Journal of Theoretical and Applied Information Technology
15th July 2016. Vol.89. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DYNAMIC ACCESS CONTROL POLICIES IN SECURE OUR SOURCED DATA IN CLOUD STOTAGE

[1]S.SAMPATH, [2]MR.B.TIRAPATHI REDDY

[1]Student, Department of CSE, KL University, Vaddeswaram, INDIA

[2]Associate Professor, Department of CSE, KL University, Vaddeswaram, INDIA

E-mail: [1]sampathsarnala@gmail.com, [2]tirapathireddyb@kluniversity.in

ABSTRACT

Cloud computing has emerged as maximum influential parameter in actual time IT enterprise in recent 12 Month's configuration for with appropriate occasions in allotted computing. Out sourced backup data in third birthday celebration cloud storage is a successful service to reduce statistics management costs and security concerns of integrity records of cloud statistics garage. Historically layout FADE (policy primarily based document assured Deletion), is a practical deployable of cloud garage machine in covered cloud facts. FADE is built upon trendy cryptographic techniques with outsourced facts in cloud storage system. FADE be afflicted by inflexibility in get entry to manipulate of out sourced data. As a way to recognize scalable and flexible with find grained get admission to manage in cloud computing. So on this paper we advise to develop Hierarchical attribute based Encryption (HASBE) by using extending cypertext guidelines with hierarchical shape of users. We enforce our software in each green and flexible in handling get entry to control in out sourced records in cloud computing with complete applications and experiments. Our experimental results display efficient get entry to control in consumer revocation and grant permission in real time evaluation of processing cloud packages.

Keywords: *Cloud computing, Attribute Based Encryption, Policy based file assured deletion, Prototype Implementation*.

1. INTRODUCTION

Cloud storage gives an abstraction of limitless storage space for clients to host information, in a pay-as-you-pass manner. as a result, in preference to self-keeping data facilities, groups can now outsource the storage of a bulk amount of digitized content material to those 1/three-birthday party cloud garage companies on the way to store the financial overhead in statistics control. However, privacy and integrity problems grow to be relevant as we now anticipate 0.33 parities to host possibly touchy statistics. To defend outsourced information a straightforward method is to use cryptography encryption onto touchy statistics with a hard and fast of encryption keys, but preserving and protective such encryption keys will create any other safety hassle.

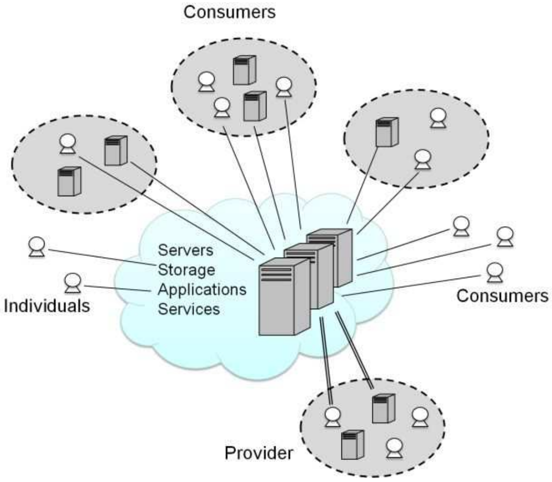

Figure 1: Cloud Computing Outsourced Data With Respect To Processing Data Integrity.

One particular difficulty is that upon requests of deletion of files, cloud garage providers might not completely get rid of all document copies (e.g., cloud garage companies may additionally moreover make a couple of report backup duplicate and distribute them over cloud for reliability, and clients do no longer recognize the amount or maybe the existence of these backup copies), and in the end have the information disclosed if the encryption keys are abruptly received, each with the aid of manner of accidents or via malicious assaults. FADE, a comfy overlay cloud storage machine that ensures record assured deletion and works seamlessly atop these days' cloud garage offerings. FADE decouples the look after encrypted information and encryption keys, such that encrypted data remains on zero.33-celebration (untrusted) cloud garage carriers, whilst encryption keys are independently maintained with the aid of a key supervisor provider, whose trustworthiness may be enforced the usage of a quorum scheme [12]. FADE generalizes time-based completely report confident deletion (i.e., files are generally deleted upon time expiration) right into a extra high-quality-grained method referred to as coverage based totally document confident deletion, wherein documents are related to extra bendy record get right of entry to hints (e.g., time expiration, read/write permissions of prison users) and are assuredly deleted when the related file get entry to guidelines are revoked and come to be out of date. Statistics confidentiality isn't always the best safety requirement. Flexible and great-grained get right of entry to manipulate is also strongly desired inside of the organization orientated cloud computing adaptation. A fitness-care records system on a cloud is needed to restriction get right of entry to of blanketed scientific records to eligible docs and a consumer relation control gadget walking on a cloud may additionally allow get right of access to of customer statistics to excessive-level executives of the agency handiest. In the ones instances, get admission to manipulate of sensitive statistics is both required by using manner of regulation (e.g., HIPAA) or organization recommendations.

