ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

A Survey on Decentralized Access Control Strategies for Data Stored in Clouds

J.Ganeshkumar[1], N.Rajesh[2], J.Elavarasan[3], Prof.M.Sarmila[4], Prof.S.Balamurugan[5]

Department of IT, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[1,2,3,4,5]

ABSTRACT: This paper details about various methods prevailing in literature of anonymous authentication mechanisms for data stored in clouds. It is a Decentralized access of system in which every system have the access control of data . The Cloud which is a Secured storage area where the anonymous authentication is used, so that only the permitted users can be accessed. Decrypting of data can be viewed only by a valid users and can also stored information only by Valid users. This Scheme prevents Replay attack which mean Eaves Dropping can be avoided, Support Creation of data inside storage, Modifying the data by unknown users , and Reading data stored in Cloud. User can revocate the data only by addressing through the cloud. The authentication and accessing the Cloud is Robust, Hence Overall Communication Storage are been developed by comparing to the Centralized approaches. This paper would promote a lot of research in the area of Anonymous Authentication.

KEYWORDS: Data Anonymization, Matching Dependencies(MDs), Object, Similarity Constraints, Information Mining.

I. INTRODUCTION

Accountability of cloud which means the amount of storage, which is been a Challenging task by an Technical issue and Law Enforcement. The Transaction involved in the Cloud by the user should maintain the log of transaction to know how much data are been Transacted and to address in the trust cloud and for the Secure provenance For example Alice the law student wants to send the report of malpractice by an University X to all the Professors of University X, Research Chairs and students belonging to the law department in all universities in the provenance , She needs to send the data in an anonymous and she stores the evidence of malpractice in Cloud. Accessing of this data should be permitted only by the authorized user and the problems which include in this like access control , Authentication, Privacy Protection which are solved is been explained through this paper

Access control of data which involves a secured data retrieval by the user, so that the accessing data like sensible data should be much care taken. There are three types of access control such as User Based Access Control(UBAC), Role Based Access Control(RBAC), and Attribute Based Access Control(ABAC). The UBAC which is a User Based Access Control can be accessed only through the users so that it is not feasible to use in Cloud. The RBAC which is a Role Based Access Control can be accessed only based roles for example the accessing of data can be permitted only for the Seniors and the Faculty membersnot for the Juniors .The ABAC which is a Attribute Based Access Control where only with the accessing of valid set of attribute only is used for access data for example the certain record can be accessed only by the faculty member having an Experience of 10 years or the Senior secretaries with more than 8 years. All these three access control are used in the Cloud by a Cryptographic primitive is known as Attribute Based Encryption(ABE). For example the patients staff nure in the hospital can be stored as data in Cloud, these data can be accessed through the ABE by a some set of conditions to identify the attribute and keys. Using this attribute and keys the user can identify by matching and can retrieve the information.

II. TRUSTCLOUD: A FRAMEWORK FOR ACCOUNTABILITY AND TRUST IN CLOUD COMPUTING

R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M.Kirchberg, Q. Liang, and B.S. Lee,(2013) proposed Potential customer has a lack of trust in the Cloud, where the security and the privacy is been researched to developed in the cloud ,but still there is focuson the accountability and the auditability. The sheer amount of data revealed from the virtualization and the data distribution is been researched in the cloud accountability. As it has the responsible of customers concern of server health and the utilization in integrity of data and the safety of end user's data. This paper

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

tells the trusted cloud throught the detective control and presents the Trust cloud framework which are approached through technical and policy based approach

III. SECURE PROVENANCE: THE ESSENTIAL OF BREAD AND BUTTER OF DATA FORENSICS IN CLOUD COMPUTING

R. Lu, X. Lin, X. Liang, and X. Shen,(2010) proposed a Secure provenance is the technique in which the users data ownership and the story of the data object is stored and this one of the success in the cloud. In this paper the a new secure provenance scheme is used on the bilinear pairing techniques. As the bread and Buffer of data forensic and post investigation in cloud which proposes the information is confidential , anonyomous authentication of data access by the user and its an provenance of tracking the disputed document. With this technique this paper proves its an security model

