Research Article Impact Factor: 0.621 ISSN: 2319-507X
SR Jadhao, IJPRET, 2014; Volume 2 (8): 608-615 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ANALYSIS OF ANONYMOUS TECHNIQUES USED IN SECURING PRIVACY OF DATA IN CLOUD

S. R. JADHAO[1] , KU. SAMPADA V. BHONDE[2]

1. Assistant Professor, Department of Computer Science and Engineering, Babasaheb Naik College of Engineering, Pusad.

2. M.E(2nd year), Department of Computer Science and Engineering, Babasaheb Naik College of Engineering, Pusad.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: Cloud computing is a field which is evolving and growing consistently in the field of computer. But, the security issues and threats associated with it still stay as a cumbersome. The focal point of this paper is Privacy preserving of data in cloud computing. There are different approaches for preserving privacy of data in cloud. Our main focus would be securing privacy of data in cloud by using *anonymity techniques*. In this paper algorithms are discussed for anonymous sharing of private data among N parties. Iterative technique is used so that ID numbers are used ranging from 1 to N. This assignment is anonymous in that the identities received are unknown to the other members of the group.

Keywords: Anonymization and deanonymization, cloud and distributed computing systems, multiparty computation, privacy preserving data mining, privacy protection.

PAPER-QR CODE

Corresponding Author: S. R. JADHAO

Access Online On:

www.ijpret.com

How to Cite This Article:

SR Jadhao, IJPRET, 2014; Volume 2 (8): 608-615

1. INTRODUCTION

The construction of cloud and storing data in it has tremendous benefits. The main benefit of cloud computing is centralized data, having the data all in the same place assists in forensic readiness**,** which leads to quicker, coordinated response to incidents[1]. Whenever required, the user can request and gain the access in an easy way and at low cost, irrespective of the user location. Also, cloud computing takes away the expenses spent on installing all hardware and software, by allowing users to rent the resources based on their needs. The problem of sharing privately held data individual using that data cannot be identified has been studied extensively[4].Researchers have also investigated the importance of anonymity in various applications patient's medical record[5], e-mail[7], social networking[8], electronic voting[6].

2. Analysis of the problem

Although cloud computing has many benefits to offer, there is still a degree of speculation over its security.

Cloud computing attracts considerable attention and interest from both academia and industry. However, it also has at least three challenges that must be handled before applied to our real life.

- First of all, data confidentiality should be guaranteed.
- Secondly, personal information (defined by a user's attributes) is at risk because one's identity is authenticated according to his information.
- Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers.

The privacy of the data must be preserved while disclosing it to third party or while placing it in long time storage [3].

According to Data Protection Act,1998 (DPA) 'Personal Data' can be defined as data related to living individual who can be identified from that data or from that data and other information which includes expression of opinion about the individual[2].

3. Privacy preserving methods:

There are different methods in preserving privacy of data in cloud[14].

- Anonymity-based Method
- A privacy-preserving Architecture
- Privacy-Preserved Access Control
- A Privacy Preserving Authorization System
- A Privacy Preserving Data Outsourcing.
- PccP Model for Cloud
- Dynamic Metadata Reconstruction

4. Proposed System Analysis and Design:

In this paper we have discussed about *anonymity-based method.* Our 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 N nodes, this assignment is essentially a permutation of the integers {1....N} with each ID being known only to the node to which it is assigned [13].

There are many applications which requires unique dynamic IDs for network nodes[9]. An application where IDs need to be anonymous is grid computing where one may take service without disclosing the identity of service requestor[10].

An algorithm for anonymous sharing of private data among parties is developed. This technique is used iteratively to assign these nodes ID numbers ranging from 1 to N. This assignment is anonymous in that the identities received are unknown to the other members of the group. Resistance to collusion among other members is verified in an information theoretic sense when private communication channels are used.

The assignment of serial numbers allows more complex data to be shared. The required computations are distributed without using a trusted central authority [13].

