IJITKM 0973-4414
International Journal of IT & Knowledge Management (ISSN: 0973-4414) www.csjournals.com
Volume 11 • Issue 2 pp. 87-93 Jan 2018 - June 2018 Published on 12-04-18

Fine-Grained Data Access Control with Aspect of Time and Attribute for Time-Sensitive Cloud Data

Shaik Mohammed Zakir[1] and Md Ateeq Ur Rahman[2]
[1]Research Scholar, Dept. of Computer Science & Engineering, SCET, Hyderabad
[2]Professor and Head, Dept. of Computer Science & Engineering, SCET, Hyderabad

Abstract: Cloud computing has emerged collectively of the foremost powerful paradigms within the IT business in recent years. Since this new computing technology needs users to entrust their valuable information to cloud suppliers, there are increasing security and privacy issues on outsourced information. many schemes using attribute-based encoding (ABE) are projected for access management of outsourced information in cloud computing; but, most of them suffer from inflexibility in implementing complicated access management policies. The new paradigm of outsourcing knowledge to the cloud could be a ambiguous blade. On the one hand, it frees knowledge homeowners from the technical management, and is simpler for knowledge homeowners to share their knowledge with supposed users. On the opposite hand, it poses new challenges on privacy and security protection. to guard knowledge confidentiality against the honest-but-curious cloud service supplier, varied works are projected to support finegrained knowledge access management. However, till now, no schemes will support each fine-grained access management and time-sensitive knowledge publication. during this paper, by embedding timed-release cryptography into CP-ABE (Ciphertext-Policy Attribute-based Encryption), we tend to propose a brand new time and attribute factors combined access management on time-sensitive knowledge for public cloud storage (named TAFC). supported the projected theme, we tend to any propose associate economical approach to style access policies visaged with numerous access needs for time-sensitive knowledge.

in depth security and performance analysis shows that our projected theme ishighly economical and satisfies the protection needs for timesensitive knowledge storage publically cloud. so as to understand climbable, flexible, and fine-grained access management of outsourced information in cloud computing, during this paper, we have a tendency to propose graded attribute-set-based encoding (HASBE) by extending ciphertext-policy attribute-set-based encoding (ASBE) with a hierarchical data structure of users. The projected theme not solely achieves measurability attributable to its hierarchical data structure, however conjointly inherits flexibility and fine-grained access management in supporting compound attributes of ASBE. additionally, HASBE employs multiple price assignments for access expiration time to manage user revocation additional with efficiency than existing schemes. we have a tendency to formally prove the protection of HASBE supported security of the ciphertext-policy attribute-based encoding (CP-ABE) theme by Bethencourt and analyze its performance and process complexness. we have a tendency to implement our theme and show that it's each economical and versatile in managing access management for outsourced information in cloud computing with comprehensive experiments.

Index Terms: Cloud Storage, Access control, Time-sensitive data, Fine granularity.

I. INTRODUCTION

Cloud storage service has important benefits on each convenient knowledge sharing and price reduction. However, this new paradigm {of knowledge|of knowledge|of information} storage brings regarding new challenges regarding data confidentiality protection. knowledge are not any longer in knowledge owner's trustworthy domain, and he/she cannot trust the cloud server to conduct secure knowledge access management. Therefore, the secure access management drawback has become a difficult issue in cloud storage. There are various works on privacy conserving knowledge sharing in cloud supported varied cryptanalytic primitives, within which the schemes supported CP-ABE attract in depth attentions, since they will guarantee knowledge owner fine-grained and versatile access management of his/her own knowledge. However, these schemes confirm user's access privilege solely supported his/her inherent attributes with none different crucial aspects, like the time issue. In reality, the time issue sometimes plays a vital role in managing time sensitive knowledge (e.g. to publish a modern electronic magazine, to reveal a company's future business plan). once uploading time-sensitive knowledge to the cloud, the information owner might want totally different| completely different} users to access the content when different time. However, to the simplest of our data, existing CP-ABE based mostly schemes cannot meet such demand. To tackle the on top of issue of regular unleash, it's necessary to introduce an efficient theme, which is able to not unleash the information access privilege to supposed user till corresponding predefined time. A trivial answer is to go away knowledge homeowners to manually unleash the time-sensitive knowledge: The owner uploads the encrypted data beneath totally different policies at every unleash time, so supposed users cannot access the information till the corresponding time arrives. However, such answer restricts the owner to be on-line to repeatedly transfer the various secret writing versions of constant knowledge, that makes the information owner during a significant bother. From the attitude of cryptography, the goal of regular unleash will be achieved by Timed-Release secret writing (TRE). Rivest et al. have projected an efficient TRE theme, and it's been after introduced into totally different aspects, like searchable secret writing , proxy re-encryption , conditional oblivious transfer. during a TRE-based system, a trust time agent, instead of knowledge owner, will uniformly unleash the access privilege at every predefined time. Androulaki et al. have designed associate approach to comprehend time-sensitive knowledge access management in cloud. Whereas, this approach lacks fine graininess, which can leave the information homeowners associate unendurable burden during a large-scale system. Fan et al. have projected timed-release predicate secret writing for cloud computing. In their theme, every file will be tagged with only 1 unleash time purpose, that cannot unleash the access privilege of 1 file to totally different| completely different} supposed users at different time. a way to come through the capability of each timed-release associated fine-grained access management in cloud storage? a right away however naive methodology is to handle time as an attribute . However, unendurable range of time-related keys are going to be issued {to every |to every} user at each corresponding time, and this may give birth to significant overhead on each computation and communication. In existing literatures, Qin et al. have created a preliminary decide to integrate time with attributes. It solely addresses the problem that the attributes' life amount of every user could also be restricted by time. However, a additional sensible theme is that: every user with totally different |completely different} attribute sets can have different unleash time for constant file. Thus, the theme in cannot meet this necessary demand. during this paper, we tend to propose associate economical time and attribute factors combined access management theme for time-sensitive knowledge publically

