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

Certain Investigations on Anonymous Authentication Mechanisms 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

Researching a Cloud ,which makes to know about the use both in Academic and as well as in industrial Works.The Cloud can be used only through the Internet and the data stored in Cloud is very Secure and privacy so that the Authentication in Cloud by User can retrieve a Secure Transaction , in other hand the user must ensure that data received doesn't had an any error. Wang et al who addressed cloud is a Secured and Dependable storage area. Cloud servers can have a Byzantine failure which mean any unknown error can occur in Cloud and even an Colluding attack , to prevent the error data must be encrypted while Designing the Secure storage techniques. The Searching of encrypted data is an important concern in the Cloud in which queries are used to Obtain the data. Cloud should not know the Query but it must be able to return the records by specifying the keyword through the Query,thus the records are obtained only with the exact keyword. Many researcher had addressed about the security and privacy that protects in clouds, Wang et al had introduced Reed-Solomon erasure coding which is used to check the Multiple random symbol error. The Authentication by the users are been using the public Cryptographic Technique. Many Homomarphic Encryption have been suggested that cloud couldn't able to read the data while the cloud Computation , Using the homomarphic Encryption the cloud gets the Encrypted data by the User which mean a Cipher Text and this text is decoded and sended to the Reciever and checks the cipher text received,but the Cloud cannot know what the data is been operated.

II. PRIVACY PRESERVING ACCESS CONTROL WITH AUTHENTICATION FOR SECURING DATA IN CLOUDS

S. Ruj, M. Stojmenovic, and A. Nayak(2012) proposed a privacy preserving authentication access for the cloud security. The proposed scheme of the paper tells that user can store information without knowing the user's identitfy , this scheme also prevent replay attack, support creation ,modification, and reading the stored data. The data can be decrypted only by the valid user. Since it is a Decentralized authentication access which is compared and developed according to the Centralized users.

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

III. TOWARDS SECURE AND DEPENDABLE STORAGESERVICES IN CLOUD COMPUTING

C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou,(2012) proposed a Cloud storage makes the user to store the information remotely and can be accessed the high definition quality without burden using the hardware and the software. Thought it had a benefit the service makes the user to find a security risk in the access and the storage. So that this paper proposed a flexible distributed storage integrity auditing mechanism and utilizing the homomarphic token and distributed erasure code data . This design which makes very light weight communication of data and a computation cost , auditing result not only ensure the storage correctness guarantee but it also achieves an error by the modification of an location error failure by the server . Considering the cloud is an dynamic in nature ,the cloud can produce an secured outsourced data including the block modification deletion, and an append. Thus this paper proposed it is an highly efficient against a byzantine failure ,malicious data modification attack and server colluding attack.

IV. ENABLING EFFICIENT FUZZY KEYWORD SEARCH OVERENCRYPTED DATA IN CLOUD COMPUTING

J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou,(2010) proposed a cloud storage which becomes a prevalent and a storage of more sensible data it is secured by a privacy, since the data which is outsourced from the cloud is encrypted and the data can be accessed using the keywords and only with the exact keywords the data can be retrieved. This drawback which makes in pre-existence of the cloud computing to be greatly affect by system usability, rendering user searching experienced very frustrating and system efficacy very low. In this paper the author uses the fuzzy keyword to search the data in the cloud,this fuzzy key word which returns the result by showing the data matching to existed search or by relating the search when the data matching fails.In this solution the fuzzy keyword develop two advanced techniques on constructing fuzzy keyword sets, which achieve optimized storage and representation overheads. Thus the paper proposed a technique symbol based tree traversing in which the fuzzy key words are constructed through the multi way tree structure. Hence through this paper the fuzzy key words is used for the security and privacy purpose of the retrieval data and a efficient access.

V. IDENTITY-BASED AUTHENTICATION FOR CLOUD COMPUTING

H. Li, Y. Dai, L. Tian, and H. Yang, (2009) proposed a Cloud computing is one of the recently developed technology which is used in a massive scale between the user and the server, and it is also a secured way of accessing. SSL Authentication Protocol (SAP) which is applied and become a complex in both computation and communication , based on the identity-based hierarchical model for cloud computing(IBHMCC) and its corresponding encryption and signature schemes a new authentication protocol which is used in the Cloud and the service. Through this authentication it is shown as light weight and more efficient compared to the SAP thus it is used in the great scalability between the Cloud and the service.

VI. A FULLY HOMOMARPHIC ENCRYPTION SCHEME

C. Gentry,(2009) proposed fully a homomarphic encryption technique is used in which one allows to encrypt the data using the arbitrary function over the encrypted data without decrypting.i.e., given encryptions E(m1),….,E(mt) of m1,….,mt, one can efficiently compute a compact ciphertext that encrypts f(m1,….,mt) for any efficiently computable function f. This problem was posed by Rivest et al. in 1978. Homomarhic encryption scheme has a numerous application for example the the private query used in the search engine returns the succinct encrypted answer without looking the query clearly ,a user stores encrypted files on aRemote file server and can later have the server retrieve, only files that (when decrypted)satisfy some boolean constraint. Thus the construction begins with the "boostrappable " encryption that works when the function f own by its own during the decryption function.Hence through recursive self embedding and bootstrappable encryption the homomarphic encryption is used and it makes use of hard problems on ideal lattices

VII. TOKEN-BASED CLOUD COMPUTING SECURE OUTSOURCING OF DATA AND ARBITRARY COMPUTATIONS WITH LOWER LATENCY

A.-R. Sadeghi, T. Schneider, and M. Winandy,(2010) proposed the Secured outsourcing of data from untrusted cloud service is more important and the cryptographic solution is fully based on the homomarphic

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

encryption and its an verifyable encryption , recently proposed that this has an high latency where other proposal performs on tamper proof hardware and get suffer from the same problem ,so that the Trusted computing (TC) wich is an another approach where the trusted hardware and the trusted software is been used in computer platform to verify the integrity of the cloud and its computation. Thus these are in under physical control of cloud provider and it have to face the challenging face of run time attestation . In this paper the author focuses mainly on the application to minimize the latency of computation i.e the timing between the query submission and the outsourcing of the data is must be small as possible . to achieve this they combines the trusted hardware with the Secured Function Encryption (SFE) to produce the arbitrary function so that it doesn't leaks any information and its an verifyable Thus the token is used in the setup phase only whereas in the time-critical online phase the cloud computes the encrypted function on encrypted data using symmetric encryption primitives only and without any interaction with other entities.

VIII. 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.
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.

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

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^{3}SP)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.
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