4.1 System flow

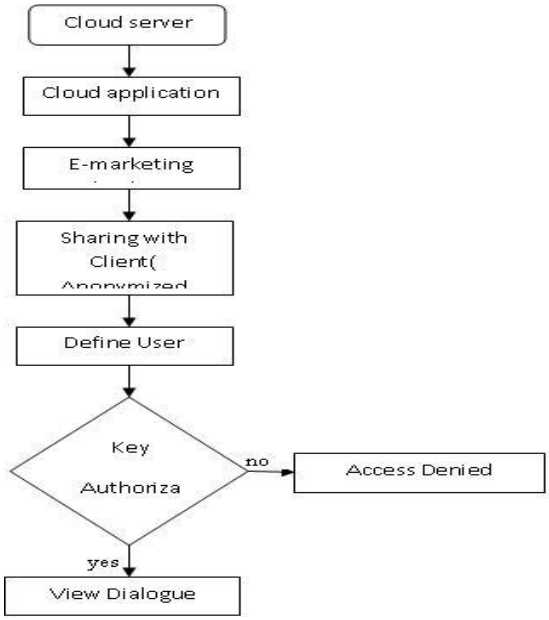

Figure 1: System Flowchart

4.2 System Architecture

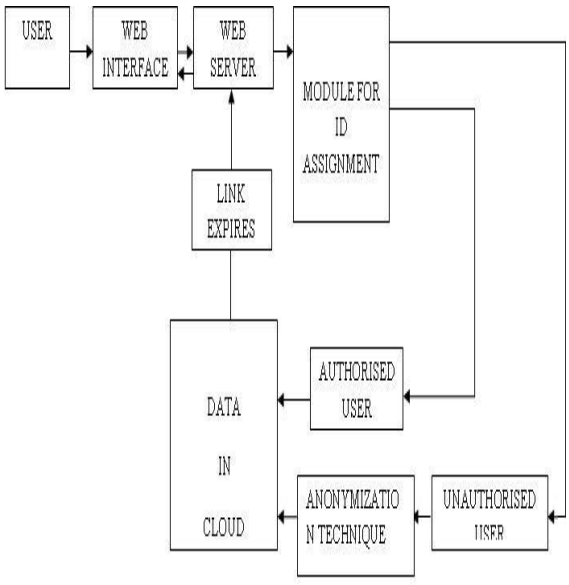

Figure 2: System Architecture

5. Algorithms:

The problem of sharing privately held data so that the individuals who are the subjects of the data cannot be identified has been researched extensively [3]. There are some algorithms are as follows like[13]:-

1. Secure sum

Given nodes $n_1, \ldots \ldots n_n$each holding an data item d_i from a finitely representable abelian group, share the values $T = \sum d_i$ among the nodes without revealing the values d_i.

1) Each node n_i, where $i = 1, \ldots . N$ chooses random values $r_{i,1}, \ldots r_{i,N}$ such that

$$r_{i,1}, \ldots r_{i,N} = d_i$$

2) Each "random" value $r_{i,j}$ is transmitted from node $n_i$to node n_j. The sum of all these random numbers $r_{i,j}$ is, of course, the desired total T.

3) Each node n_j totals all the random values received as:
$s_j = r_{1,j}+, \ldots + r_{N,j}$

4) Now each node n_i simply broadcasts s_i to all other nodes so that each node can compute:

$$T = s_1, \ldots . s_n$$

2. Anonymous Data Sharing With Power Sums

Given nodes $n_1, \ldots \ldots n_N$ each holding a data item d_i. from a finitely representable field F, make their data items public to all nodes without revealing their sources.

1) Each node n_i computes d_i^n over the field F for $n = 1, \ldots . N$. The nodes then use secure sum to share knowledge of the power sums:

$P_1 = \sum_{i=1}^{N} d_i^1$	$P_2 = \sum_{i=1}^{N} d_i^2$	$\cdots$	$P_N = \sum_{i=1}^{N} d_i^N$

2) The power sums $P_1, \ldots . P_N$ are used to generate a polynomial which has $D_1, \ldots . D_N$ as its roots using Newton's Identities as developed in [30]. Representing the Newton polynomial as:

$p(x) = c_{Nx^N} + \cdots + c_{1x} + c_0$

the values s $c_0, \ldots . c_N$ are obtained from the equations:

$$
\begin{aligned}
c_N &= -1 \\
c_{N-1} &= -\frac{1}{1}(c_N P_1) \\
c_{N-2} &= -\frac{1}{2}(c_{N-1} P_1 + c_N P_2) \\
c_{N-3} &= -\frac{1}{3}(c_{N-2} P_1 + c_{N-1} P_2 + c_N P_3) \\
c_{N-4} &= -\frac{1}{4}(c_{N-3} P_1 + c_{N-2} P_2 + c_{N-1} P_3 + c_N P_4) \ldots \\
c_{N-m} &= -\frac{1}{m} \sum_{k=1}^{m} c_{N-m+k} P_k
\end{aligned}
$$

3) The polynomial $p(x)$ is solved by each node, or by a computation distributed among the nodes, to determine the roots $d_1, \ldots . d_N$.

