International Journal of Applied Sciences, Engineering and Management
ISSN 2320 – 3439, Vol. 07, No.03, May 2018, pp. 109-116

Dynamic Access Control and Secure Data Storage in Cloud Computing using Hybrid Cryptography Framework

Mounika[1], K Sridhar[2]
[1]M. Tech Scholar, Department of CSE, Universal College of Engineering and Technology, Guntur, AP, India
[2]Assistant Professor, Department of CSE, Universal College of Engineering and Technology, Guntur, AP, India
Email id. sridhar.kdl@gmail.com [2]

Abstract: Reasoning processing has appeared as one of the most influential paradigms in the IT market recently. Since this new processing technological innovation needs customers to trust their valuable data to cloud suppliers, there have been improving protection and privacy issues on contracted information. Several techniques employing attribute-based protection (ABE) have been suggested for access control of contracted information in cloud computing; however, most of them experience from inflexibility in applying complicated accessibility control policies. In purchase to recognize scalable, versatile, and fine-grained access management of contracted information in cloud processing, in this document, we recommend Hybrid cryptographic system by improving cipher text-policy attribute-set-based encryption (ASBE) with a ordered framework of customers. The proposed scheme not only accomplishes scalability due to its ordered framework, but also gets versatility and fine-grained accessibility management in supporting substance features of ASBE. We apply our plan and display that it is both effective and versatile in working with accessibility management for outsourced data in cloud processing with extensive tests.
Index Terms. Cloud Computing, Attribute based encryption, Scalable and reliable data encryption and decryption, secure Hashing.

INTROUDCTION

Cloud computing depends on limiting sharing of resources to attain coherence and economies of scale, just like a utility (like the electricity grid) over a network. At the inspiration of cloud computing is that the broader construct of converged infrastructure and shared services. Cloud computing, or in easier shorthand simply "the cloud", additionally focuses on increasing the effectiveness of the shared resources. Cloud resources square measure sometimes not solely shared by multiple users however is dynamically reallocated per demand. this will work for allocating resources to users. for instance, a cloud laptop facility that serves European users throughout European business hours with a selected application (e.g., email) might apportion a similar resources to serve North Yankee users throughout North America's business hours with a unique application (e.g., an online server). This approach ought to maximize the utilization of computing power therefore reducing environmental harm likewise since less power, air-con, rack space, etc. square measure needed for a range of functions. With cloud computing, multiple users will access one server to retrieve and update their information while not buying licenses for various applications.

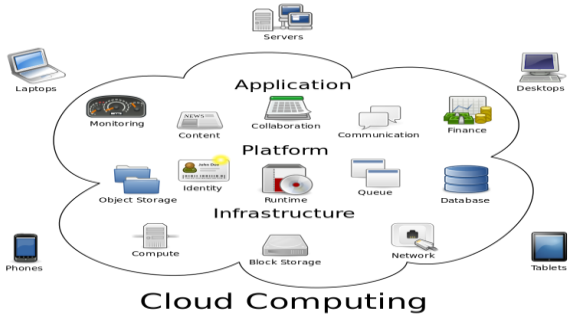

Fig.1. Cloud computing architecture regarding services. [1]

As shown in the above figure cloud computing provides three types of services regarding cloud service and other proceedings present in distributed computing operations. SAAS(Software As a Service), PAAS(Platform As a Service), and Infrastructure As a Service are three basic services of the cloud computing for storage data, processing data and maintains of data which includes all the activities of the users presentation may appears recent progression of data incentive application. Consider the examples of Mediafire.com, SendSpace.com and Amazon Cloud Web services and other services are storage of data in cloud and other proceeding website registration process. These are the sequential web sites for providing services to various users for storing their data processing application process. Reasoning contains share of solutions of details. All kinds of customer demands are implemented with

good performance and interaction expense contains high. Any customer can require any kind of sources to provide the solutions like pay per use manner requirements. Reasoning processing provides the solutions like endless sources of details. We are going to work on calculations sources requirements. In previous whenever to get more system fill to purchase the software and components procedure requirements procedure.

