International Journal for Rapid Research in Engineering Technology & Applied Science
ISSN (Online): 2455-4723
Vol 2 Issue 2 March 2016

Scalable Data Sharing in Cloud Storage Using Ciphertext Poling Attribute Base Encryption

Prajakta D.Patil[1], Chhaya Nayak[2]

Department of CSE, RGPV University, BM Technology, Madhya Pradesh Bhopal, India
Department of CSE, RGPV University, BM Technology, Madhya Pradesh Bhopal, India[2]
Prachipatil13@gmail.com[1],hod.computers@bmcollege.ac.in

Abstract -with the recent adoption and diffusion of the information sharing paradigm in distributed systems like online social networks or cloud computing, there are increasing demands and considerations for distributed knowledge security. One in every of the foremost difficult problems in knowledge sharing systems is that the social control of access policies and therefore the support of policies updates. With the event of cryptography, the attribute-based encoding (ABE) attracts widespread attention of the researchers in recent years. The ABE theme that belongs to the general public key encoding mechanism takes attributes as public key and associates them with the cipher text or the user's secret key. it's associate economical thanks to solve open issues in access management situations, as an example, the way to provide knowledge confidentiality and expressive access management at the same time. Cipher text policy attribute-based encoding (CP-ABE) is changing into a promising cryptologic answer to the current issue. It allows knowledge house owners to outline their own access policies over user attributes and enforce the policies on the information to be distributed.

Therefore, during this study, we have a tendency to propose a completely unique CP-ABE scheme for an information sharing system by exploiting the characteristic of the system design. The proposed scheme options the subsequent achievements: 1) the key written agreement drawback may well be solved by escrow-free key supplying protocol, that is made using the secure two-party computation between the key generation centre and also the data-storing centre, and 2) fine-grained user revocation per every attribute may be done by proxy cryptography that takes advantage of the selective attribute group key distribution on high of the ABE. The performance and security analyses indicate that the proposed scheme is economical to securely manage the data distributed within the data sharing system. Index Terms--Data sharing, attribute-based cryptography, revocation, access management, removing written agreement.

Keywords— Data sharing, attribute-based encryption,revocation, access control, removing escrow.

I. INTRODUCTION (HEADING 1)

With the development of the web and also the distributedcomputing technology, there is a growing demand for knowledge sharing and process in an open distributed computing atmosphere. RECENT development of the network and computing technology enables many of us to simply share their knowledge with others victimization on-line external storages. people will share their lives with friends by transferring their private photos or messages into the web social networks like Facebook and Myspace; or upload sensitive personal health records (PHRs) into online knowledge servers like Microsoft HealthVault, Google Health for easy sharing with their primary doctors or for price saving. As people enjoy the benefits of those new technologies and services, their issues concerning knowledge security and access management also arise. Improper use of the knowledge by the storage server or unauthorized access by outside users may be potential threats to their data. People would really like to make their sensitive or private knowledge only accessible to the authorized people with credentials them such as the knowledge supplier must provide communicatory access management and data confidentiality once human activity with customers. Recently, a lot of attention has been attracted by a

