows a short comparison about the various schemes proposed by a researcher by taking different parameters. The table gives the description about the basic technique used with the benefits that researcher gets as well as the limitations found in schemes.

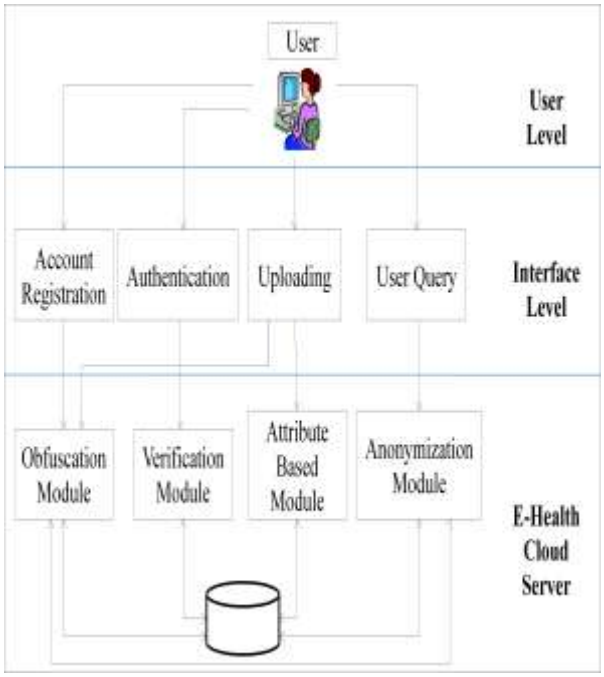
## IV. PROPOSED WORK

**Overview :** Related work A Cloud Based e-Health for Privacy Preserving security Solution.E-health Care Solutions Anonymization in efficient Technique used this

 ISSN: 2321-8169
153 – 156

proposed privacy model called T- closeness for Privacy Preserving. System in secure and fast Stored and Access Data Using Attribute Based obfuscated used. Trusted third party (agent based) base Privacy Preserving.

**Proposed Methodology:**




Here different task is carried out by the user the first one is to register himself on the cloud premises using the Registration interface. The Cloud server stores the information by obfuscated it in the database. In the next part user need to authenticate himself to access all the services of Cloud. For this purpose its send its login credentials to Cloud which handle by the authentication module which will verify the user.

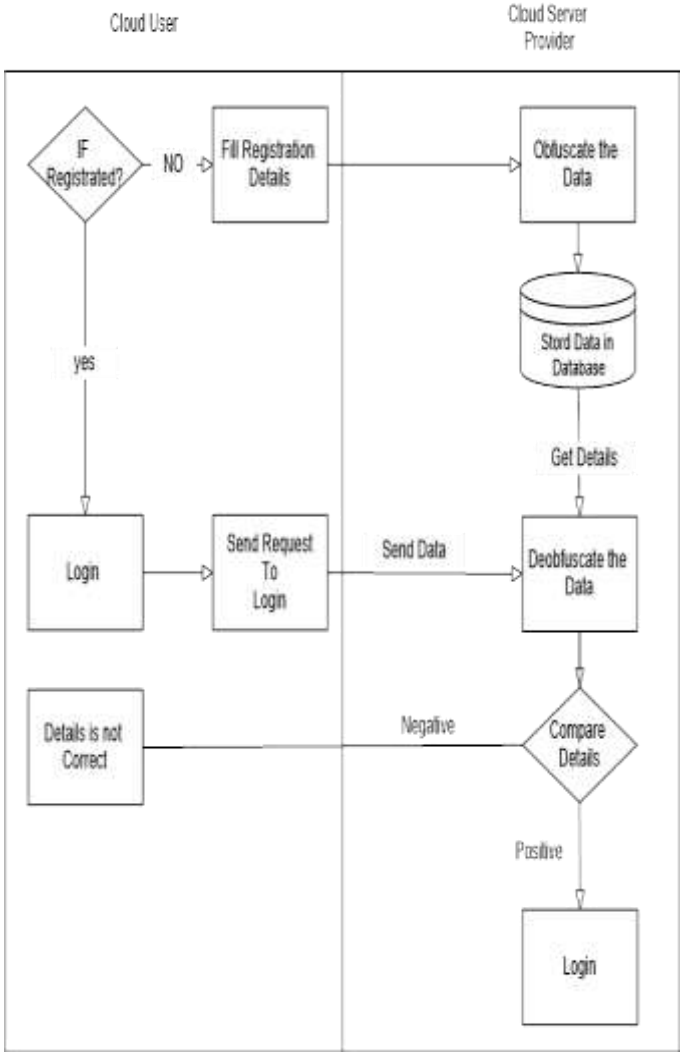
When a user have data for uploading purpose he send the details using Interface provided by the Cloud which manage by uploading handle module at server and the Cloud server by taking help together with attribute based obfuscation module store this uploaded details in database for further use.

When in future user wants to fetch required information it send a query to Cloud which handle by the Anonimization module which use T-Closeness method and find the relative information for the user and send it back to Client.