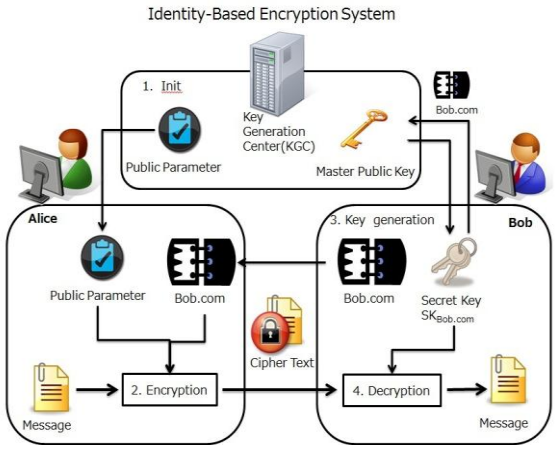

Fig.2. Attribute-Based-Encryption for secure storage in cloud computing [2].

Attribute-Based Encryption (ABE) allows only organizations having a specified set of features can decrypt cipher texts. ABE is appropriate to accessibility management such as the computer file discussing techniques, because several organizations can be provided for the decryption of a cipher text. We have been suggesting an enhanced ABE plan that is more effective than past one. Through present delegate calculations we are going to consume the solutions usage with new security difficulties execution procedure. In the storage space service program, the reasoning can let the customer, information proprietor to shop his information, and discuss this information with other customers via the reasoning, because the reasoning can provide the pay as you go atmosphere where people just need to pay the money for the storage space they use. For defending the privacy of the saved information, the information must be secured before posting to the reasoning. The security plan used is attribute-based security. The ABE plan used a customer's identification as features, and a set of features were used to secure and decrypt information. One of the main efficiency disadvantages of the most current ABE techniques is that decryption is costly for resource-limited gadgets due to coupling functions, and the number of coupling functions required to decrypt a cipher written text develops with the complexness of the accessibility plan. The ABE plan can outcome the issue that information proprietor needs to use every approved customer's community key to secure information. Key-policy attribute-based security (KP-ABE) plan designed the accessibility plan into the customer's personal key and described the secured information with customer's features. The KP-ABE plan can accomplish the grained accessibility management and more edibility to management customers than ABE plan. But the drawback of KP-ABE is that the accessibility plan is designed into an customer's personal key, so information proprietor can't choose who can decrypt the information except selecting a set of features which can explain this information. And it is inappropriate in certain program because a information proprietor has to believe in the key company. CP-ABE plan designed the accessibility plan into the secured data; a set of features is in a customer's key. The CP-ABE plan details the issue of KP-ABE that information proprietor only trusts the key company. To evaluate the efficiency of our ABE plan with proven contracted decryption, we apply the CP-ABE plan with proven contracted decryption and perform tests. In this paper we propose to develop Advanced Attribute Based Encryption will be applicable for constructing scalable and flexible and fine grained access control of out sourcing data in cloud computing. EABE expands the cipher text-policy attribute- set-based security (CP-ASBE, or ASBE for short) scheme by Bobba et al. [3] with a ordered structure of program customers, so as to accomplish scalable, flexible and fine-grained accessibility management. The participation of the document is multifold. First, we display how EABE expands the ASBE criteria with a hierarchical structure to enhance scalability and versatility while at the same time gets the function of fine-grained accessibility management of ASBE. Second, we illustrate how to apply a full-fledged access control plan for reasoning processing depending on EABE. The plan provides complete assistance for ordered customer allow, file creation, computer file removal, and customer cancellation in reasoning processing. Third, we officially confirm the protection of the suggested scheme based on the protection of the CP-ABE plan by Bethen-court et al. [4] and evaluate its efficiency with regards to computational overhead. Finally, we apply EABE and perform comprehensive experiments for efficiency assessment, and our experiments demonstrate that EABE has acceptable efficiency.

The remaining of this paper organized as follows: Section II provides overview of the related work presented in previous application procedures, In Section III present Traditional approach with security considerations; Section III describes effective data

presentation and construction of the proposed approach. Section IV analyze the security cloud with flexible and effective computation with real time performance evaluation and implementation. Section V describes concluded process of cloud security process.

