P VENKATESWARLU, et al , International Journal of Research Sciences and Advanced Engineering [IJRSAE]™

Volume 2 , Issue 01, PP: 42 - 47 , JAN - MAR ' 2013.

ASPECT-BASED DATA DISTRIBUTION TO PROVIDE PREFERENCE BASED SURVEILLANCE TO IMPROVE THE ACT EFFICIENCY

P VENKATESWARLU 1*

1 . Professor , Dept of CSE, Chilkur Balaji Institute of Science & Technology, Hyderabad.

ABSTRACT:

Time and Technology has its own significance, in the aspect of Information Technology and its security constraint is always a question mark to the demographic of the world of technology ion the system of Information Technology. With the Kind of concept in the today's market we have wide use of parallel and distributed computing environment along with the next technology or we can call as derived cloud computing which provide a pacific render based service in the distributed environment. More or less we are in the loop of security concern to that mechanism, where Banking & Financial Sectors are having fear to use the technology, because we cannot confirm everything to them in the point of security concern. In the Paradigm of such concern we take forward the concept to implement which we have given a glimpse in this paper, where we implemented attribute based data encryption sharing mechanism in the public domain of network with the key point of applying private keys with the basis of priority and data holder keeping the eye of performance and efficiency which we take as most important concept as well.

KEYWORDS: Data sharing, attribute-based encryption, open ID, access control.

I.INTRODUCTION:

Finally, most data sharing scenarios have important dynamic aspects. Data is constantly being updated refined, corrected, and expanded and the participants naturally desire the most recent version of it. As has been observed since the earliest data integration investigations, this creates a tension between the efficiency of answering queries and the freshness of the obtained answers, with data warehousing favoring the former and virtual integration the latter. Moreover, it is not just the data that is dynamic, but also the set of participants, their schemas, and the relationships among them. Especially in the "bootstrapping" phase of a collaboration where the complex relationships among participants and data are only partially understood such changes can occur as often as changes to the source data. We need a platform which copes with changes both to data and to the mappings among data sources. In this section we present the security model for K2C. We assume that the root user, representing the data owner, is trusted. The clouds providers are honest-but-curious who follow the

protocol and faithfully execute the operations, but May actively attempt to gain additional knowledge, such as the sensitive data stored in the cloud. An adversary may attempt to perform unauthorized read or write access against the stored data, or attempt to learn the identities of readers or writers. For example, end-users may try to perform unauthorized read or write operations on stored data objects. To perform their attacks, unauthorized users may use their existing access keys for other objects and categories or cooperate with other unauthorized users and cloud providers to derive/guess credentials required to perform unauthorized access. Similarly, cloud providers may try to read or modify stored data or learn about the identities of the end users. Cloud providers may collude with each other or some unauthorized end-users to break the security of K2C. We assume communication channels between participants are secure.

II. RELATED WORK

Assuming that each user has a unique identity in an IBE system, a natural security requirement is that no attacker can read the plaintext encrypted to a user without knowing that user's private key. However, when the KGC is the attacker, the user has no security at all. This is due to the basic functionality requirement of IBE ensuring that any party who owns the master secret key can perform user private key generation, and all it takes for decryption is a user private key. Indeed, that is a problem also related to the privacy issue of IBE – the KGC knows the identity of all users of the system since it is responsible for user authentication. The KGC could decrypt any message addressed to a user by generating that user's private key.

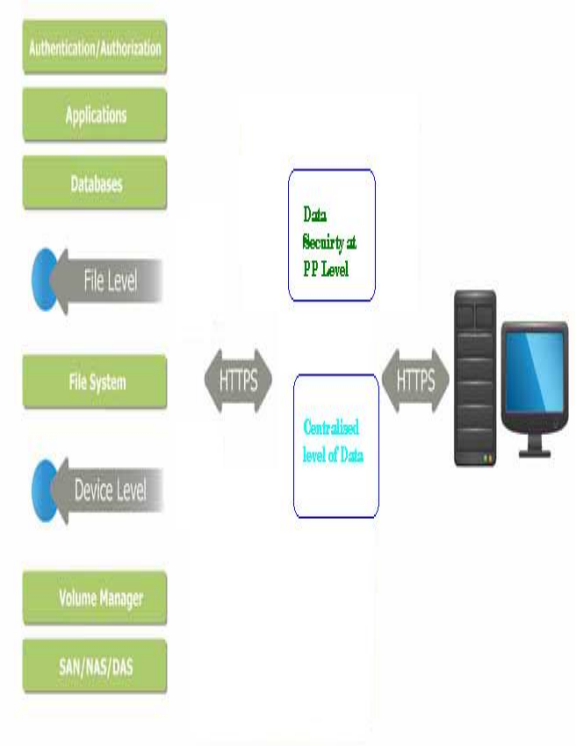

Fig.2.1 Illustrates Model View Transformation in the Authentication Mechanism of Data Security

Security

Our protocol must protect the confidentiality and integrity of stored data against cloud providers and unauthorized end-users.

Meaning that the stored data should be readable for authorized users only and any unauthorized change to the data should be prevented or detectable. Access rights of a specific end-user as well as his usage trends should not be visible to other users or cloud service providers to provide

Efficiency and Scalability

To avoid unjustified cost of re-encryption, the protocol should support lazy revocation. Also, the complexity of operations should be independent of number of data objects and users in the system. This ensures that the protocol wills not affect the scalability of existing cloud services.

Flexibility

The protocol should allow data owners and end-users to organize and manage their data in hierarchies similar to conventional systems. Directories also represent access class hierarchies, users who have access to a directory/folder also assume the same access to all and directories below that directory. Also, they should be able to grant/revoke part of their access rights to/from other users in a decentralized and scalable manner.