cloud, named TAFC. Our theme has 2 necessary capacities: on one aspect, it inherits the property of fine graininess from CP-ABE; on the opposite aspect, by introducing the trapdoor mechanism, it additional has the feature of regular unleash from TRE. In our theme, the introduced trapdoor mechanism is just associated with the time issue, within which only 1 corresponding secret ought to be revealed at when to reveal the connected trapdoors. This makes our theme extremely economical, with solely very little additional overhead more to the first CP-ABE based mostly theme. th the most contributions of this paper will be summarized as follows: 1) To the simplest of our data, this paper is that the 1st at proposes 2 factors (time and attributes) combination based mostly access management theme in cloud storage, which might at the same time come through the options of fine graininess and regular unleash. 2) we tend to style an efficient design to comprehend our theme, within which we tend to plan associate entity (the central authority, CA) to be to blame for the timed-release perform. Besides distributing attribute-associated personal keys, CA solely has to sporadically publish universal time-related tokens to unleash access privileges. Such design occupies solely alittle quantity of price to produce our needed access management theme, that is cheap and worthy. 3) For the perform of regular unleash, there's no use of a secure tunnel between CA and also the knowledge owner. Thus, the extra overhead is light-weight.

II. Related Works

Cloud computing has emerged collectively of the foremost prestigious paradigms within the IT trade in recent years. Since this new computing technology needs users to entrust their valuable knowledge to cloud suppliers, there are increasing security and privacy considerations on outsourced knowledge. many schemes using attribute-based cryptography (ABE) are projected for access management of outsourced knowledge in cloud computing; but, most of them suffer from inflexibility in implementing advanced access management policies. so as to comprehend ascendable, flexible, and fine-grained access management of outsourced knowledge in cloud computing, during this paper, we tend to propose stratified attribute-set-based cryptography (HASBE) by extending ciphertext-policy attribute-set-based cryptography (ASBE) with a hierarchical data structure of users. The projected theme not solely achieves measurability owing to its hierarchical data structure, however additionally inherits flexibility and fine-grained access management in supporting compound attributes of ASBE. additionally, HASBE employs multiple worth assignments for access expiration time to upset user revocation additional with efficiency than existing schemes. we tend to formally prove the safety of HASBE supported security of the ciphertext-policy attribute-based cryptography (CP-ABE) theme by Bethencourt et al. and analyze its performance and procedure quality. we tend to implement our theme and show that it's each economical and versatile in addressing access management for outsourced knowledge in cloud computing with comprehensive experiments.

Cloud computing could be a new computing paradigm that's engineered on virtualization, parallel and distributed computing, utility computing, and service-oriented design. within the last many years, cloud computing has emerged collectively of the foremost prestigious paradigms within the IT trade, and has attracted in depth attention from each world and trade. Cloud computing holds the promise of providing computing because the fifth utility when the opposite four utilities (water, gas, electricity, and telephone). the advantages of cloud computing embrace reduced prices and capital expenditures, accrued operational efficiencies, measurability, flexibility, immediate time to promote, and so on. completely different service-oriented cloud computing models are projected, as well as Infrastructure as a Service

(IaaS), Platform as a Service (PaaS), and code as a Service (SaaS). varied business cloud computing systems are engineered at completely different levels, e.g., Amazon's EC2 , Amazon's S3 , and IBM's Blue Cloud square measure IaaS systems, whereas Google App Engine and Yahoo Pig square measure representative PaaS systems, and Google's Apps and Salesforce's client Relation Management (CRM) System belong to SaaS systems. With these cloud computing systems, on one hand, enterprise users not got to invest in hardware/software systems or rent IT professionals to keep up these IT systems, therefore they save value thereon infrastructure and human resources; on the opposite hand, computing utilities provided by cloud computing square measure being offered at a comparatively low worth in an exceedingly pay-as-you-use vogue.