LITERATURE REVIEW

In this section we describe the process of application, we evaluation the idea of attribute-based security (ABE), and offer a brief summary of the ASBE plan by Bobba et al. After that, we analyze current accessibility management techniques based on ABE. Attribute-Based Encryption The idea of ABE was first presented by Sahai and Rich waters [4] as a new means for unclear identity-based security. The main disadvantage of the plan in [4] is that its limit semantics does not have impressibility. Several initiatives followed in the literary works to try to fix the impressibility issue. In the ABE plan, cipher texts are not secured to one particular customer as in conventional community key cryptography. Rather, both cipher texts and users' decryption important factors are associated with a set of features or a plan over features. A customer is able to decrypt a cipher text only if there is a coordinate between his decryption key and the cipher text. ABE techniques are categorized into key-policy attribute-based security (KP-ABE) and cipher text-policy attribute-centered security (CP-ABE), based upon how features and plan are associated with cipher texts and users' decryption important factors. However, primary CP-ABE techniques (e.g., [5]) are far from enough to back up accessibility management in contemporary business surroundings, which need significant versatility and performance in specifying guidelines and handling customer features [4]. In a CP-ABE plan, decryption important factors only assistance customer features that are structured rationally as only one set, so customers can only use all possible mixtures of features in only one set released in their important factors to fulfill guidelines. To fix this issue, Bobba et al. [4] presented cipher text-policy attribute-set-based security (CP-ASBE or ASBE for short). ASBE is a prolonged way of CP-ABE which arranges customer features into a recursive set framework. The following is an example of a key framework of depth 2, which is the detail of the recursive set structure:

{Dept: CS, Role: Grand – Student,
{Course ID: 101, Role: TA,}
{Course ID: 525, Role: Grand-→Student}}

The above example symbolizes a key framework allocated to a graduate school student in CS division of an excellent, who is the TA for course 101 and has registered in course 525. It can be seen that the same function can be allocated several principles, e.g., the function "Role" is allocated value "TA" and "Grad-Student" in different places. This function provides ASBE more versatile and versatile in assisting many realistic circumstances. In this example, the graduate school student having such a personal key should not be able to merge the function "Role: TA" with "Coursed 525" so as to accessibility course qualities of other learners who enroll in course 525. Such a function cannot be applied with the original CP-ABE criteria.

The conventional technique to secure delicate information contracted to third events is to shop secured information on web servers, while the decryption keys are revealed to approve customers only. However, there are several disadvantages about this simple remedy. First of all, such a remedy needs an effective key management mechanism to spread decryption important factors to approved customers, which has been confirmed to be very challenging. Next, this strategy lacks scalability and flexibility; as the variety of approved customers becomes large, the remedy will not be effective any longer. In situation a previously genuine customer needs to be suspended, relevant information has to be re-encrypted and new important factors must be allocated to existing legitimate customers again. Last but not least, information entrepreneurs need to be online all time so as to secure or re-encrypt information and distribute keys to approve customers. This plan allows a information proprietor to assign most of the computational expense to reasoning web servers. The use of KP-ABE provides fine-grained accessibility management beautifully. Each data file is secured with a symmetrical information encryption key ( ), which is in convert secured by a community key corresponding to a set of features in KP-ABE, which is produced according to an accessibility framework.
Wang et al. [3] suggested ordered attribute-based encryption (HABE) to accomplish fine-grained accessibility management in cloud storage space solutions by mixing ordered identity-based encryption (HIBE) and CP-ABE. This plan also supports fine-grained accessibility management and completely assigning calculations to the reasoning suppliers. However, HABE uses disjunctive normal form plan and represents all features in one conjunctive clause are administrated by the same sector expert. Thus the same attribute may be administrated by several sector masters according to particular guidelines, which is challenging to implement in exercise. Furthermore, in contrast to ASBE, this scheme cannot assistance substance features effectively and does not support several value projects.

BACKGROUND APPROACH

Traditionally observe system specific management attribute based encryption outsourced schema was introduced In contrast to the design for common ABE, a KGSP and a DSP are furthermore engaged. . KGSP is to execute assisted key-issuing calculations to reduce AA fill in a range program when a huge variety of customers create demands on personal key generation and key-update. DSP is to finish assigned costly functions to get over the drawback that the decryption stage in common ABE needs a huge variety of excess functions at U.