IV. ROLE-BASED ACCESS CONTROLS

D.F. Ferraiolo and D.R. Kuhn,(1992) proposed a Mandatory access Control (MAC) which is been used in the Secure Military application whereas the Discretionary Access Controls (DAC) is used in the Security processing of industria and the Civilian of Government.This paper argues that DAC is not found and it is inappropriate access for many commercial and civilian Government Organisation.This paper describes the non-discretionary access control and the role-based access control (RBAC) -that is more central to the secure processing needs of non-military systems than DAC.

V. ADDING ATTRIBUTES TO ROLE-BASED ACCESS CONTROL

D.R. Kuhn, E.J. Coyne, and T.R. Weil,(2010) proposed the Role Based Access Control(RBAC) which is a Information security helps to reduce the complexity of the Secure administration and it provides the permission to the user . It is been criticized for the difficulty of setting up an initial role structure and for inflexibility in rapidly changing domains. The Pure RBAC provide inadequate attribute for the user , to provide the dynamic attribute , particulary in large Organization the “Role Explosion” which results in thousands of roles been seprated to use for the different collection of the permission. Thus the attributes and the rules could either replace RBAC or make it simple and flexible

VI. SECURING PERSONAL HEALTH RECORDS IN CLOUD COMPUTING: PATIENT-CENTRIC AND FINE-GRAINED DATA ACCESS CONTROL IN MULTI-OWNER SETTINGS

M. Li, S. Yu, K. Ren, and W. Lou,(2010) the Personal health Record is the way of storing the data of a patient personally in a Centralized way, this PHR service which facilitate the storage, access and sharing of personal health data. The PHR data should be encrypted so that it is scalable with the number of users having access. Since there is multiowners (patients) of records, each records are identified through the set of Cryptographic key. it is important to reduce the key distribution complexity in such multi-owner record storage . The Existing Cryptographic key is mostly used for the single owner. To enable fine-grained and scalable access control for PHRs, we use Attribute Based Encryption (ABE) techniques to encrypt each patients’ PHR data. To reduce the key distribution complexity, we divide the system into multiple security domains,where each domain manages only a subset of the users. In this way, each patient has full control over their own privacy, and the key managementis reduced. This scheme is flexible, in that it supports efficient and on-demand revocation of user access rights, and break-glass access under emergency scenarios.

VII. ATTRIBUTE BASED DATA SHARING WITH ATTRIBUTE REVOCATION

S. Yu, C. Wang, K. Ren, and W. Lou,(2010) proposed the Ciphertext-policy Attribute Based Encryption(CP-ABE) is a Fine grained access control for sharing of data. Inthis each user has a set of attributes to identify their records, the user can decrypt the record only if the attribute satisfy the Ciphertext. In this paper the author focuses on importance of attribute revocation on CP-ABE scheme. As compared to existing schemes, the proposed solution enables the authority to revoke user attributes with minimal effort.Thus by uniquely integrating the technique of proxy re-encryption with CP-ABE, and enable the authority to delegate most of laborious tasks to proxy
servers. The proposed scheme is secure against the cipher text attack. Hence this record is also applicable in Key-Policy Attribute Based Encryption (KP-ABE)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