replacement public key primitive known as Attribute-based cryptography (ABE). ABE has important advantage over the standard PKC primitives because it achieves flexible one-to-many cryptography rather than one-to-one. ABE is visualised as an important tool for addressing the problem of secure and fine-grained knowledge sharing and access management. In an ABE system, a user is known by a collection of attributes. Attribute-based cryptography (ABE) may be a promising cryptographic approach that achieves a fine-grained knowledge access management [4], [5], [6], [7]. It provides some way of defining access policies supported completely different attributes of the requester, environment, or the information object. Especially, cipher text policy attribute-based cryptography (CP-ABE) enables an encryption to outline the attribute set over a universe of attributes that a descriptor has to possess so as to decrypt the cipher text, and enforce it on the contents [6]. Thus, every user with a completely different set of attributes is allowed to decrypt different items of information per the security policy. This effectively eliminates the requirement to accept the data storage server for preventing unauthorized data access, which is that the traditional access management approach of like the reference monitor. Traditionally, this kind of communicative access management is implemented by using a trusty server to store knowledge locally. The server is entrusted as a reference monitor that checks that a user presents proper certification before permitting him to access records or files. However, services are progressivelyStoring knowledge in a distributed fashion across many servers. Replicating knowledge across many locations has blessings in each performance and responsibility. The disadvantage of this trend is that it is progressively difficult to ensure the safety of knowledge using traditional methods; once data is hold on at many locations, the possibilities that one of them has been compromised will increase dramatically. For these reasons we would prefer to need that sensitive knowledge is stored in an encrypted kind so it will stay private even if a server is compromised. Fashionable distributed information systems need flexible access management models that transcend discretionary, necessary and role-based access management. Recently planned models, like attribute-based access management, outline access management policies supported completely different attributes of the requester, surroundings, or the information object. On the opposite hand, the present trend of service-based info systems and storage outsourcing need increased protection of information together with access management strategies that are cryptographically enforced. The concept of Attribute-Based Encryption (ABE) fulfils the same requirements. It provides a sublime method of encrypting information such the encrypted information such the attribute set that the descriptor must possess so as to decrypt the cipher-text. This is helpful for applications wherever the information provider knows specifically that user he needs to share with, in several applications the supplier can wish to share information according to some policy supported the receiving user's credentials.

II. LETERATURE SERVEY

ABE comes in two flavours known as key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, attributes are used to describe the encrypted information and policies are built into users 'keys; whereas in CP-ABE, the attributes area unit used to describe users 'credentials, and an encryptor determines a policy on who can decode the information. Between the two approaches, CP-ABE is a lot of acceptable to the information sharing system as a result of it puts the access policy selections within the hands of the information owners. Most of the present ABE schemes are created on the design wherever one trusty authority, or KGC has the facility to get the total private keys of users with its master secret information. Thus, the key written agreement drawback is inherent specified the KGC can decrypt each ciphertext self-addressed to users within the system by generating their secret keys at any time.

Junbeom Hur [1], planned CP-ABE schemes with slight changes in attribute instead of from the scratch and remove the matter that is encountered in Bethencourt et al. [5], like key written agreement and revocation. However during this system there is machine overhead.M. Chase and S.S.M. Chow [2], planned a distributed KP-ABE scheme that solves the key written agreement drawback in a multi-authority system. Most of the present ABE schemes are made on the design wherever one trusty authority, or KGC has the facility to come up with the total private keys of users with its master secret information. Thus, the key written agreement drawback is inherent specified the KGC can decrypt each ciphertext self-addressed to users in the system

by generating their secret keys at any time. One disadvantage of this type of totally distributed approach is the performance degradation. S.S.M. Chow [3], proposed an anonymous private key generation protocol in identity-based literature such that the KGC can issue a private key to an authenticated user without knowing the list of users 'identities. However, found that this can't be adapted to ABE systems thanks to primarily two reasons. First, in Chow's protocol, identities of users are not public any longer, a minimum of to the KGC, as a result of the KGC will generate users 'secret keys otherwise. Second, the collusion attack between users is that the main security threat in ABE.J. Bethencourt, A. Sahai, and B. Waters [4], and A.Boldyreva, V. Goyal, and V. Kumar [5], planned first key revocation mechanisms in CP-ABE and KP-ABE settings, respectively. These schemes change an attribute key revocation by encrypting the message to the attribute set with its validation time. These attribute-revocable ABE have the security degradation problem in terms of the backward and

