IJARES/July 2014/Volume-2/Issue-7/1129-1134 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

CONSIDERING ENCRYPTION SYSTEM FOR CONSTANT ACCESSION IN CLOUD ENVIRONMENT

D.Shiva Kumar[1], U.Ramya Sree[2]

[1]M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

ABSTRACT:

Information security in addition to confidentiality is one of the important safety concerns in cloud system exceptional to its Internet basis information organization. Data represents an exceptionally important advantage in support of any association. To access the shared data files, data users download the data files of encrypted of their concentration from the cloud and subsequently decrypt them. Hierarchical attribute-set-based encryption intended for access control in cloud computing organizes attributes of user into a structure of recursive set and allows users to compel dynamic limits on how those attributes may possibly be combined to convince a policy. Cipher text-policy attribute-set-based encryption was extended with a structure of hierarchical towards effectively entrusts the trustworthy operation of authority's private attribute key generation towards lower-level domain authorities. Intended for cloud computing an access control mechanism is proposed which is based on key-policy attribute-based encryption, jointly with a re-encryption technique for proficient user revocation. Since owners of data and providers of service are typically not in similar trusted field in cloud computing, a novel scheme of access control utilizing attributed-based encryption was introduced that assumes key-policy attribute-based encryption to put into effect the control of fine-grained access.

Keywords: Data files, Encryption, Cloud computing, Domain authority.

1. INTRODUCTION:

Flexible and fine-grained access control is also strongly preferred in the service-oriented cloud computing model. Usage of key-policy attribute-based encryption provides fine-grained access control elegantly [4]. The provider of cloud service administers a cloud to make available the service of data storage. Governors of the data encrypt their data files and store up them in the cloud which is intended for contribution with data users. The user can decrypt the cipher text only if the attributes associated with the cipher text satisfy the tree access structure. Each file is encrypted by means of a key of symmetric data encryption which is consecutively encrypted by means of a public key that is equivalent to attributes set in key-policy attribute-based encryption [8]. Cipher texts are not encrypted towards individual user. Rather, both cipher texts and users' decryption keys are linked by features. If there is a competition among his key of decryption in addition to cipher text then only the user is capable to decrypt a cipher text. A scheme of hierarchical attribute-set-based encryption intended for access control in cloud computing was proposed which extends the encryption of attribute-set-based cipher text-policy by means of a hierarchical organization of system users, to achieve flexible, scalable and fine-grained access control [1]. The conventional method to defend perceptive data that is outsourced to third parties is to accumulate the data of encrypted on servers, although the decryption keys are revealed to approve users only. Depending on how attributes and policy are associated with cipher texts and users' decryption keys, attribute basis encryption schemes are classified into encryption of key-policy attribute-based and method of cipher text-policy attribute-based encryption [11]. A cipher text is connected by means of a set attributes set and a decryption key of user and is connected with a structure of monotonic tree access in a key policy encryption scheme. To accomplish flexible and managing of fine-grained access, a number of systems have been introduced in the recent times [6]. To access the shared data files, data users download the data files of encrypted of their concentration from the cloud and subsequently decrypt them [3]. Data privacy is not the only safety requirement. Access control is a standard defence issue and a variety of representations concerning access control have been projected. However these

systems are simply appropriate to systems in which owners of data and providers of service are within similar confidential province. In view of the fact that owners of data and providers of service are typically not in similar trusted field in cloud computing, a novel scheme of access control utilizing attributed-based encryption was introduced that assumes key-policy attribute-based encryption to put into effect the control of fine-grained access [14]. The cloud service provider is typically an industrial project that is not completely confidential as client encompass to surrender their information towards cloud service contributor in support of industry procedure in cloud computing. Data represents an exceptionally important advantage in support of any association; in addition to project client will face severe consequences if its private data is disclosed to their business competitors [9]. Thus, the cloud users will first wish for to making certain that their information are reserved secret towards outcast, as well as possible competitors. This is the first data safety requirement. For fuzzy identity-based encryption the notion of attribute based encryption was first introduced as a new method [7]. The main disadvantage of the scheme is that its threshold semantics lacks expressible. Service familiarized cloud representation was introduced, together with communications as a provision, proposal as a provision and Software as a provision.

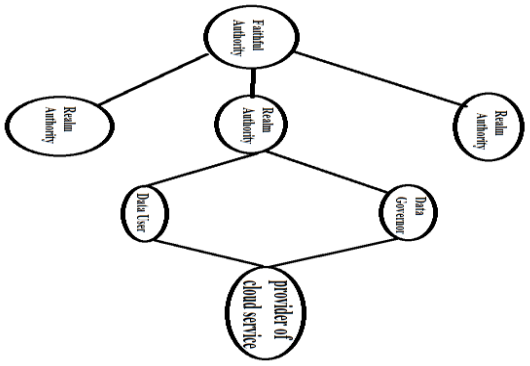

Fig 1: Model of Cloud Computing System

2. METHODOLOGY:

With cloud computing systems the enterprise users no longer need to spend in hardware or software systems, conversely, computing effectiveness offered by cloud system were obtainable at comparatively low worth [2]. Information security in addition to confidentiality is one of the important safety concerns in cloud system exceptional to its Internet basis information organization. Organization of attributes concerning user into a structure of recursive set was performed by hierarchical attribute-set-based encryption and allows users to compel dynamic limits on how those

