IJCAT International Journal of Computing and Technology, Volume 1, Issue 7, August 2014
ISSN : 2348 - 6090
www.IJCAT.org

An Anonymity-Based Secure and Preserving Data in Social Networks Using Cloud

[1] P. Preethi , [2] K. Narayana

[1] Post-Graduate Student,
Department of Computer Science and Engineering,
SIT, PUTTUR, India

[2] Head & Associate Professor,
Department of computer Science and Engineering,
SIT, PUTTUR, India

Abstract - Presently the mankind are progressively relying much more about a number of online storage stores to backup our data and making use of it instantly which provides an anywhere, anytime access. Every one of these services bring by using it, concerns of security and privacy weaknesses for the services given by them because the user's data are stored and maintained beyond user's premises. Our main focus could be securing privacy of information in social network by utilizing anonymity techniques. In this particular paper algorithms are discussed for anonymous sharing of private data among N parties. Iterative strategy is used to ensure that ID numbers are utilized starting from 1 to N. This assignment is anonymous for the reason that the identities received are unknown towards the other members from the group.

Keywords **- Anonymization, deanonymization cloud, distributed computing systems.**

1. Introduction

Secure and anonymous communication has many applications. Dissidents residing in totalitarian states should communicate without concern with retribution. Companies should protect their trade secrets from industrial espionage. Whistleblowers have to be capable to get in touch with the press without concern with punishment. Freedom of expression sometimes needs anonymity to survive attacks mounted against it. Anonymity is usually important. The mere information about two parties having exchanged messages might be compromising even if the content with the correspondence remained secret. However, neither party on the message exchange should be anonymous towards other party, along with the way it is in a few systems the design of cloud nor storing data within it has tremendous benefits. The advantage of cloud computing is centralized data, obtaining the data all in the same position assists in forensic readiness, that leads to quicker, coordinated respond to incidents. Whenever required, an individual can request and gain the access within the easy way and also at inexpensive, regardless of the user location. Also, cloud computing eliminates the expenses invested on installing all hardware and software, through getting users to rent the resources depending on the requirements. The issue of sharing privately owned data individual using that data cannot be identified has become studied extensively. Researchers have also investigated the significance of anonymity in a variety of applications patient's medical history, e-mail, social networking, and electronic voting.

2. Related Work

Confidentiality, integrity and availability are requirements for just about any secure communication system. No system can fulfill all three requirements in most circumstances; however the probability of the successful attack that compromises some of the three needs to be minimal. The confidentiality requirement ensures that an email's content must remain secret between its sender and its particular intended recipient. This content must consequently be protected in a way against unauthorized readers. Normally, this is done with a couple kind of encryption, but ciphering alone is insufficient:

The communicating parties must also authenticate each other to make certain what it's all about actually emanates from the proper source and reaches the proper destination. Without an authentication mechanism it is also possible

for a man in the centre to intercept what it's all about by pretending to be the recipient towards the sender and because the sender towards the recipient, rendering any encryption useless. Maintaining availability is very important. If the adversary can disable a secure way of communication, it might be capable of force the communication to some less secure channel. If you want to maintain availability, a communication system should never have any single point of failure.

The purpose of failure can Be technical, for instance reliance upon an individual server. In this case a malfunction within the server or possibly a denial of service attack against it might disable the system. It is also organizational, in which particular case an individual entity has the strength to disable the system. The prior paragraphs have listed many requirements to get a secure and anonymous communication system. These requirements are summarized from the following list:

- The system must use cryptographically strong encryption to defend the information of messages.
- The communication parties will need to have the opportunity to authenticate one another by using a cryptographically strong authentication scheme.
- The system should have a robust and secure procedure to manage and exchange encryption keys and codes.
- There should be no single point of failure within the system, whether it is organizational or technical.
- The system need to be resilient to attacks against its infrastructure that make an effort to compromise availability.
- The system will need to have the opportunity to hide the identities of communication participants from third parties.

Privacy preserving methods generally there are wide and varied methods in preserving privacy of data in cloud.

- 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

3. Proposed System Analysis and Design

In this particular paper we now take over discussed about anonymity-based method. Our work refers to efficient algorithms for assigning identifiers (IDs) towards the nodes of the network in a way how the IDs are anonymous utilizing a distributed computation without any central authority. Given N nodes, this assignment it's essentially a permutation with the integers {1....N} with each ID being known simply to the node that it can be assigned. There are various applications which require unique dynamic IDs for network nodes. An application where IDs have to be anonymous is grid computing where one could take service without disclosing the identity of service requestor. An algorithm pertaining to anonymous sharing of private data among parties is developed.

This method is needed iteratively to assign these nodes ID numbers which range from 1 to N. This assignment is anonymous for the reason that the actual identities received are unknown towards the other members with the group. Effectiveness against collusion among other members is verified within an information theoretic sense when private communication channels are utilized. The assignment of serial numbers allows more difficult data to become shared. The necessary computations are distributed without making use of a reliable central authority.

3.1 Algorithm

Algorithm (secure sum): Given nodes $n_1,....n_N$ each holding a data item di from represent able abelian group.

