ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Investigations on Decentralized Access Control Strategies for Anonymous Authentication of Data Stored In Clouds

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

The Security of storage is not only enough to store , the user must also check the anonymity of the user. For example the user wants to post a comment on Article but doesn't want his/her to disclosed. There are three cryptographic protocols such as Ring Signature, Mesh Signature ,Group Signature. The Ring Signature which meam a large number of users are been involved so it is not feasible. The Mesh Signature which does not ensure whether the message is from the single user or from a group user and it colludes the information .The Group Signature which is not possible because of the pre-existing in the group.For these kind of reasons a new protocol Attribute Based Signature is been introduced in which the users have claim predicate associate with the message. Hence the ABS is Combined with ABE for the authenticaton Access Control by not showing users identity in the Cloud.

The Author take a centralized approach in where the Single Key Distribution center(KDC) which distributes the Secret key and the attributes to all user. In this the failure not only occurred at a Single point and it is also difficult to maintain by a large number of user in Cloud, finally the author decided to have a decentralized sytem to make the work less and to access by the user from varios location from the world using many KDC's. Yang et al proposed, this decentralized access must also need the technique of anonymous of accessing the cloud while authentication. In earlier Ruj et al proposed the distributed access Control and this does not provide the authentication. The other drawback is the Creator can only create and store the file. So that user who reads the Data can have only the read access and doesn't had the permission to write in the data except by Creator. In the preliminary version the data which enables the authentication of validity message without identifying the user who had stored in Cloud . We use ABS scheme for the authentication and the privacy for the Cloud , it is a resistant from replay attack , revoling of its attribute might no lomger be able to write to the cloud. Therefore in this scheme the writing multiple times was permitted which was not supportedin earlier work.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

II. DACC: DISTRIBUTED ACCESS CONTROL IN CLOUDS

S. Ruj, A. Nayak, and I. Stojmenovic,(2011) proposed a data storage and access in which the multiple encrypted copies of data can be avoided. The main novelty of this paper is producing the key distribution centers where one or more KDCs distribute keys to data owners and users. KDC provide access to particular fields in all records. Single keys seprates the data and the data owners, using this technique the user own the data by having the attribute it had, and this can be retrieved only if the attribute matches the data. The Author apply the attribute-basedencryption (ABE) based on bilinear pairings on elliptic curves. This scheme is collusion secure in which two users cannot together decode any data , that no one has individual right to access. DACC also supports revocation of users, without re-distributing keys to all the users of cloud services. We show that our approach resultsin lower communication, computation and storage overheads, compared to existing models and schemes.

III. EASIER: ENCRYPTION-BASED ACCESS CONTROL IN SOCIAL NETWORKS WITH EFFICIENT REVOCATION

S. Jahid, P. Mittal, and N. Borisov,(2011) proposed it is an approach of privacy risk in the Online Social Network (OSN's) , in which it shifts OSN provider to User by Encryption. This creates a key management and the dynamic groups , to address this problem the author proposed the EASiER an architectural support in Fine grained access control and the dynamic group by the Attribute based Encryption. It is possible to remove access from a user without issuing new keys to other users or re-encrypting existing ciphertexts , this is achieved by creating the proxies and using this proxy can minimally trusted and cannot decrypt ciphertexts or provide access to previously revoked users. This type of technique is used in FACEBOOK

IV. ATTRIBUTE-BASED SIGNATURES: ACHIEVING ATTRIBUTE-PRIVACY COLLUSION-RESISTANCE

D. Chaum and E.V. Heyst,(1991) proposed a Attribute based Signature in which the signature attests not to identify the individual of the message by a user instead it claim regarding the attribute that produced by the user.The signature was produced by a single party whose attributes satisfy the claim being made i.e it is not colluding the all individuals instead it just make the attribute together who pooled it.The author explains the security requirements of ABS as a cryptographic primitive, and then tells that efficient ABS construction based on groups with bilinear pairings. Thus by proving the construction is secure in the generic group model, ABS fills a critical security requirement in attribute-based messaging(ABM) systems.A powerful feature of ABS construction is that unlike many other attribute-based cryptographic primitives, it can be readily used in a multi-authority setting, wherein users can make claims involving combinations of attributes issued by independent and mutually distrusting authorities.