Forward secrecy. N. Attrapadung and H. Imai [6], advised another user-revocable ABE schemes addressing the key revocation problem by combining broadcast cryptography schemes with ABE schemes. However, in this scheme, the information owner should take full charge of maintaining all the membership lists for every attribute cluster to enable the direct user revocation. This scheme is not applicable to the information sharing system, as a result of the data owners cannot be directly in control of information once storing their data to the secondary storage server. S. Yu, C. Wang, K. Ren, and W. Lou [7], recently addressed the user revocation within the ABE-based knowledge sharing system. During this scheme, the user revocation is completed exploitation proxy re-encryption by the information server. However, so as to revoke users, the KGC ought to generate all secret keys as well as the proxy key on behalf of the information server. Then, the server would re-encrypt the ciphertext beneath the proxy key received from the KGC to forestall revoked users from decrypting the ciphertext. Thus, the key written agreement drawback is additionally inherent during this theme. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati [8], planned an answer for securing outsourced knowledge on semi-trusted servers supported isobilateral key derivation strategies which might accomplish fine-grained access management. Sadly, the complexities of file creation and user grant/revocation operations area unit linear to the quantity of licensed users, that is less scalable. Shilpa Elsa Abraham and R. Gokulavanan [10], planned the system scalability is increased using ABE and MA-ABE. The expressibility of our encryptor's access policy is somewhat restricted by that of MA- BE's. In follow, the credentials from completely different organizations is also thought of equally effective, in this case distributed ABE schemes are going to be required. The subsequent drawbacks are characteristic from the present system. User identity bases access management mechanism is not supported underneath matters. Dynamic policy management is one more issue. Recently, the analysis community has planned Attribute-based cryptography (ABE) systems wherever cryptography and decryption are determined by the attributes of the info and also the recipients. An ABE cryptosystem is designed to change fine-grained access management of the encrypted information. It permits the encryptor to connect attributes or policies to a message being encrypted so only the receiver(s) World Health Organization is (are) appointed compatible policies or attributes will decrypt it.Formally, the attributes will be considered as Boolean variables with capricious labels, and also the policies are expressed as conjunctions and disjunctions of attribute variables.The ABE systems will be viewed as a generalization of Identity primarily based cryptography (IBE) systems [10]. In IBE systems, only one attribute is employed that is the identity of the receiver, whereas ABE systems modify the employment of multiple attributes at the same time. In fact, current ABE schemes are engineered by smartly combining the essential techniques of IBE with a linear secret sharing scheme. In these schemes, the access policies within the variety of a monotonic mathematician formula over the attribute variables [11]. There are two alternatives in imposing the access policy. The access policy will be embedded within the private key of a user, which ends in a very cryptosystem known as Key Policy ABE (KP-ABE) [11]. As an alternative, the access policy will be embedded within the ciphertext, which ends within the Ciphertext Policy ABE (CP-ABE) system. Both KP-ABE and CP-ABE systems make sure that a bunch of users cannot access any

unauthorized information by colluding with one another.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

PROPOSED SYSTEM

According to the present schemes, the functionalities in a perfect ABE scheme is listed as follows:

1. Information confidentiality: Unauthorized users UN agency don't have enough attributes satisfying the access policy should be prevented from accessing the plaintext of the information.Additionally, the KGC is not any longer totally trusty within the informationsharing system. Thus, unauthorized access from the KGC also because the data-storing centre to the plaintext of theencrypted information should be prevented.

2. Collusion resistance: Collusion resistance is one among the most necessary security property required in ABE systems [4], [5], [6]. If multiple users interact, they will be ready to decrypt a ciphertext by combining their attributes even though every of the users cannot decrypt the ciphertext alone. Do not want these colluders to be ready to decrypt the personal knowledge within the server by combining their attributes. Since we have a tendency to assume the KGC and data-storing centre are honest, contemplate any active attacks from them by colluding with revoked users as in [3],[12].

3. User/attribute revocation: If a user equal the system, the scheme will revoke his access right. Similarly, attributerevocation is inevitable.

4. Scalability: the quantity of licensed users cannot have an effect on the performance of the scheme. That is to mention, the scheme will modify the case that the quantity of the licensed users will increase dynamically.

Table 1: Comparision Table

Existing System	Proposed System
Accuracy is a smaller amount.	Accuracy is larger.
Precision is less.	Exactness is a lot of.
Security is a smaller amount.	Security is larger.

