ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 11 , November 2015

A Survey on Data Stored in Clouds

M.R.KAVITHA RANI,M.E, S.BRINDHA,M.E.,

Department of CSE, K.L.N. College of Engineering, ANNA UNIVERSITY, Sivagangai , India
Assistant Professor, Dept. of CSE, K.L.N. College of Engineering, ANNA UNIVERSITY, Sivagangai , India

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. Users 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

CLOUD computing is recognized as another to traditional data technology attributable to its resource -sharing and low-maintenance characteristics. In cloud computing, the cloud service suppliers (CSPs), like Amazon, area unit ready to deliver numerous services to cloud users with the assistance of powerful datacenters. By migrating the native knowledge management systems into cloud servers, users will fancy high-quality services and save significant investments on their native infrastructures. One of the foremost basic services offered by cloud providers is knowledge storage. Allow us to think about a sensible knowledge application. An organization permits its staffs within the same cluster or department to store and share files within the cloud. By utilizing the cloud, the staffs are often fully discharged from the difficult native knowledge storage and maintenance. However, it additionally poses a major risk to the confidentiality of those hold on files. Specifically, the cloud servers managed by cloud suppliers aren't totally trustworthy by users while the information files hold on within the cloud could also be sensitive and confidential, like business plans. To preserve knowledge privacy, a basic resolution is to write in code knowledge files, and then upload the encrypted knowledge into the cloud.

Accountability of cloud which means the amount of storage, which is been a Challenging task by a 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

Several expressive data access policies have been enforced by the Cipher text Policy Attribute Based Encryption (CP-ABE). [2] With the given number of attributes, the Privacy Preserving Constant CP-ABE (denoted as PP-CPABE) significantly reduces the ciphertext to a constant size. Regardless of the number of attributes it also enforces hidden access policies with wildcards and incurs constant-size conjunctive headers. In CP-ABE, a ciphertext is embedded with an access control policy associated with user attributes. It can be viewed as a one-to-many public key encryption scheme and it enables a data owner to grant access to an unknown set of users. The access policies will be

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 11 , November 2015

defined by the data owner and encryption will be carried out based on those policies. A secret key reflecting its attributes will be given to each user and the user can decrypt the data only when its attributes satisfies those access policies. An attribute authority will be responsible for providing the secret keys for the attributes of each user. Any subset of attribute set can be used by the user for signing the messages with the secret key. The signature can be verified against a policy of attributes and verification will be successful only if the attributes used during signing satisfies the policies. The requirement of ABE with outsourced decryption is verifiability.

Access control of data which involves 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)[1]. 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 members not 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)[5]. For example the patient's staff nurse 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. RELATED WORK

Taeho Jung, Xiang-Yang Li [1] proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer.

Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak[2] presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud.

R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M.Kirchberg, Q. Liang, and B.S. Lee [3] 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 focus on 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 tells the trusted cloud throught the detective control and presents the Trust cloud framework which is approached through technical and policy based approach.

F. Zhao, T. Nishide, and K. Sakurai [4] 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).

R. Lu, X. Lin, X. Liang, and X. Shen [5] proposed a secure provenance is the technique in which the user's data ownership and the story of the data object is stored and this one of the success in the cloud. In this paper a new

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 11 , November 2015

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 it's a provenance of tracking the disputed document. With this technique this paper proves it's a security model

D.R. Kuhn, E.J. Coyne, and T.R. Weil [6] 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 , particularly in large Organization the "Role Explosion" which results in thousands of roles been separated 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

S. Yu, C. Wang, K. Ren, and W. Lou [7] proposed the Ciphertext-policy Attribute Based Encryption (CP-ABE) is a Fine grained access control for sharing of data. In this 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)

G. Wang, Q. Liu, and J. Wu [8] 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 the sensitive 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 confidential data for the outsourcing the encryption system not only supports the fine grained access control but also provide the high performance to obtain the data. Thus to obtain the confidential 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.

Table 1: Comparison of proposed scheme with existing access control scheme

Schemes	**Fi-ne-graine d access control**	**Central-ized/Decentraliz ed**	**Write/ read ac-cess**	**Type of access control**	**Privacy pre-serving authen-tication**	**User revocati -on**
Secure and Efficient Access	Yes	Centralized	1-W-M-R	Symmet-ric key cryptog-raphy	No authentication	No
Fine Grained Access Control	Yes	Centralized	1-W-M-R	ABE	No authentication	No
Attribute Based data Sharing	Yes	Centralized	1-W-M-R	ABE	No authentication	No
Outsourc-Ing The Decryption	Yes	Centralized	1-W-M-R	ABE	No authentication	No
Proposed Scheme	Yes	Decentralized	M-W-M-R	ABE	Authentication	Yes

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 2, Issue 11 , November 2015

Table 2: Comparison of computation and size of cipher text while creating a file

Schemes	Computation by creator	Computation by cloud	Size of cipher text
Fine grained data access control	(m+2)E_0	0	mlog $\|G_0\|$ + $\|G_T\|$ + m log m+ $\|MSG\|$
Attribute based data sharing	(m+2)E_0	0	mlog $\|G_0\|$ + $\|G_1\|$ + $\|MSG\|$
Proposed approach	(3m + 1)E_0 + 2mE_T + τp (encrypt)(2l + 2)E1 + 2t E2 + $\tau\mathcal{H}$ (sign)	2m $^{\tau p}$ + $\tau\mathcal{H}$ + O(mh)(decrypt)	2m $\|G_0\|$ + m $\|G_T\|$ + m^2 + $\|MSG\|$ + (l+ t+2) $\|G_1\|$

Table 3: Comparison of computation during read and write by user and cloud

Schemes	Computation by user while write	Computation by user while read	Computation by cloud while write
Fine grained data access control	No write access	m	No write access
Attribute based data sharing	No write access	m	No write access
Proposed approach	(3m + 1)E_0 + 2mE_T + (encrypt)(2l + 2)E1 + 2tE2 + (sign)	2m + O(mh) (decrypt)	(l +2t) + l(E_1 + E_2) + (verify)

III. CONCLUSION

This paper dealt about various methods prevailing in literature of anonymous authentication mechanisms for data stored in clouds. The *AnonyControl-F* directly inherits the security of the *AnonyControl* and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-*n* oblivious transfer.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

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 11 , November 2015

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. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes. This paper would promote a lot of research in the area of Anonymous Authentication.

IV.ACKNOWLEDGEMENT

This work was supported in part by grants from the Dr. A.V. Ram Prasad, Principal of K.L.N. College of engineering and also supported by grants from DR.N. Lakshmi Narasimman, Professor & Head of Computer Science and Engineering and Ms.S.Brindha (Project Guide), K.L.N. College of engineering, who had helped us during preparation and also provided valuable feedback for guidance.

REFERENCES

1. Taeho Jung, Xiang-Yang Li, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption" IEEE Transactions on Information Forensics and Security, Vol. 10, No. 1, January 2015.
2. Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, , " Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.