3. AIDS

Given nodes $n_1, \ldots \ldots n_N$, use distributed computation (without central authority) to find an anonymous indexing permutation $s: \{1, \ldots, N\} \rightarrow \{1, \ldots, N\}$

1) Set the number of assigned nodes $A = 0$

2) Each unassigned node n_i chooses a random number r_i in the range 1 to s. 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 in Section III. Denote the shared values by $q_1, \ldots \ldots q_N$

4) Let $q_1, \ldots \ldots q_N$ denote a revised list of shared values with duplicated and zero values entirely removed where k the number of unique random values is. The nodes n_i which drew 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:

$$s_i = A + \mathrm{Card}\{q_j : q_j <= r_i\}$$

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

6) If $A < N$ then return to step (2).

6. Objectives

Sharing privately held data so that the individuals who are the subjects of the data cannot be identified.

- Deal with efficient algorithms for assigning identifiers (IDs) to the nodes of a network in such a way that the IDs are anonymous.
- It is necessary that every cloud user must be guaranteed that his data is stored, processed, accessed and audited in a secured manner at any time. Attaining all these would end up in achieving the long dreamt vision of secured Cloud Computing in the nearest future.
- Our use of the Newton identities greatly decreases communication overhead. The solution of a polynomial can be avoided at some expense by using Sturm's theorem.

7. Conclusion

The proposed system would be to secure privacy of shared data by Anonymous ID Assignment, by implementing discussed algorithms. This technique effectively preserves both information utility and individual's privacy.

Privacy preserving is growing field of research. It is clear that there are many privacy preserving techniques available but still they have shortcomings. Anonymity technique gives privacy protection and usability of data. This technique will secure anonymous sharing of private data by anonymous ID assignment.

8. REFERENCE

1. Denis Reilly, Chris Wren, Tom Berry, "Cloud Computing_Pros and Cons for Computer Forensic Investigations" International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, March 2011

2. Information Commissioner's office, "Anonymization: managing data protection risk, code of practice", 2012

3. Tomas Isdal, Michael Piatek, Arvind Krishnamurthy, Thomas Anderson: "Privacy-preserving P2P data sharing with OneSwarm".

4. A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

5. A. Friedman, R. Wolff, and A. Schuster, "Providing k-anonymity in data mining," VLDB Journal, vol. 17, no. 4, pp. 789–804, Jul. 2008.

6. F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli, "Seas, a secure e-voting protocol: Design and implementation," Comput. Security, vol. 24, no. 8, pp. 642–652, Nov. 2005.

7. D. Chaum, "Untraceable electronic mail, return address and digital pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84–88, Feb. 1981.

8. Q. Xie and U. Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users," in Proc. 9th Ann. IEEE Conf. Privacy, Security and Trust, Jul. 2011, pp. 252–259.

9. J. Smith, "Distributing identity [symmetry breaking distributed access protocols]," IEEE Robot. Autom. Mag., vol. 6, no. 1, pp. 49–56, Mar.1999.

10. D. Jana, A. Chaudhuri, and B. B. Bhaumik, "Privacy and anonymity protection in computational grid services," Int. J. Comput. Sci. Applicat., vol. 6, no. 1, pp. 98–107, Jan. 2009.

11. J. Wang, T. Fukasama, S. Urabe, and T. Takata, "A collusion-resistant approach to privacy preserving distributed data mining," IEICE Trans. Inf. Syst. (Inst. Electron. Inf. Commun. Eng.), vol. E89 D, no. 11, pp. 2739–2747, 2006.

12. J. Smith, "Distributing identity [symmetry breaking distributed access protocols]," IEEE Robot. Autom. Mag., vol. 6, no. 1, pp. 49–56, Mar. 1999.

13. Larry A. Dunning, Member, IEEE, and Ray Kresman "Privacy Preserving Data Sharing With Anonymous ID Assignment", IEEE Transactions on information forensic and security, vol. 8, no. 2, February 2013

14. T. Jothi Neela1* and N. Saravanan2A. Dunning "Privacy Preserving Approaches in cloud – A Survey" International journal Of Science and Technology.