IV. PLANNED METHODOLOGY

The first CP-ABE scheme planned by Bethencourt et al. [5],which are principally motivated by a lot of rigorous security proof within the commonplace model. However, most of the schemes did not accomplish the quality of the Bethencourt et al. 'scheme. Therefore, during this planned, develop a variation of the CP-ABE algorithmic rule partly supported (but not restricted to) Bethencourt et al. 's construction so as to boost the quality of the access management policy rather than building a brand new CP-ABE scheme from scratch. The attribute primarily cryptography scheme is increased to handle distributed attribute based cryptography method. Information update and key management operations area unit tuned for multi user access surroundings. Its key generation procedure is changed for removing key written agreement. The planned scheme is then designed on this new CP-ABE variation by any desegregation it into the proxy

Re-encryption protocol for the user revocation. To handle the fine-grained user revocation, the information storing centre should get the user access (or revocation) list for every attribute cluster, since otherwise revocation cannot get in any case. This setting wherever the data-storing centre is aware of the revocation list doesn't violate the protection necessities, as a result of its only allowed to re-encrypt the ciphertexts and might by no means that get any info regarding the attribute keys of users. The two parties have interaction within the arithmetic 2PC protocol with master secret keys of their own, and issue independent key elements to users throughout the key supply section. The 2PC protocol deters them from knowing every other's master secrets in order that none of them will generate the complete set of secret keys of users on an individual basis. Thus, we have a tendency to take associate assumption that the KGC doesn't interact with the data-storing centre since they're honest.

1)*Key generation centre*: it is a key authority that generates public and secret parameters for CP-ABE. It is incharge of supply, revoking, and change

attribute keys for users. It grants differential access rights to individual users supported their attributes. That is, it will honestly execute the assigned tasks within the system; but, it might prefer to learn info of encrypted contents the maximum amount as potential. Thus, it ought to be prevented from accessing the plaintext of the encrypted information though it is honest.

2) Data-storing centre: it is an entity that gives an information sharing service. It is accountable of dominant the accesses

From outside users to the storing information and providing corresponding contents services. The data-storing canter isanother key authority that generates personalised user key with the KGC, and problems and revokes attribute group keys to valid users per every attribute, that are accustomed enforce a fine-grained user access management.

3) Information owner: it is a consumer WHO owns information, and desires to transfer it into the external data-storing centre for easy sharing or for price saving. An information owner is accountable for process (attribute-based) access policy, and implementing it on its own information by encrypting the information below the policy before distributing it.

4) User: it is associate entity WHO desires to access the information. If a user possesses a collection of attributes satisfying the access policy of the encrypted information, and is not revoked in any of the valid attribute teams, then he are going to be able to decrypt the ciphertext and acquire the information.

IV WORK DONE

In this section, we have a tendency to introduce input dataset, System demand and sensible atmosphere and results.

A. System Specification

For implementation we will be using hardware contents of Pentium – IV processor, has 1.1 GHz speed, RAM should be minimum 256 Mb and 20 GB Hard Disk to storage purpose. The implementation are done Java technology in NetBeans and Apache tomcat web server are used, for information storage of project MySQL information are often used. This can be compatible with any of windows XP/7/8/10.

B. Results of sensible Work

Practical work done is as shown in figure given below.Following figure shows the graphical representation of your time verses algorithms. Performance is computed in line with the time needed for set of transactions.

In fig 1. We have shown time comparison between existing and proposed within time needed for planned system is a smaller amount as compared to existing.

In fig 2. We have shown accuracy prediction i.e. thanks to introducing LTI accuracy are increases.