2.1 Existing System

 All CP-ABE based mostly schemes alter information house owners to comprehend fine-grained and versatile access controlon their own information. However, CP-ABE determines users' access privilege based mostly solely on their inherent attributes with none different crucial factors, like the time issue.

 ABE-based access management schemes, in general, may be divided into 2 main categories: key-policy ABE (KP-ABE) {based|based mostly|primarily based mostly} schemes andciphertext-policy ABE (CP-ABE) based schemes , such as . The latter one is a lot of appropriate for achieving versatile and fine-grained access management for the general public cloud, within which every file is tagged with AN access structure.

 Goyal et al. and principle et al. have planned policy update strategies for KP-ABE {based|based mostly|primarily based mostly} and CP-ABE based schemes severally. In , if the info owner desires to unharness the access privilege to new sets of users, he/she doesn't ought to reencrypt and transfer the complete file.

2.2 Disadvantages:

 Existing ABE based mostly schemes don't supportthe situation wherever the access privilege of 1 file is needed tobe severally discharged to totally different sets of users once differenttime points.

 Yang'sscheme have simply mentioned the way to update the access structure,but not embedded the time issue into the access structure,which requires that the information owner should be on-line whenimplementing policy change.

III. PROPOSED SYSTEM

 In this paper, we tend to propose Associate in Nursing economical time and attribute factors combined access management theme, named TAFC, fortime-sensitive information publicly cloud. Our theme possesses 2 vital capabilities: 1) It inherits the property of fine

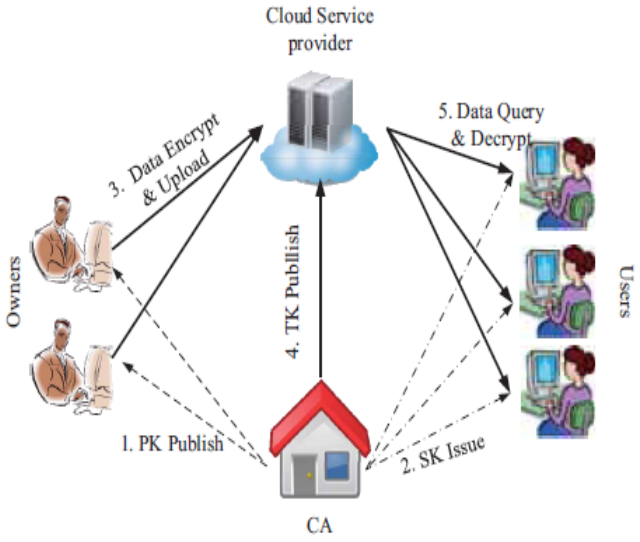
roughness from CP-ABE; 2) By introducing the trapdoor mechanism, it any retains the feature of regular unharness from TRE. Note that in TAFC, the introduced trapdoor mechanism is merely associated with the time issue, and only 1 corresponding secret must be printed once exposing the connected trapdoors. This makes our theme extremely economical, that solely brings concerning very little overhead to the first CP-ABE primarily based theme. we must always address a way to style Associate in Nursing economical access structure for whimsical access privilege construction with each time and attribute factors, particularly once Associate in Nursing access policy embeds multiple access privilege cathartic time points. As Associate in Nursing extension of the previous conference version , we tend to provide the potential sub-policies for time-sensitive information, and so presentan economical and sensible methodology to construct relevant access structures.

 The main contributions of this paper may be summarized as follows:

i. By group action TRE and CP-ABE publicly cloud storage, we tend to propose Associate in Nursing economical theme to understand secure finegrained access management for time-sensitive information. within the planned theme, the information owner will autonomously designate supposed users and their relevant access privilege cathartic time points. Besides realizing the operate, it isproved that the negligible burden is upon homeowners, users and also the trustworthy CA.

ii. we tend to gift a way to style access structure for any potential regular unharness access policy, particularly embeddingmultiple cathartic time points for various supposed users. To the most effective of our information, we tend to square measure the primary to check theapproach to style structures for general time-sensitive access necessities.

IV. System Architecture



A. System Model

As delineated in Fig. 1, the system consists of the subsequent entities: cloud service supplier (cloud), a central authority
(CA), many knowledge homeowners (owner), and plenty of knowledge shoppers

(user).• Cloud service supplier (cloud) includes the administrator of the cloud and cloud servers. The cloud stores a collection of information from homeowners, accepts transfer request from any users, similarly as helps homeowners and users conduct burdensome computations. • The central authority (CA) is accountable to manage
the security protection of the full system: It publishes system parameters and distributes personal keys related to specific attributes for every user. additionally, it acts as a time agent to publish the time-related secret
(denoted as time token, TK) at every pre-defined time (This will be simplified as a periodic operation). • the info owner (owner) decides the access policy based on attributes and unharness time, then encrypts the data underneath the policy before uploading it.
• the info client (user) is allotted a personal keyfrom CA. He/she will question any ciphertext keep in the cloud, however is in a position to rewrite it as long as he/she satisfies each of the subsequent constraints: 1) His/her attribute set satisfies the access policy; 2) this access time is later than the corresponding unharness time.