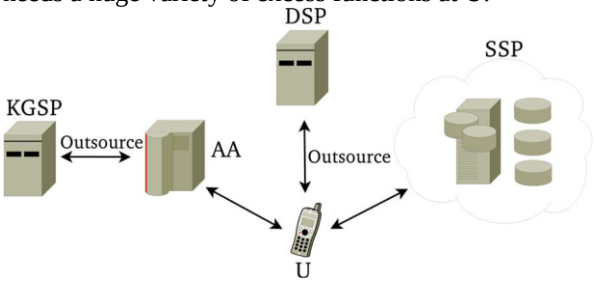

Fig.3. Data outsourcing model using ABE

Using some of the key presentation over estimated on the out sourcing data with representation of the encrypted key with data sharing and other sources using cloud computing secure services which includes commitment and other resource services. We signify (Ienc; Ikey) as the input to protection and key creation [13, 14]. In CP-ABE scheme, (Ienc; Ikey) = (w, A) while that is (w, A) in KPABE, where w and a feature set and accessibility framework, respectively. Then, in accordance with the suggested program design, we offer criteria explanations as follows:

Setup (μ): The installation criteria needs as input V a security parameter μ. It results a community key PK and a expert key MK.

. KeyGeninit (Ikey; MK) : For each user's personal key request, the initialization criteria for delegated key creation needs as input Van accessibility plan (or attribute set) Ikey and the expert key MK. It outputs the key couple (OKKGSP; OKAA).

KeyGenout (Ikey; OKKGSP): The assigned key generation algorithm needs as input the accessibility structure (or feature set) Ikey and the key OKKGSP for KGSP. It results a limited modification key TKKGSP.

KeyGenin (Ikey; OKAA): The within key generation algorithm needs as input the accessibility framework (or attribute set) Ikey and the key OKAA for attribute authority. It results another limited transformation key TKAA.

KeyBlind (TK): The modification key blinding algorithm needs as input V the modification key TK ¼ (TKKGSP; TKAA). It results a personal key SK and a distracted modification key f TK.

Encrypt (μM; Ienc): The protection criteria needs as input V a concept M and a feature set (or access structure) Ienc to be secured with. It results the cipher text CT.

Decryptout (CT; f TK) : The assigned decryption algorithm takes as input V a cipher text CT which was assumed to be secured under the feature set (or access structure) Ienc and the distracted transformation key f TK for accessibility framework (or feature set) Ikey. It outputs the partly decrypted ciphertext CTpart if (Ikey; Ienc) ¼ 1, otherwise results, where μ is a predicate predetermined.

Decrypt (CTpart; SK): The decryption criteria takes as inputVthe partly decrypted ciphertext CTpart and the personal key SK. It results the original message M.

Consider the above procedure of secure data outsourcing in cloud may perform efficient procedure for security in data proceeding of recent procedures. Secure outsourcing ABE system, which facilitates both protected contracted key-issuing and decryption. Our new technique offloads all accessibility plan and feature relevant functions in the key-issuing procedure or decryption to a Key Creation Support Company (KGSP) and a Decryption Support Company (DSP), respectively, making only a continuous number of simple functions for the feature power and qualified customers to execute regionally. Moreover, for the first time, we recommend an outsourced ABE development which provides check ability of the contracted calculations outcomes in an effective way. Extensive security and efficiency research display that the suggested techniques are confirmed protected and practical. Effective Hierarchal structure of the access control using attribute based encryption (ABE), better system was required for during above considerations effectively.

Enhanced Attribute Based Encryption

Consider procedure of the section II and section III, In this paper we propose to develop efficient realize scalable and flexible fine grained access control data outsourcing in cloud computing, in this section we propose to develop Enhanced Attribute Based Encryption based on hierarchal attribute set based security in out sourced data of cloud computing. The reasoning computing system under consideration consists of five types of parties: a reasoning support agency, information entrepreneurs, information customers, a number of sector regulators, and a reliable power. The reasoning support agency manages a reasoning to provide information storage support. Data entrepreneurs encrypt their information and store them in the reasoning for sharing with information customers. To access the shared information, information customers download

encrypted information of their interest from the reasoning and then decrypt them. Each information owner/consumer is administrated by a sector power. A sector power is managed by its parent sector power or the reliable power. [8][9] Data entrepreneurs, information customers, sector regulators, and the reliable power are organized in a hierarchical manner as shown in figure 4.