V. SECURED SCHEME FOR SECRET SHARING AND KEY DISTRIBUTION

A. Beimel,(1996) proposed the sharing of data, now a days take place in Computer Networks, and the data which is been communicated inside the network may affected through the bad users,to overcome this user users two Cryptographic tools such as Generalized Secret Sharing scheme and Key distribution scheme. This make it possible to store only the secret information in the network such that only good users can access the information . the secret sharing scheme mostly received through the threshold secret sharing schemes, only through the certain threshold the information can accessed and can used by the user. In generalized secret sharing it is capable of arbitrary monotone collection whereas in Key distribution scheme the keys can be used Communication key Distribution scheme does not help in unrestricted scheme on other hand secured and restricted scheme can be accessed only through limits.Linear Secret Sharing Scheme , Monotone Span programs ,Secret sharing the public reconstruction , computation function of shared secret keys are used

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

VI. FUZZY IDENTITY-BASED ENCRYPTION

A. Sahai and B. Waters,(2005) Proposed a new Identity-Based Encryption (IBE) scheme that is called as Fuzzy Identity-Based Encryption ,A Fuzzy IBE private key was identity by ω whereas the ciphertext encrypted is identified by ω'.It identities ω and ω' are close to each other as measured by the "set overlap" distance metrics. It used to apply the Encryption by obtaining the biometric input as identifier which inherently will have some noise each time they are sampled.Thus it is used for a type of application that we term "attribute-based encryption".In this paper two construction of Fuzzy IBE scheme are involved where the Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Hence in this scheme both are error-tolerant and secure against collusion attacks.

VII. CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION

J. Bethencourt, A. Sahai, and B. Waters,(2007) proposed Certain distributed system the user can access the data only if the data consist of credential or attributes. Only way of enforcing such data in Cloud can be performed through the Trusted server to store the data and accessing the cloud. In this paper the complex access control on the encrypted data is performed in which the Cipher text policy Attribute-Based Encryption is used. By using this scheme the storage data can be kept confidential even when the storage is untrusted, and this method secures against the collusion attack. The Previous Attribute Based Encryption systems used attributes to describe the encrypted data and even to built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus this method uses the Role Based access Control (RBAC).

VIII. MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION

M. Chase,(2007) proposed identity based encryption the user use the identity to search the data whereas in attribute based ecryption involves attribute to search the data. Sahai and water introduced a single authority attribute encryption scheme and left the question whether the multiple authorities allowed todistribute system. This scheme allows any polynomial number of independent authoritiesto monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number *dk* and a set of attributes. Thus this scheme tolerate an arbitrary number of corrupt authoritites.

IX. OUTSOURCING THE DECRYPTION OF ABE CIPHERTEXTS

M. Green, S. Hohenberger, and B. Waters,(2011) proposed ABE is only used in cloud storage and many Computing application.The main drawback of the Ciphertext is size of the text and the time required to complexity of the access formula. ABE ciphertexts are stored in the cloud. In which a user can provide the cloud with a single transformationkey that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes into a (constant-size) El Gamal-style ciphertext, without the cloud being able to read any part of the user's messages. This provide a new secured definitions for both CPA and replayable CCA security with outsourcing ,several new constructions, an implementation of our algorithms and detailed performance measurements. In a typical configuration, the user saves significantly on both bandwidth and decryption time, without increasing the number of transmissions.

X. SECURE AND EFFICIENT ACCESS TO OUTSOURCED DATA

W. Wang, Z. Li, R. Owens, and B. Bhargava,(2009) proposed by providing secure and efficient access to outsourced data should be must in cloud computing .To encrypt every data block with a different key the flexible cryptography-based access control is used. Through this key derivation methods, the owner should maintain only a few secrets in the storage . and this key derivation procedure is used in hash functions which will introduce very limited computation .Thus to use over-encryption and or lazy revocation to prevent revokedusers from getting access to updated data blocks. A Mechanism is used to handle both updates to outsourced data and changes in user access rights. Hence it is investigated in the overhead and safety of the proposed approach.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

XI. 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.
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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

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.
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