VIII. HIERARCHICAL ATTRIBUTE-BASED ENCRYPTION FOR FINE-GRAINED ACCESS CONTROL IN CLOUD STORAGE SERVICES

G. Wang, Q. Liu, and J. Wu,(2010) proposed Cloud Computing is an emerging paradigm where the user can access the data remotely to store and access the data. In medium sized and small sized enterprise uses the Cloud for their cloud based service in the Project.Thus by allowing cloud service providers (CSPs), which are not in the same trusted domains as enterprise users, to take care of confidential data,may raise potential security and privacy issues. To keep thesensitive user data confidential against untrusted CSPs, a cryptographic technique is need to use in it so that only authorized user can decrypt the information. When Enterprise user uses the confeditial data for the outsourcing the encryption system not only support the fine grained access control but also provide the high performance to obtain the data. Thus to obain the confedential data from the cloud server need to combine the hierarchical identity-based encryption (HIBE) system and the ciphertext-policy attribute-based encryption (CP-ABE) system and finally applying proxy re-encryption and lazy re-encryption to this paper.

IX. REALIZING FINE-GRAINED AND FLEXIBLE ACCESS CONTROL TO OUTSOURCED DATA WITH ATTRIBUTE-BASED CRYPTOSYSTEMS

F. Zhao, T. Nishide, and K. Sakurai,(2011) proposed a problem for the security of the storage in case of sharing the outsourced data to others , where server is not trusted by the customer.Cloud storage service denotes an architectural shift toward thin clients and conveniently centralized provision of both computing and storage resources. While utilizing the data storage, the main problem faced in it is, both strong data confidentiality and flexible fine-grained access control without imposing additional cost on the clients.To achieve this protocol the author proposed by combining the cryptographic technique as, attribute-based encryption (ABE) and attribute-based signature (ABS) .

X. CONCLUSION AND FUTURE WORK

This paper dealt about various methods prevailing in literature of anonymous authentication mechanisms for data stored in clouds. It is a Decentralized access of system in which every system have the access control of data . The Cloud which is a Secured storage area where the anonymous authentication is used, so that only the permitted users can be accessed. Decrypting of data can be viewed only by a valid users and can also stored information only by Valid users. This Scheme prevents Replay attack which mean Eaves Dropping can be avoided, Support Creation of data inside storage, Modifying the data by unknown users , and Reading data stored in Cloud. User can revocate the data only by addressing through the cloud. The authentication and accessing the Cloud is Robust, Hence Overall Communication Storage are been developed by comparing to the Centralized approaches. This paper would promote a lot of research in the area of Anonymous Authentication.

REFERENCES

1. Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, , " Decentralized Access Control with AnonymousAuthentication of Data Stored in Clouds", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014
2. S. Ruj, M. Stojmenovic, and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds,” Proc. IEEE/ACM Int’l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.
3. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing,” IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.
4. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,” Proc. IEEE INFOCOM, pp. 441-445, 2010.
5. S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.
6. H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication for Cloud Computing,” Proc. First Int’l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.
7. C. Gentry, “A Fully Homomorphic Encryption Scheme,” PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.
8. A.-R. Sadeghi, T. Schneider, and M. Winandy, “Token-Based Cloud Computing,” Proc. Third Int’l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.
9. R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, “Trustcloud: A Framework for Accountability and Trust in Cloud Computing,” HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.
10. R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.
11. D.F. Ferraiolo and D.R. Kuhn, “Role-Based Access Controls,” Proc. 15th Nat’l Computer Security Conf., 1992.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

