International Journal of scientific research and management (IJSRM)
\||Volume||3||Issue||6||Pages|| 3098-3102||2015||
Website: www.ijsrm.in ISSN (e): 2321-3418

Proficient Cloud Based Authenticated Database Scheme for Web services

Mrs. Evangeline. S [#1], Mr. S.Vijayanand [*2], Ms. Abirami.S.,[@3]
[#1] PG Scholar, Department of CSE, College, Shree Venkateshwara Hi-Tech Engg College, Gobi,Tamilnadu, India,
[*2] Assistant Professor, Department of CSE, College, Shree Venkateshwara Hi-Tech Engg College, Gobi,Tamilnadu, India,
[@3] PG Scholar, Department of CSE, College, Shree Venkateshwara Hi-Tech Engg College, Gobi,Tamilnadu, India,
[1] evasamuvel@gmail.com
[2] anand.vijay87@gmail.com
[3]abiramishanmugamn@gmail.com

***Abstract*— In this research article, I support the disguise access control scheme and propose a new decentralized provide secure data storage clouds. Under the proposed scheme the cloud data storage without knowing the identity of the user to verify the authenticity of the series. My plan is to decrypt the information can be stored for only a valid user access control. The program prevents replay attacks and the creation, modification and supports reading data deposited in the cloud. We cancelled a lecture by the user. Also, the clouds are designed as centralized authentication and access control and access control programs, our program is a versatile and robust. Communication, computation, and storage costs are comparable to centralized approaches.**

***Keywords*— Authenticity, Decentralized data control, Anonymous authentication, versatile and robust.**

I. INTRODUCTION

A rationally developed technology to store data from more than one client. Cloud computing is an environment that enables users to remotely store their data. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization. It helps enterprises and government agencies reduce their financial overhead of data management. They can archive their data backups remotely to third party cloud storage providers rather than maintain data centers on their own. An individual or an organization may not require purchasing the needed storage devices. Instead they can store their data backups to the cloud and archive their data to avoid any information loss in case of hardware / software failures. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. There are three objectives to be main issue
Confidentiality – preserving authorized restrictions on information access and disclosure. The main threat accomplished when storing the data with the cloud.
Integrity – guarding against improper information modification or destruction.
Availability – ensuring timely and reliable access to and use of information.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must encrypt the file and then store file to the cloud. If a third person downloads the file, he/she may view the record if he/she had the key which is used to decrypt the encrypted file. Sometimes this may be failure due to the technology development and the hackers. To overcome the problem there are lot of techniques introduced to make secure transaction and secure storage. The encryption standards used for transmit the file securely. The assured deletion technique aims to provide cloud clients an option of reliably destroying their data backups upon requests. The encryption technique was implemented with set of key operations to maintain the secrecy.

The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to a breach of security. Access control relies on and coexists with other security services in a computer system. Access control is concerned with limiting the activity of legitimate users.

It is enforced by a reference monitor which mediates every attempted access by a user (or program executing on behalf of that user) to objects in the system. The reference monitor consults an authorization database in order to determine if the user attempting to do an operation is actually authorized to perform that operation. Authorizations in this database are administered and maintained by a security administrator. The administrator sets these authorizations on the basis of the security policy of the organization. Users may also be able to modify some portion of the authorization database, for instance, to set permissions for their personal files.

Ability to limit and control the access to host systems and applications via communication links. To achieve, access must be identified or authenticated. After achieved the authentication process the users must associate with correct policies with the files. To recover the file, the client must request the key manager to generate the public key.

For that the client must be authenticated. The attribute based encryption standard is used for file access which is authenticated via an attribute associated with the file. With file access control the file downloaded from the cloud will be in the format of read only or write supported. Each user has associated with policies for each file. So the right user will access the right file. For making file access the attribute based encryption scheme is utilized.

depend. Without good authentication there is little point in focusing attention on strong access control or strong intrusion detection. The reader is surely familiar with the process of signing onto a computer system by providing an identifier and a password. In this most familiar form authentication establishes the identity of a human user to a computer. In a networked environment authentication becomes more difficult. An attacker who observes network traffic can replay authentication protocols to masquerade as a legitimate user.

Similarly, authentication of a computer to a user is also useful to prevent against spoofing attacks in which one computer masquerades as another (perhaps to capture user identifiers and passwords). Often we need a combination of user – to – computer and computer – to –computer authentication. Roughly speaking, user-to-computer authentication is required to establish identity of the user to a workstation and computer-to-computer authentication is required for establishing the identity of the workstation acting on behalf of the user to a server on the system (and vice versa). In distributed systems authentication must be maintained through the life of a conversation between two computers. Authentication needs to be integrated into each packet of data that is communicated. Integrity of the contents of each packet and perhaps confidentiality of contents must also be ensured.