**Algorithm -1**

Step 1: User send registration information on cloud.
Step 2: If filled details is proper then server store into database and go to Next step otherwise go
To step 8
Step 3: User send login details on cloud
Step 4: Server Deobfuscate the data in their database and then compare user login data and
Database data.
Step 5: If comparison is negative then go to next step otherwise go to step no.7
Step 6: Server Send the negative acknowledgement to user
Step 7: Send positive response with corresponding page to the user.
Step 8: Fill registration details again and send back to Cloud server.

**Flow chart - 1:**

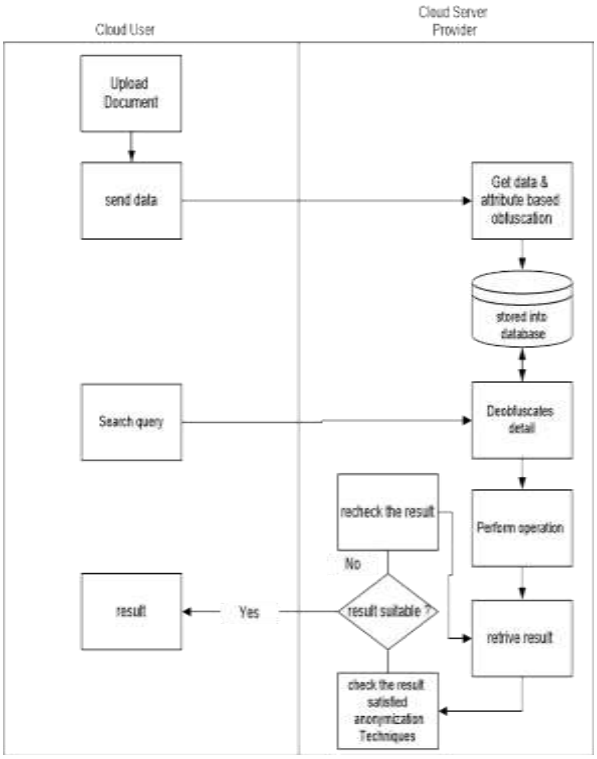



**Algorithm -2**

Step 1: User is uploading File Information.
Step 2: Server get the data and perform attribute based obfuscation and store into database.
Step 3: User send Search Query on to Server.
Step 4: Server deobfuscates the data in database and performs searching operation on data.
Step 5: Retrieve the important details from result.
Step 6: Server check is the user identity hidden in the result or not?

Step 7: If Result is Suitable then Server send the Result to User otherwise go to next step.
Step 8: If result not suitable or user identity is not completely hidden Server recheck the result and repeat the process from step no 6 to 8 before sending result to User.

**Flow chart - 2:**




## V. CONCLUSION

Flexible, On-Demand and Low-Cost, Personal health information Provides using E-health Cloud. Secure authorization mechanism provided using proper anonymization technique (T-Closeness). Provides Group based searching for faster execution of proposed scheme. Database details are secure on Cloud because of Obfuscated data. Privacy Preserving Health Records in Cloud Computing using Attribute based Obfuscation. Fast Data Access and Reduce load on server using Agent based coordination System provides higher performance with low cost on cloud environment.

## REFERENCES

[1] Alevtina Dubovitskaya , Visara Urovi1 , Matteo Vasirani , Karl Aberer, and Michael I. Schumacher ‘‘A Cloud-Based eHealth Architecture for Privacy Preserving Data Integration” in IFIP International Federation for Information Processing 2015 H. Federrath and D. Gollmann (Eds.): SEC 2015, IFIP AICT 455, pp. 585–598, 2015.

[2] Yue Tong, Jinyuan Sun, Sherman S. M. Chow, and Pan Li, Member, IEEE ‘‘Cloud-Assisted Mobile-Access of Health Data with Privacy and Auditability” in IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 2, March 2014.

[3] Kushal P. Kulkarni1, Arati M.Dixit1, “Privacy Preserving System Using Attribute Based Encryption for e-Health Cloud” International Journal of Science and Research (IJSR) Volume 3 Issue 12, December 2014.

[4] DAVID E. BAKKEN Washington State University , RUPA PARAMESWARAN AND DOUGLAS M. BLOUGH Georgia Institute of Technology , ANDY A. FRANZ AND TY J. PALMER Washington State University“Data Obfuscation: Anonymity and Desensitization of Usable Data Sets’’ Published By The IEEE Computer Society ,2004,Ieee Security & Privacy .

[5] Arvind Narayanan and Vitaly7 Shmatikov ‘‘Obfuscated Databases and Group Privacy” The University of Texas at Austin {arvindn,shmat}@cs.utexas.edu, CCS’05, November 7–11, 2005, Alexandria, Virginia, USA.

[6] Chaitra, Narasimha Murthy “E-Health Care Solutions Using Anonymization” International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) Vol. 4, Issue 5, May 2015.

[7] Anu Rinny Sunny “Privacy Preserving of Data Using K-Anonymisation And T-Closeness” International Journal for Research in Applied Science & Engineering (IJRASET) Volume 3, IssueIII, March 2015.

[8] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, “ℓ-Diversity: Privacy Beyond k-Anonymity” on Department of Computer Science, Cornell University.