Share the value $T=\sum d_i$ among the nodes without revealing the values d_i.

Step 1: Each node n_i, i=1,.....,N Choose random values $r_{i1},...r_{iN}$ such that

$$r_{i1}+.....+r_{iN}=d_i$$

Step 2: Each "random" value $r_{i,j}$ is transmitted from node ni to node nj. The sum of all these random numbers r_i, desire total T.

Step 3: Each node nj totals all the random values received as

$$sj=r_1j+...+r_Nj$$

Step 4: Each node ni simply broadcasts si to all other nodes so that each node can compute.

$$T= s_1+....+S_N$$

3.2 System Architecture

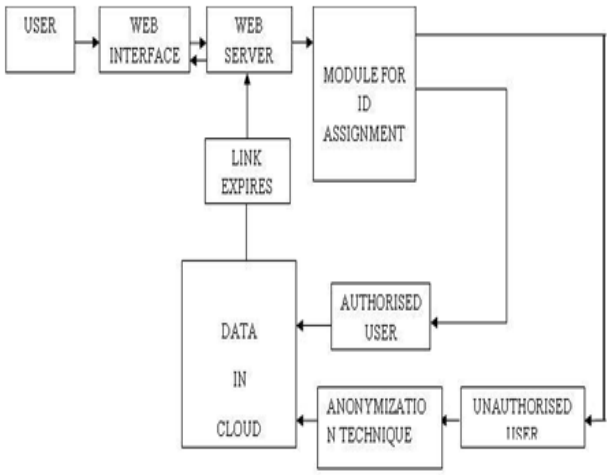

Fig 1: System Architecture

- Sharing privately owned data in order that the who are the subjects with the data cannot be identified.
- Handle efficient algorithms for assigning identifiers (IDs) towards the nodes of the network in a way which the IDs are anonymous.
- It will be important that each cloud user have to be guaranteed that his information is stored, processed, accessed and audited in a much secured manner whenever you want. Attaining every one of these would end up in achieving the long dreamt vision of secured Cloud Computing Within the nearest future.
- Our technique Newton identities greatly decrease communication overhead. The most effective Of any polynomial is usually avoided at some expense through the use of Sturm's theorem.

4. Conclusion

The actual suggested system should be to secure privacy of shared data by Anonymous ID Assignment, by implementing discussed algorithms. This system effectively preserves both information utility and individual's privacy. Privacy preserving keeps growing field of research. It can be clear that we now have much privacy preserving techniques available however they have got shortcomings. Anonymity technique gives privacy protection and usability of knowledge. This system will secure anonymous sharing of private data by anonymous ID assignment.

References

[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.

[5] Jayalatchumy, D., Ramkumar, P., & Kadhirvelu, D. 2010, November. Preserving Privacy through Data Control in a Cloud Computing Architecture Using Discretion Algorithm. In Emerging Trends in Engineering and Technology (ICETET), pp. 456-461

[6] Ruj, S., Stojmenovic, M., & Nayak, A. 2012, May. Privacy Preserving Access Control with Authentication for Securing Data in Clouds. In Cluster, Cloud and Grid Computing (CCGrid),12th IEEE/ACM International Symposium on(pp. 556-563). IEEE.

[7] Liu, Q., Wang, G., & Wu, J. 2009, August. An efficient privacy preserving keyword search scheme in cloud computing. In Computational Science and Engineering, 2009. CSE'09. International Conference on (Vol. 2, pp. 715-720). IEEE.

[8] Sayi, T. J. V. R. K., Krishna, R. S., Mukkamala, R., & Baruah, P. K. 2012. Data Outsourcing in Cloud Environments: A Privacy Preserving Approach. In Information Technology: New Generations (ITNG), 2012 Ninth International Conference on (pp. 361-366).

[9] Shah, M. A., Baker, M., Mogul, J. C., & Swaminathan, R. 2007, May. Auditing to keep online storage services honest. In Proceedings of the 11th USENIX workshop on Hot topics in operating systems (pp. 1-6). USENIX Association.

[10] Yang, K., & Jia, X. 2012. Data storage auditing service in cloud computing: challenges, methods and opportunities. World Wide Web, 15(4), 409-428.

[11] Chen, L., & Guo, G. 2011. An efficient remote data possession checking in cloud storage. International Journal of Digital Content Technology and its Applications, 5(4), 43-50.

[12] Gohel, M., & Gohil, B. 2012. A New Data Integrity Checking Protocol with Public Verifiability in Cloud Storage. Trust Management VI, 240-246.

[13] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. 2011. Enabling public auditability and data dynamics for storage security in cloud computing. Parallel and Distributed Systems, IEEE Trans. on, 22(5), 847-859.

[14] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Khan, O., Kissner, L., ... & Song, D. 2011. Remote data checking using provable data possession. ACM Transactions on Information and System Security (TISSEC), 14(1), 12.

[15] Hao, Z., Zhong, S., & Yu, N. 2011. A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability. Knowledge and Data Engineering, IEEE Transactions on, 23(9), 1432-1437.