Our focus in this chapter is on user-to-computer authentication. User-to-computer authentication can be based on one or more of the following:

Something the user knows, such as a password,

Something the user possesses, such as a credit-card sized cryptographic token or smart card, or

Something the user is, exhibited in a biometric signature such as a finger print or voice-print.

Key-based authentication is the most common technique but it has significant problems. A well-known vulnerability of keyword is that they can be guessed, especially since users are prone to selecting weak keywords. Such compromise can occur without the user even being aware of it. It is also hard for users to remember too many passwords, especially for services that are rarely used. Nevertheless, because of low cost and low technology requirements, passwords are likely to be around for some time to come. Password management is required to prod users to regularly change their passwords, to select good ones and to protect them with care. Excessive password management makes adversaries of users and security administrators which can be counter-productive.

The response is to disallow frequent changes to a user's password. Passwords are often used to generate cryptographic keys which are further used for encryption or other cryptographic transformations. Encrypting data with keys derived from passwords is vulnerable to so-called dictionary attacks. The former search is usually computationally infeasible while the latter can be accomplished in a matter of hours using common place workstations. These attacks have been frequently demonstrated and are a very real threat. Operating systems typically store a user's password by using it as a key to some cryptographic transformation. Access to the so-called encrypted passwords provides the attacker the necessary known plaintext for a dictionary attack.

This can be achieved by looking up a large dictionary. Such dictionaries can be very big (tens of mega bytes) and may need to be replicated at multiple locations. They can themselves pose a security hazard. Statistical techniques for proactive password checking have been proposed as an alternative.

In this paper key anonymous authntication Based Encryption scheme is used to control unauthorized access. In addition to this centralized access control was provided with less storage costs and centralized controlling approaches.

II. Related Works

Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption. The keywords are sent to the cloud encrypted and the cloud returns the result without knowing the actual keyword for the search. The problem here is that the data records should have keywords associated with them to enable the search. The correct records are returned only when searched with the exact keywords.

Security and privacy protection in clouds are being explored by many researchers. The addressed storage security using authentication of users using public key cryptographic techniques and many homomorphic encryption techniques have been suggested to ensure that the cloud is not able to read the data while performing computations on them. Using homomorphic encryption, the cloud receives ciphertext of the data and performs computations on the ciphertext and returns the encoded value of the result. The user is able to decode the result but the cloud does not know what data it has operated on. In such circumstances, it must be possible for the user to verify that the cloud returns correct results. Accountability of clouds is a very challenging task and involves technical issues and law enforcement. Neither clouds nor users should deny any operations performed or requested. It is important to have log of the transactions performed; however, it is an important concern to decide how much information to keep in the log. Accountability has been addressed in TrustCloud.

In existing system propose privacy preserving authenticated access control scheme. According to our scheme a user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS. We will first discuss our scheme in details and then provide a concrete example to demonstrate how it works. There are three users, a creator, a reader and writer.

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. In future, we would like to hide the attributes and access policy of a user.

.

III. System Design

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must encrypt the file and then store the file to the cloud. If a third person downloads the file, he/she may view the record if he/she had the key which is used to decrypt the encrypted file. Sometimes this may be failure due to the technology development and the hackers. to overcome the problem