12. D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role- Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.
13. M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.
14. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.
15. G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.
16. F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.
17. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.
18. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs- 01-en.pdf, 2013.
19. http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud, 2013.
20. S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation,"Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.
21. R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, 2001.
22. X. Boyen, "Mesh Signatures," Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 210-227, 2007.
23. D. Chaum and E.V. Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 257-265, 1991.
24. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.
25. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.
26. A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," PhD thesis, Technion, Haifa, 1996.
27. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.
28. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
29. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
30. X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.
31. M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.
32. H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure Threshold Multi- Authority Attribute Based Encryption without a Central Authority," Proc. Progress in Cryptology Conf. (INDOCRYPT), pp. 426-436,2008.
33. M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.
34. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," Proc. USENIX Security Symp.,2011.
35. K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IACR Cryptology ePrint Archive, p. 419, 2012.
36. A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.
37. http://crypto.stanford.edu/pbc/, 2013.
38. "Libfenc: The Functional Encryption Library,"http://code.google.com/p/libfenc/, 2013.
39. W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data," Proc. ACM Cloud Computing Security Workshop (CCSW), 2009.
40. J. Hur and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July2011.
41. B.Powmeya , Nikita Mary Ablett ,V.Mohanapriya,S.Balamurugan,"An Object Oriented approach to Model the secure Health care Database systems,"In proceedings of International conference on computer , communication & signal processing(IC^3SP)in association with IETE students forum and the society of digital information and wireless communication,SDIWC,2011,pp.2-3
42. Balamurugan Shanmugam, Visalakshi Palaniswami, "Modified Partitioning Algorithm for Privacy Preservation in Microdata Publishing with Full Functional Dependencies", Australian Journal of Basic and Applied Sciences, 7(8): pp.316-323, July 2013
43. Balamurugan Shanmugam, Visalakshi Palaniswami, R.Santhya, R.S.Venkatesh "Strategies for Privacy Preserving Publishing of Functionally Dependent Sensitive Data: A State-of-the-Art-Survey", Australian Journal of Basic and Applied Sciences, 8(15) September 2014.
44. S.Balamurugan, P.Visalakshi, V.M.Prabhakaran, S.Chranyaa, S.Sankaranarayanan, "Strategies for Solving the NP-Hard Workflow Scheduling Problems in Cloud Computing Environments", Australian Journal of Basic and Applied Sciences, 8(15) October 2014.
45. Charanyaa, S., et. al., , A Survey on Attack Prevention and Handling Strategies in Graph Based Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 2(10): 5722-5728, 2013.
46. Charanyaa, S., et. al., Certain Investigations on Approaches forProtecting Graph Privacy in Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 1(8): 5722-5728, 2013.
47. Charanyaa, S., et. al., Proposing a Novel Synergized K-Degree L-Diversity T-Closeness Model for Graph Based Data Anonymization. International Journal of Innovative Research in Computer and Communication Engineering, 2(3): 3554-3561, 2014.
48. Charanyaa, S., et. al., , Strategies for Knowledge Based Attack Detection in Graphical Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 3(2): 5722-5728, 2014.
49. Charanyaa, S., et. al., Term Frequency Based Sequence Generation Algorithm for Graph Based Data Anonymization International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

50. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Certain Investigations on Strategies for Protecting Medical Data in Cloud", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
51. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Investigations on Remote Virtual Machine to Secure Lifetime PHR in Cloud ", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
52. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Privacy Preserving Personal Health Care Data in Cloud" , International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
53. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, "Investigations on Evolution of Strategies to Preserve Privacy of Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
54. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Certain Investigations on Securing Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
55. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Survey on Approaches Developed for Preserving Privacy of Data Objects" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
56. S.Jeevitha, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Privacy Preserving Personal Health Care Data in Cloud" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014.
57. K.Deepika, P.Andrew, R.Santhya, S.Balamurugan, S.Charanyaa, "Investigations on Methods Evolved for Protecting Sensitive Data", International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 4, Decermber 2014.
58. K.Deepika, P.Andrew, R.Santhya, S.Balamurugan, S.Charanyaa, "A Survey on Approaches Developed for Data Anonymization", International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 4, Decermber 2014.
59. S.Balamurugan, S.Charanyaa, "Principles of Social Network Data Security" LAP Verlag, Germany, ISBN: 978-3-659-61207-7, 2014
60. S.Balamurugan,M.Sowmiya and S.Charanyaa, "Principles of Scheduling in Cloud Computing" Scholars' Press, Germany,, ISBN: 978-3-639-66950-3, 2014
61. S.Balamurugan, S.Charanyaa, "Principles of Database Security" Scholars' Press, Germany, ISBN: 978-3-639-76030-9, 2014