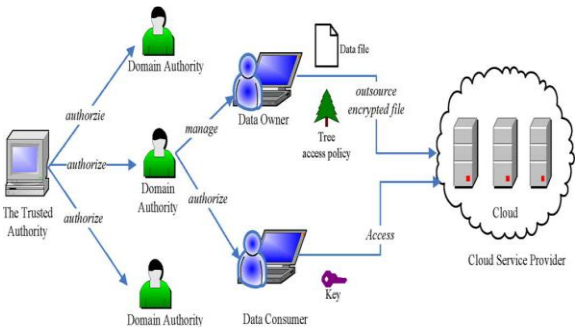

Fig.4. Architecture for developing Enhanced Attributed based encryption**.**

The reliable power is the main power and accountable for handling top-level sector regulators. Each top-level sector power matches to a top-level company, such as a federated business, while each lower-level sector power matches to a lower-level company, such as an associated company in a federated business. Information owners/consumers may match to workers in an company [16] . Each sector power is accountable for handling the sector regulators at the next stage or the information owners/consumers in its sector. In our system, neither data entrepreneurs nor data customers will be always on the internet. They come on the internet only when necessary, while the reasoning service agency, the reliable power, and sector regulators are always on the internet. The reasoning is believed to have numerous storage space potential and calculations power. In addition, we believe that data customers can access information for studying only.

Security Model Implementation

We believe that the reasoning server company is un-trusted in the feeling that it may collude with harmful customers (short for information owners/data consumers) to collect data file material saved in the reasoning for its own advantage. In the ordered framework of the system customers each celebration is associated with a community key and a personal key, with the latter being kept privately by the celebration.

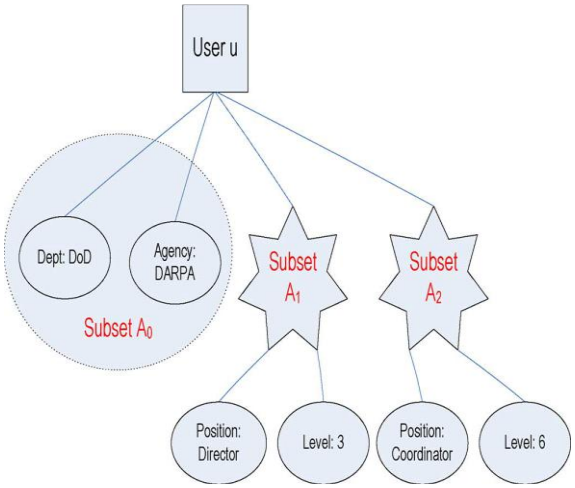

Fig.5. Example of key structure in hierarchal specification.

The reliable power functions as the main of believe in and allow the top-level sector regulators. [7] A sector power is reliable by its subordinate sector regulators or customers that it administrates, but may try to get the personal important factors of customers outside its sector. Users may try to accessibility information either within or outside the opportunity of their accessibility rights, so harmful customers may collude with each other to get delicate data files beyond their rights. Moreover to we believe interaction programs between all events with protected method framework. The procedure will follow efficient security communication. In our proposed work we implement key structure for user performance categorization in data accessing of cloud.

The detail of the key framework is the stage of recursions in the recursive set, similar to meaning of detail for a shrub. For a key framework with detail 2, associates of the set at detail 1 can either be feature components or places but associates of a set at detail 2 may only be feature components [14]. The key framework describes exclusive brands for places in it. For key structures of detail 2, just a catalog of the places at detail 2 is sufficient to exclusively recognize the places. Remember that our program design includes a reliable power, multiple sector regulators, and numerous customers corresponding to information owners and information customers. The reliable power is responsible for producing and circulating program factors and root master important factors as well as permitting the top-level sector regulators. A sector power is accountable for assigning keys to subordinate sector regulators at the next stage or customers in its sector. Each user in the program is allocated a key structure which identifies

the features associated with the user's decryption key.