III. METHODOLOGY

In the Methodology, where in this paper, we put forward the lasts technology mechanism by comparing the all cyclic value where we meant to put forward the mechanism of the best encryption and authentication mechanism. We use the term anonymous cipher text" to refer a cipher text that the KGC holds without the knowledge of who is the intended recipient. We do not model the case where the KGC maliciously generates the system parameters, but we provide a new embedded-identity encryption" oracle, which lets the adversary adaptively get many cipher texts designated to the same person, without knowing the real identity. The absence of such an oracle gives the adversary no way to see more than one cipher text for the unknown recipient. For the ease of discussion, we suppose an identity is of n-bit length. In the Path of cyclic protocol mechanism to send t he data through network we implemented the following algorithm, where we have followed the authentication mechanism of tuple or row wise mechanism initialized to some variable here we used Tuple: θ.

.

Algorithm Data Assoctation with tuple $t \in [Q]^I$

All-Trees

1: Initialize $F \leftarrow \{t : t \in \text{supp}(I)\}$
2: Initialize $\Omega \leftarrow \emptyset$
3: repeat
4: $F' \leftarrow T_Q^V(F, \Omega)$
5: for every tree $\tau \in F'$ do
6: if any child of root(τ) is in Ω or any proper descendant of root(τ) to a node associated with the same tuple then
7: $\Omega \leftarrow \Omega \cup \{\text{root}(\tau)\}$
8: else
9: $F \leftarrow F \cup \{\tau\}$
10: end if
11: end for
12: until nothing added to either F or Ω in last iteration
13: for every $t \in [Q]^{\text{supp}(I)}$ do
14: if $t \in \Omega$ then
15: $P(t) \leftarrow \infty$
16: else
17: $P(t) \leftarrow \sum_{\substack{\tau \in F \text{ s.t.} \\ \text{root}(\tau) = t}} \prod_{R(t') \in \text{fringe}(\tau)} R^I(t')$
18: end if
19: end for
20: return P

An authorization delegation protocol allows a user to delegate permissions to a consumer to access her resources hosted at a service provider. For example, a user may be able to delegate permissions needed to access her on a photo-sharing website to a website that provides photo editing utilities. An authorization delegation protocol should be privacy-preserving in that it must not reveal the user's identity.

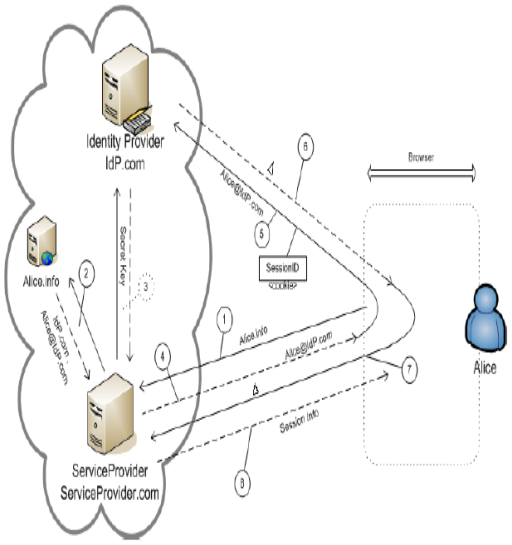

Fig.3.1 Illustrates the Authentication Mechanism

In the example above, for instance, the user may wish to grant the photo editing service read access to her photos hosted on the photo sharing website without revealing her identity to the photo editing service. Protocol in this section, we outline the Open ID protocol, which is relatively a popular identity management solution on the Web, and explain its shortcomings for the next generation of Web applications. The main purpose of this section is to give some background to the reader that is not familiar with Open ID. We have deliberately omitted details, and encourage interested readers to consult the Open ID specification.

IV. CONCLUSION

In the technology of mitigation and the With high-speed encryption, integrated key management, and context-aware access controls, Encryption protects valuable information in order to address industry and government regulations, secure virtual and cloud-based environments, and most importantly, drastically lower the risk of devastating data breaches. The primary conclusion of our research is that adoption of user-centric security models and shifting certain parts of communication and computation to the client side allows us to provide the cloud consumers with more visibility and control over their resources. Therefore, using this approach not only the security and privacy concerns of cloud consumers can be addressed more effectively, but also the burden of managing end-users' identities and fine-granular access control will be reduced from cloud service providers.

V. REFERENCES

[1] Amazon S3 . http://aws.amazon.com/s3/.

[2]GoogleJuice.
http://code.google.com/p/google-guice/

[3] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt '05), pp. 457-473, 2005.

[4] 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.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[6] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and Comm. Security, pp. 195-203, 2007.

[7] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy, pp. 273-285, 2010.

[8] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.

[9] N. Attrapadung and H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption," Proc. Int'l Conf. Palo Alto on Pairing-Based Cryptography (Pairing), pp. 248-265, 2009.

[10] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems," Proc. ACM Conf. Computer and Comm. Security, 2006.

[11] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," ACM Computing Surveys, vol. 35, no. 3, pp. 309-329, 2003.

[12] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A Content- Driven Access Control System," Proc. Symp. Identity and Trust on the Internet, pp. 26-35, 2008.

[13] 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 '10), 2010.

[14] S.D.C. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-Encryption: Management of Access Control Evolution on Outsourced Data," Proc. Int'l Conf. Very Large Data Bases (VLDB '07), 2007.

[15] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[16] A. Kate, G. Zaverucha, and I. Goldberg, "Pairing-Based Onion Routing," Proc. Privacy Enhancing Technologies Symp., pp. 95-112, 2007.

[17] L. Cheung and C. Newport, "Provably Secure Ciphertext Policy ABE," Proc. ACM Conf. Computer and Comm. Security, pp. 456-465, 2007.