B. Security Model

In our access system, the cloud is assumed to be "honest-but-curious", that is comparable to most of the connected literatures within the topic of cloud secure storage [2–5]: On one hand, it offers reliable storage service and properly executes every computation mission for different entities; On the opposite hand, it should try and gain unauthorized info for its own benefits. on the far side the cloud, the full system consists of 1CA, many house owners and users, during which CA is assumed to be
fully-trust, whereas users will be malicious. CA is answerable for key distribution and time token business enterprise. we tend to assume that a malicious user might try and rewrite the ciphertext to get unauthorized knowledge by all means that, together with colluding with different users.

The planned TAFC will understand a fine-grained and timedrelease access management system: solely a user with happy attribute set will access the info when the designate time. The proposed theme is outlined to be compromised if either of
the following 2 varieties of users will with success rewrite the ciphertext:

1) A user whose attribute set doesn't satisfy the access policy of corresponding ciphertext;
2) A user World Health Organization tries
to access the info before the required unharness time, even if he/she has happy attribute set.

V. Conclusion

This paper aims at fine-grained access management for timesensitivedata in cloud storage. One challenge is to at the same time
achieve versatile regular unharness and fine roughness withlightweight overhead, that isn't provided in connected work.In this paper, we tend to propose a theme to attain this goal. Ourscheme seamlessly incorporates the conception of timed-release
encryption to the design of ciphertext-policy attributebasedencryption. With a suit of planned mechanisms, thisscheme provides knowledge house owners with the aptitude to flexiblyrelease the access privilege to totally {different|completely different} users at different time,according to a well-defined access policy over attributes andrelease time. The analysis shows that our theme will defendthe confidentiality of time-sensitive knowledge, with a light-weightoverhead on each CA and knowledge house owners, therefore well suits the practical large-scale access system for cloud storage. the HASBE theme for realizing ascendible, flexible, and fine-grained access control in cloud computing. The HASBE theme

seamlessly incorporates a data structure of system users by applying a delegation algorithmic rule to
ASBE. HASBE not solely supports compound attributes as a result of versatile attribute set combos, but conjointly achieves economical user revocation attributable to
multiple price assignments of attributes. we have a tendency to formally proved the safety of HASBE supported the safety
of CP-ABE by Bethencourt et al.. Finally, we implemented the planned theme, and conducted comprehensive performance analysis and analysis, which showed its potency and blessings over existing schemes.

References

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Instit. Standards Technol., vol. 53, no. 6, p. 50, 2009.
[1] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 743–754, 2012.
[2] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1790–1801, 2013.
[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.
[4] Z. Zhou, H. Zhang, Q. Zhang, Y. Xu, and P. Li, "Privacypreserving granular data retrieval indexes for outsourced cloud data," in *Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM2014)*, pp. 601–606, IEEE, 2014.
[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," in *Proceedings of the 2011 IEEE Global Communications Conference (GLOBECOM2011)*, pp. 1–5,
IEEE, 2011.
[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the 28th IEEE Symposium on Security and Privacy (S&P2007)*, pp. 321–334, IEEE, 2007.
[7] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 191–233, 2001.
[8] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," tech. rep., Massachusetts Institute of Technology, 1996.
[9] K. Yuan, Z. Liu, C. Jia, J. Yang, and S. Lv, "Public key timed-release searchable encryption," in *Proceedings of the 2013 Fourth International Emerging Intelligent Data and Web Technologies (EIDWT2013)*, pp. 241–248, IEEE, 2013.
[10] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Information Sciences*, vol. 258, no. 3, pp. 355–370, 2014.
[11] L. Xu, F. Zhang, and S. Tang, "Timed-release oblivious transfer," *Security and Communication Networks*, vol. 7, no. 7, pp. 1138– 1149, 2014.
[12] E. Androulaki, C. Soriente, L. Malisa, and S. Capkun, "Enforcing location and time-based access control on cloud-stored data," in *Proceedings of the 2014 IEEE 34th International Distributed Computing Systems (ICDCS2014)*, pp. 637–648, IEEE, 2014.
[13] C.-I. Fan and S.-Y. Huang, "Timed-release predicate encryption and its extensions in cloud computing," *Journal of Internet Technology*, vol. 15, no. 3, pp. 413–426, 2014.