Performance Evaluation & Implementation

In this area, we first evaluate theoretic calculations complexity of the suggested plan in each function. Then we implement an EASBE tool set in accordance with the tool set developed for CP-ABE. And perform a sequence of tests to evaluate efficiency of our suggested plan [14]. In this section we process performance evaluation and then implementation procedure for attribute based encryption in cloud computing.

Performance Evaluation

We evaluate the calculations complexness for each program operation in our plan as follows.

System Setup: When the program is set up, the reliable authority selects a bilinear team and some unique numbers. When keys are generated PK and MKo are produced, there will be several exponentiation functions. So the calculations complexity of Program Installation is O (1).

Top-Level Sector Power Grant: This operation is conducted by the reliable power. The master key of a sector power is in the form of $MK_i = (\mathbb{R}, D, D_{i,j}\ for a_{i,j} \in \mathbb{R}, E_i\ for A_i \in \mathbb{R}),$ where $\mathbb{R}$ is the key structure associated with a new domain authority, A_i is the set $\mathbb{R}$. Let N be the number of attributes in $\mathbb{R}$ and M be the number of sets in $\mathbb{R}$, then the combination of the procedure MK_i consists two exponential values for each attribute.

New User/Domain Power Allow. In this function, a new customer or new sector authority is associated with an attribute set, which is the set of that of the in the domain authority. The primary calculations expense of this operation is randomizing the key.

New Information file Creation: In this operation, the information owner needs to secure a computer file using the symmetrical key DEK and then encrypt DEK Using EABE. The complexity of encrypting the data file with DEK relies on the size of the data file and the actual symmetrical key security criteria.

Customer Cancellation: In this function, a sector power just maintains some condition details of users' important factors and assigns new value for expiry a chance to a user's key when updating it. When re-encrypting details, the details owner just needs two exponentiations for cipher text components associated with the expiration Time so the complexity of the operation is O(1).

Information file Access: In this function, we talk about the decrypting operation of secured information. A customer first obtains DEK with the decrypt algorithm and then decrypt the files using decrypted algorithm. We will talk about the calculations complexity of the Decrypt criteria [7]. The price of decrypting a cipher text varies based on the key used for decryption. Even for a given key, the way to fulfill the associated access tree may be various. The Decrypt criteria comprises of two coupling functions for every foliage node used to satisfy the shrub, one coupling for each converting node on the path from the foliage node used to the main and one exponentiation for each node on the direction from the foliage node to the root. So the calculations complexness differs based upon on the accessibility shrub and key framework. It should be mentioned that the decryption is conducted at the information consumers; hence, its computation complexness has little effect on the scalability of the overall program.

File Removal: This function is implemented at the demand of a information proprietor. If the reasoning can confirm the requestor is the owner of the information file, the reasoning removes the computer information file. So the computation complexness is O (1).

Implementation

We have applied a multilevel EABE tool set in accordance with the capable tool set from (http://acsc.csl.sri.com/cpabe/) developed for CP-ABE which uses the Pairing-Based Cryptography library (http://crypto.stanford.edu/pbc/). Then comprehensive experiments are performed on a laptop with dual-core 2.10-GHz CPU and 2-GB RAM, operating Ie8 10.04. We create an analysis on the trial information and provides the mathematical information.

EABE-setup: Produces a community key PK and an expert key MKo.

EABE-keygen: Given PK and MKo, generates a private key for a key framework. The key framework with detail 1 or 2 is reinforced.

EABE-keydel: Given PK and MKi of DA, delegates some areas of DA's personal important factors to a new customer or DA in its sector. The assigned key is comparative to generating private important factors by the main power.

EABE-keyup: Given PK, the personal key, the new attribute and the part, generates a new personal key which contains the new feature.

EABE-enc: Given PK, encrypts a computer file under an accessibility tree policy specified in a plan

terminology. **EABE-dec:** Given a personal key, decrypts a computer file.
EABE-rec: Given PK, a personal key and a secured computer file, re-encrypt the computer file. Observe that the personal key should be able to decrypt the secured file.