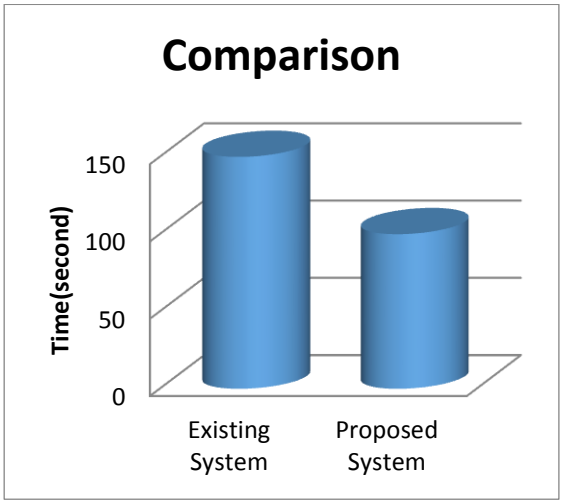

Fig 1. Time Comparison

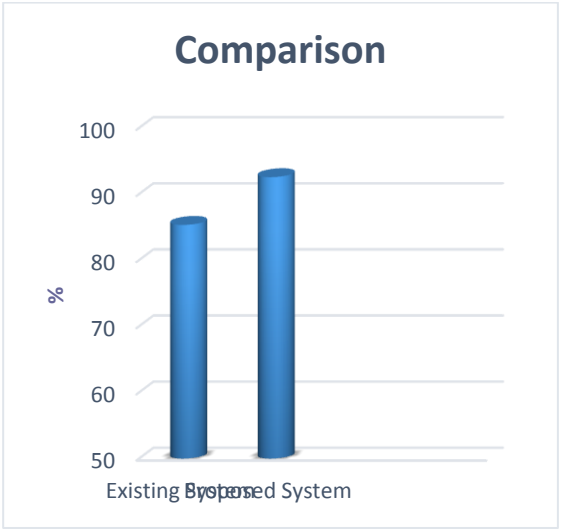

Fig 2. Accuracy Prediction

V. Conclusion and Future Work

In this paper we have a tendency to tend to studied on-line shortest path computation; supported the live traffic circumstances the shortest path results computed/updated. To the matter (due to their preventive maintenance time and large transmission overhead), we have a tendency to tend to carefully analyse the current work and discuss their irrelevancy. To affect the matter, we have a tendency to advise a promising style that broadcasts the index on the air. To work shortest path on a little portion of index, we have a tendency to tend to initial establish an important feature of the stratified index structure that allows us. In our resolution, LTI, This necessary feature is completely used. For on-line shortest path computation, our experiments confirm that LTI is also a Pareto optimum resolution in terms of 4 performance factors. Among the longer term, on time dependent networks, we are attending to extend our resolution depends not solely on current traffic info but put together supported the expected traffic circumstances, this may be a really interesting topic since the selection of a shortest path.

REFERENCES

[1] H. Bast, S. Funke, D. Matijevic, P. Sanders, and D. Schultes, "In Transit to Constant Time Shortest-Path Queries in Road Networks," Proc. Workshop Algorithm Eng. and Experiments(ALENEX), 2007.

[2] P. Sanders and D. Schultes, "Engineering Highway Hierarchies,"Proc. 14th Conf. Ann. European Symp. (ESA), pp. 804-816, 2006.

[3] G. Dantzig, Linear Programming and Extensions,series Rand Corporation Research Study Princeton Univ. Press, 1963.

[4] R.J. Gutman, "Reach-Based Routing: A New Approach to Shortest Path Algorithms Optimized for Road Networks," Proc. Sixth Workshop Algorithm Eng. and Experiments and the First Workshop Analytic Algorithmics and Combinatorics (ALENEX/ANALC),pp. 100-111, 2004.

[5] B. Jiang, "I/O-Efficiency of Shortest Path Algorithms: An Analysis,"Proc. Eight Int'l Conf. Data Eng. (ICDE), pp. 12-19, 1992.

[6] P. Sanders and D. Schultes, "Highway Hierarchies Hasten Exact Shortest Path Queries,"Proc. 13th Ann. European Conf. Algorithms(ESA), pp. 568-579, 2005.

[7] D. Schultes and P. Sanders, "Dynamic Highway-Node Routing," Proc. Sixth Int'l Conf. Experimental Algorithms (WEA), pp. 66-79,2007.

[8] F. Zhan and C. Noon, "Shortest Path Algorithms: An Evaluation Using Real Road Networks,"Transportation Science, vol. 32, no. 1,pp. 65-73, 1998.