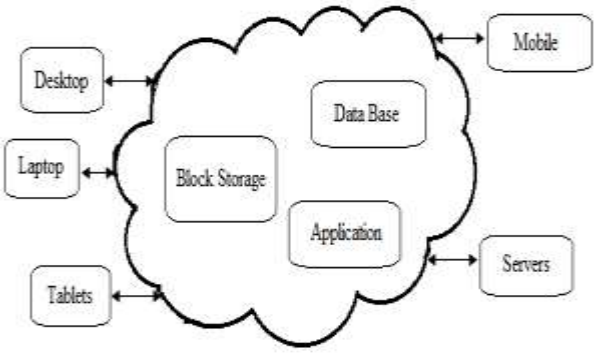

Fig. 1 Anonymous authentication

there are lot of techniques introduced to make secure transaction and secure storage. The encryption standards used for transmit the file securely. The assured deletion technique aims to provide cloud clients an option of reliably destroying their data backups upon requests. The encryption technique was implemented with set of key operations to maintain the secrecy. Recently, Sushmita ruj [1] addressed Anonymous Authentication [1] for data storing to clouds. Anonymous authentication is the process of validating the user without the details or attributes of the user. So the cloud server doesn't know the details or identity of the user, which provides privacy to the users to hide their details from other users of that cloud. Security and privacy protection in clouds are examined and experimented by many researchers. Wang et al. [16] provides storage security using Reed-Solomon erasure- correcting codes. Using homomorphic encryption, [17] the cloud receives cipher text and returns the encoded value of the result. The user is able to decode the result, but the cloud does not know what data it has operated on. Time-based file assured deletion, which is first introduced in [5], means that files can be securely deleted and remain permanently inaccessible after a predefined duration. The main idea is that a file is encrypted with a data key by the owner of the file, and this data key is further encrypted with a control key by a separate key manager (known as Ephemerizer [21]). The key manager is a server that is responsible for cryptographic key management. In [5], the control key is time-based, meaning that it will be completely removed by the key manager when an expiration time is reached, where the expiration time is specified when the file is first declared. Without the control key, the data key and hence the data file remain encrypted and are deemed to be inaccessible. Thus, the main security property of file assured deletion is that even if a cloud provider does not remove expired file copies from its storage, those files remain encrypted and unrecoverable. An open issue in the work [22] is that it is uncertain that whether time-based file assured deletion is feasible in practice, as there is no empirical evaluation. Later, the idea of time-based file assured deletion is prototyped in Vanish [23]. Vanish divides a data key into multiple key shares, which are then stored in different nodes of a public Peer-to-Peer Distributed Hash Table (P2P DHT) system. Nodes remove the key shares that reside in their caches for a fixed time period. If a file needs to remain accessible after the time period, then the file owner needs to update the key shares in node caches. Since Vanish is built on the cache-aging mechanism in the P2P DHT, it is difficult to generalize the idea from time-based deletion to a fine- grained control of assured deletion with respect to different file access policies.

IV. IMPLEMENTATION

A. Distributed Key Policy Attribute Based Encryption KP-ABE is a public key cryptography primitive for one-to-many correspondences. In KP-ABE[23], information is associated with attributes for each of which a public key part is characterized. The encryptor associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access structure. The proposed scheme consists of four algorithms[24] which is defined as follows Setup: This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.

Encryption: It takes a message, public key and set of attributes. It outputs a cipher text.

Key Generation: It takes as input an access tree, master key and public key. It outputs user secret key.

Decryption: It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

B. File Assured Deletion The policy of a file may be denied under the request by the customer, when terminating the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The point when any of the above criteria exists the policy will be repudiated and the key director will totally evacuates the public key of the associated file. So no one can recover the control key of a repudiated file in future. For this reason we can say the file is certainly erased.

To recover the file, the user must ask for the key supervisor to produce the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is verified by means of an attribute connected with the file. With file access control the file downloaded from the cloud will be in the arrangement of read just or write underpinned. Every client has connected with approaches for each one file. So the right client will access the right file. For making file access the key policy attribute based encryption.

V. CONCLUSIONS

We propose secure cloud storage using decentralized access control with anonymous authentication. The files are associated with file access policies, that used to access the files placed on the cloud. Uploading and downloading of a file to a cloud with standard Encryption/Decryption is more secure. Revocation is the important scheme that should remove the files of revoked policies. So no one can access the revoked file in future. The policy renewal is made as easy as possible. The renew key is added to the file. Whenever the user wants to renew the files he/she may directly download all renew keys and made changes to that keys, then upload the new renew keys to the files stored in the cloud. In future the file access policy can be implemented with Multi Authority based Attribute based Encryption. Using the technique we can avoid the number of wrong hits during authentication. Create a random delay for authentication, so the hacker can confuse to identify the algorithm for gaining access over the cloud data.

Hence with this I support, the disguise access control scheme and propose a new decentralized provide secure data storage clouds also the centralized authentication and access control and access control programs, our program is a versatile and robust. Communication, computation, and storage costs are comparable to centralized approaches.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentica- tion for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

[6] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.

[7] 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.

[8] 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.
9] 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

. [10] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992.

[11] 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.

[12] 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.

[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), pp. 261-270, 2010.

[14] 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.

[15] 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.

[16] 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.

[17] http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs- 01-en.pdf, 2013.

[18] http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud, 2013.

[19] 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.

[20] 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.

[21] X. Boyen, "Mesh Signatures," Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 210-227, 2007.

[22] D. Chaum and E.V. Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 257-265, 1991.

[23] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resis- tance," IACR Cryptology ePrint Archive, 2008.

[24] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

Authors:

Mrs. Evangeline.S, Completed UG in 2012, Mahendra engineering college for women, thiruchengode-namakkal and currently persuing her M.E CSE degree in Shree Venkateshwara Hi-Tech Engg College, Gobi, Tamilnadu , India. Her research interests include Cloud computing, Cloud security etc.,

Mr. S.Vijayanand, received the Bachelor of Engineering in Institute of road and transport technology(IRTT) . He is currently working as Assistant professor in Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam, Tamilnadu. His research interest includes Cloud computing and Cloud Security.