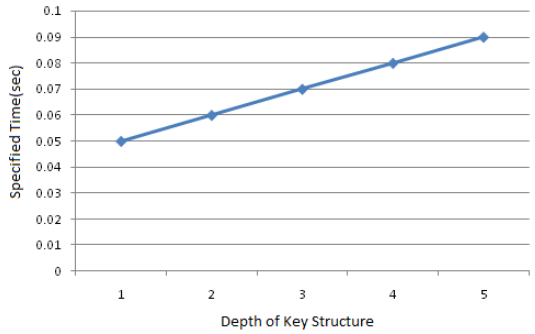

Fig.6. Experiments on program installation and top-level sector power allow. (a) Setup operation

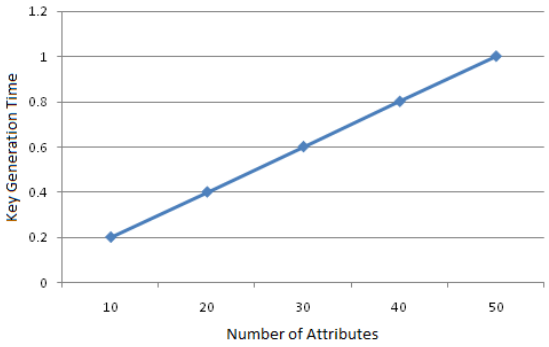

Fig.7. Experiments on program installation and top-level sector power allow. (b) Top-level sector power allow (the variety of subsets in the key framework is 1)

Our plan can be extended to assistance any detail of key framework. The price of this operation increases linearly with the key framework detail, and the installation can be finished in continuous here we are at a given detail. Except for this experiment, all other functions are examined with the key structure depth of 2. Top-Level Sector Power Allow is conducted with the command range device EABE-KeyGen. The price is identified by the variety of subsets and features in the key framework. When there is only one part in the key framework, the price grows linearly with the variety of features. While the variety of features in the key framework is set to be 50, the price also improves linearly with the variety of subsets as shown in the figure 6 and 7. With the control EABE-keydel, a site authority DA can execute New User/Domain Power Allow for a new user or another domain authority in his domain. The price relies upon on the variety of subsets and features to be assigned. Assume the domain authority DA has a personal key with 50 features. When DA wants to assign 45 of the features, the price grows linearly with the variety of subsets to be delegated.

CONCLUSION

In this we present EABE for realizing scalable, versatile, and fine-grained accessibility management in reasoning processing. Plan easily has a hierarchical structure of system customers by implementing a delegation algorithm to ASBE.EABE not only facilitates substance attributes due to versatile feature set mixtures, but also accomplishes efficient user cancellation because of several value projects of features. We officially shown the protection of EABE based on the protection of CP-ABE. Lastly, we implemented the suggested plan, and performed comprehensive performance research and assessment, which revealed its efficiency and advantages over current techniques. Further improvement of our suggested work will be developed in multiple customer accessibility management policy with real-time database integration in reasoning processing.

REFERENCES

[1]http://en.wikipedia.org/wiki/Cloud_computing#mediaviewer/File:Cloud_computing.svg.
[2]http://www.cipher.risk.tsukuba.ac.jp/?page_id=607&lang=EN.
[3] G.Wang, Q. Liu, and J.Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Chicago, IL, 2010.
[4] R. Bobba, H. Khorana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in *Proc. ESORICS*, Saint Malo, France, 2009.
[5] J. Bethen court, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, 2007.
[6] 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.
[7] Zhiguo Wan, Jun'e Liu, and Robert H. Deng," EABE: 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, April 2012.
[8] C. Gentry and A. Silverberg. Hierarchical ID-Based Cryptography. In *Proceedings of ASIACRYPT 2002*, pages 548-566.
[9] S. Muller, S. Katzenbeisser, and C. Eckert. Distributed Attribute-Based Encryption. In *Proceedings of ICISC2008*, pages 20-36.
[10] S. Yu, C. Wang, K. Ren, and W. Lou. Achieving Secure, Scalable, and Fine-grained Data Access

Control in Cloud Computing. In *Proceedings of IEEEINFOCOM 2010*, pages 534-542.
[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] A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Proc. Acvances in Cryptology—Eurocrypt*, 2005, vol. 3494, LNCS, pp. 457–473.
[13] 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.
[14] J. Lai, R. Deng, C. Guan, and J. Weng, ''Attribute-based Encryption with Verifiable Outsourced Decryption,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343-1354, Aug. 2013.
[15] 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.
[16] 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.
[17] 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.
[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, 2007.