[9] "Google Maps," http://maps.google.com, 2014.

[10] "NAVTEQ Maps and Traffic," http://www.navteq.com, 2014.

[11] "INRIX Inc. Traffic Information Provider," http://www.inrix.com, 2014.

[12] "TomTom NV," http://www.tomtom.com, 2014.

[13] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015," 2011.

[14] D. Stewart, "Economics of Wireless Means Data Prices Bound toRise," The Global and Mail, 2011.

[15] W.-S. Ku, R. Zimmermann, and H. Wang, "Location-Based Spatial Query Processing in Wireless Broadcast Environments,"IEEETrans. Mobile Computing, vol. 7, no. 6, pp. 778-791, June 2008.

[16] N. Malviya, S. Madden, and A. Bhattacharya, "A Continuous Query System for Dynamic Route Planning,"Proc. IEEE 27th Int'lConf Data Eng. (ICDE), pp. 792-803, 2011.

[17] G. Kellaris and K. Mouratidis, "Shortest Path Computation on AirIndexes,"Proc. VLDB Endowment, vol. 3, no. 1, pp. 741-757, 2010.

[18] Y. Jing, C. Chen, W. Sun, B. Zheng, L. Liu, and C. Tu, EnergyEfficient Shortest Path Query Processing on Air,"Proc. 19th ACM SIGSPATIAL Int'l Conf. Advances in Geographic Information Systems(GIS), pp. 393-396, 2011.

[19] R. Goldman, N. Shivakumar, S. Venkatasubramanian, and H. Garcia-Molina, "Proximity Search in Databases,"Proc. Int'l Conf. Very Large Databases (VLDB), pp. 26-37, 1998.

[20] N. Jing, Y.-W. Huang, and E.A. Rundensteiner, "Hierarchical Encoded Path Views for Path Query Processing: An Optimal Model and Its Performance Evaluation,"IEEE Trans. Knowledgeand Data Eng., vol. 10, no. 3, pp. 409-432, May 1998.

[21] S. Jung and S. Pramanik, "An Efficient Path Computation Model for Hierarchically Structured Topographical Road Maps," IEEE Trans. Knowledge and Data Eng., vol. 14, no. 5, pp. 1029-1046, Sept.2002.

[22] E.P.F. Chan and Y. Yang, "Shortest Path Tree Computation inDynamic Graphs,"IEEE Trans. Computers, vol. 58, no. 4, pp. 541-557, Apr. 2009.

[23] T. Imielinski, S. Viswanathan, and B.R. Badrinath, "Data on Air: Organization and Access,"IEEE Trans. Knowledge and Data Eng.,vol. 9, no. 3, pp. 353-372, May/June 1997.

[24] J.X. Yu and K.-L. Tan, "An Analysis of Selective Tuning Schemes for Nonuniform Broadcast," Data and Knowledge Eng., vol. 22,no. 3, pp. 319-344, 1997.

[25] A.V. Goldberg and R.F.F. Werneck, "Computing Point-to-PointShortest Paths from External Memory,"Proc. SIAM Workshop Algorithms Eng. and Experimentation and the Workshop Analytic Algorithmics and Combinatorics (ALENEX/ANALCO), pp. 26-40, 2005.

[26] M. Hilger, E. K€ ohler, R. M€ ohring, and H. Schilling, "Fast Point-toPoint Shortest Path Computations with Arc-Flags,"The Shortest Path Problem: Ninth DIMACS Implementation Challenge, vol. 74,pp. 41-72, American Math. Soc., 2009.

[27] A.V. Goldberg and C. Harrelson, "Computing the Shortest Path: Search Meets Graph Theory,"Proc. 16th Ann. ACM-SIAM Symp.Discrete Algorithms (SODA), pp. 156-165, 2005.

[28] D. Delling and D. Wagner, "Landmark-Based Routing in Dynamic Graphs,"Proc. Sixth Int'l Workshop Experimental Algorithms (WEA), pp. 52-65, 2007.