attributes may possibly be combined to convince a policy as a result it can sustain attributes of compound and assignments of multiple numerical intended for a specified attribute suitably [16]. A realm authority is managed by its parent realm authority or the faithful authority. The file of encrypted data is accumulated with the equivalent attributes. If the connected attributes of a file that is stored up in the cloud convince the structure of access of a user's key, subsequently the user is competent in the direction of decrypting the encrypted, that is applied consecutively to decrypt the file. Although the immense benefits brought by cloud computing paradigm are stimulating for IT companies and possible cloud users, but safety problems in cloud computing has become serious problems which, without being properly addressed, will avert cloud computing wide-ranging applications and usage in the future [12]. Flexible and fine-grained access control is also strongly preferred in the service-oriented cloud computing model. The roles of cipher texts and decryption keys are switched as the cipher text is encrypted through a tree access strategy selected in a cipher text encryption scheme, while equivalent key of decryption is formed regarding several aspects [5]. Key is applied to decrypt cipher text is abstractly quicker towards conventional access control representation. System of cloud computing under contemplation comprises of five kinds of parties that is revealed in fig1 such as a provider of cloud service, data users, a number of realm authorities systems, data governors and a trustworthy authority [15]. To distribute decryption keys to authorized users requires an efficient key management mechanism, which has been proven to be very complex. To access the shared data files, data users download the data files of encrypted of their concentration from the cloud and subsequently decrypt them [10]. Intended for cloud computing an access control mechanism is proposed which is based on key-policy attribute-based encryption, jointly with a re-encryption technique for proficient user revocation.

3. RESULTS:

Hierarchical attribute-set-based encryption intended for access control in cloud computing organizes attributes of user into a structure of recursive set and allows users to compel dynamic limits on how those attributes may possibly be combined to convince a policy as a result it can sustain attributes of compound and assignments of

multiple numerical intended for a specified attribute suitably. Since owners of data and providers of service are typically not in similar trusted field in cloud computing, a novel scheme of access control utilizing attributed-based encryption was introduced that assumes key-policy attribute-based encryption to put into effect the control of fine-grained access. Hierarchical attribute-set-based encryption extends the encryption of attribute-set-based cipher text-policy by means of a hierarchical organization of system users, to achieve flexible, scalable and fine-grained access control. Cipher text-policy attribute-set-based encryption was extended with a structure of hierarchical towards effectively entrusts the trustworthy operation of authority's private attribute key generation towards lower-level domain authorities as a result, the workload of the trustworthy root authority is transferred towards domain authorities of lower-level, which can make available generations of attribute key intended for end users.

4. CONCLUSION:

System of cloud computing under contemplation comprises of five kinds of parties such as a provider of cloud service, data users, a number of realm authorities systems, data governors and a trustworthy authority.Access control is a standard defence issue and a variety of representations concerning access control have been projected. Hierarchical Attribute-set-based encryption extends the encryption of attribute-set-based cipher text-policy by means of a hierarchical organization of system users, to achieve flexible, scalable and fine-grained access control and organizes attributes of user into a structure of recursive set and allows users to compel dynamic limits on how those attributes may possibly be combined to convince a policy as a result it can sustain attributes of compound and assignments for a specified attribute.

REFERENCES:

[1] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in *Proc. ACM Conf. Computer and Communications Security (CCS)*, Alexandria, VA, 2005.

[2] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Chicago, IL, 2010.

[3] "HASBE: A Hierarchical Attribute-Based Solutionfor Flexible and Scalable Access Control in Cloud Computing", Zhiguo Wan, Jun'e Liu, and Robert H. Deng, 2012

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE*

INFOCOM 2010, 2010, pp. 534–542.

[5] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in *Proc. IEEE Symp. Security and Privacy*, Berkeley, CA, 2002.

[6] A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Proc. Acvances in Cryptology—Eurocrypt*, 2005, vol. 3494, LNCS, pp. 457–473.

[7] K. Barlow and J. Lane, "Like technology from an advanced alien culture: Google apps for education at ASU," in *Proc. ACM SIGUCCS User Services Conf.*, Orlando, FL, 2007.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, 2007.

[9] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Alexandria,VA, 2006.

[10] D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.

[11] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in *Proc.ESORICS*, Saint Malo, France, 2009.

[12] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in *Proc. IEEE Symp. Security and Privacy*, Berkeley, CA, 2003.

[13] R. Martin, "IBM brings cloud computing to earth with massive new data centers," *InformationWeek* Aug. 2008 [Online]. Available: http://www.informationweek.com/news/hardware/data_centers/209901523

[14] K. J. Biba, Integrity Considerations for Secure Computer Sytems The MITRE Corporation, Tech. Rep., 1977

[15] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/

[16] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Comput. Syst.*, vol. 25, pp. 599–616, 2009