On this paper, we endorse a hierarchical attribute-set-based encryption (HASBE) scheme for get access to manipulate in cloud computing. HASBE extends the cipher textual content-insurance characteristic- set-based totally completely encryption (CP-ASBE, or ASBE for quick) scheme via Bobba et al. [14] with a hierarchical shape of tool clients, if you want to accumulate scalable, flexiblem and great-grained get entry to manipulate. The contribution of the paper is multifold. First, we display how HASBE extends the ASBE algorithm with a hierarchical shape to improve scalability and flexibility at the equal time as at the same time inherits the function of superb-grained get entry to manipulate of ASBE. Second, we display the manner to put into effect a full-fledged get entry to control scheme for cloud computing based totally on HASBE. The scheme offers complete aid for hierarchical person furnish, document introduction, record deletion, and individual revocation in cloud computing.

The remainder of this paper proceedings as follows: Section II describes related work behind privacy and auditability in cloud data sharing. Section III defines FADE and its implementation in secure outsourced data in cloud. Section IV describes HASBE frame work and its implementation in privacy for access control policy in outsourced data. Section V defines experimental evaluation with comparison of FADE and HASBE in data security of outsourced cloud data storage. Section VI concludes overall conclusion in auditable secure cloud data.

2. RELATED WORK

Cryptographic protection on outsourced records garage has been consider. As an instance, Wang et al. [13] propose secure outsourced facts get admission to mechanisms that aid modifications in patron access rights and outsourced information. Ateniese et al. [4] and Wang et al. [12] propose an auditing system that verifies the integrity of outsourced data. However, all of the above structures require new protocol help at the cloud infrastructure, and such extra functionalities might also make deployment greater difficult. Safety answers which can be compatible with existing public cloud storage services had been proposed. Yun et al. [24] advocate a cryptographic report system that gives privacy and integrity guarantees for outsourced information using a ordinary hash based totally MAC tree. They prototype a device which can have interaction with an un-depended on storage server thru a modified report system. Jungle Disk [7] and Cumulus [21] are proposed to shield the privacy of outsourced data, and their implementation use Amazon S3 [2] because the garage again-forestall. Specially, Cumulus focuses on making powerful use of storage area at the same time as supplying essential encryption on outsourced information. The above structures mainly placed the protocol functionalities at the customer side, and the cloud storage carriers really offer the garage region. Attribute-based totally Encryption

The belief of ABE was first introduced through Sahai and Waters as a cutting-edge method for fuzzy identification-based totally definitely encryption. The number one drawback of the scheme in [20] is that its threshold semantics lacks expressibility. Several efforts located in the literature to try and clear up the impressibility problem. In the ABE scheme, cipher texts are not encrypted to as a minimum one precise customer as in traditional public key cryptography. As a substitute, each cipher texts and clients' decryption keys are associated with a hard and fast of attributes or a coverage over attributes. A consumer is capable of decrypt a cipher textual content simplest if there can be a in shape among his decryption key and the cipher textual content. ABE schemes are classified into key-coverage attribute- based encryption (KP-ABE) and cipher text-insurance feature- based encryption (CP-ABE), depending how attributes and coverage are associated with cipher texts and customers' decryption keys.

In a KP-ABE scheme [16], a cipher textual content is associated with a fixed of attributes and a person's decryption key is associated with a monotonic tree get admission to structure. Satisfactory if the attributes associated with the cipher text satisfy the tree get right of entry to structure, can the client decrypt the cipher text. In a CP-ABE scheme [14], the jobs of cipher texts and decryption keys are switched; the cipher textual content is encrypted with a tree get entry to insurance selected by using manner of an encryptor, even as the corresponding decryption secret is created with respect to a fixed of attributes. So long as the set of attributes related to a decryption key satisfies the tree access policy related to a given cipher textual content, the critical component can be used to decrypt the cipher textual content. Considering customers' decryption keys are related to a set of attributes, CP-ABE is conceptually closer to traditional get right of entry to manipulate models along with function-primarily based completely get admission to govern (RBAC) [12]. Therefore, its miles extra natural to apply CP-ABE, in desire to KP-ABE, to put into effect get proper of entry to manipulate of encrypted records.

3 .POLICY BASED SECURE ENCRYPTION

To manage the cryptographic key operations that empower document assured deletion. We first evaluation time-based totally report confident deletion. We then provide an explanation for how it could be prolonged to coverage-primarily based definitely file assured deletion.

Background

Time-based totally report assured deletion, that's first introduced in [14], way that files can be securely deleted and stay absolutely inaccessible after a predefined length. The main idea is that a document is encrypted with a statistics key, and this data key is similarly encrypted with a manage key that is maintained with the aid of a separate key supervisor service (known as Ephemerizer [14]). In [14], the manipulate secret's time-based totally, which means that it is going to be completely removed through the crucial factor manager while an expiration time is reached, wherein the expiration time is genuine when the record is first declared. Without the manipulate key, the facts key and as a end result the data record stay encrypted and are deemed to be inaccessible.

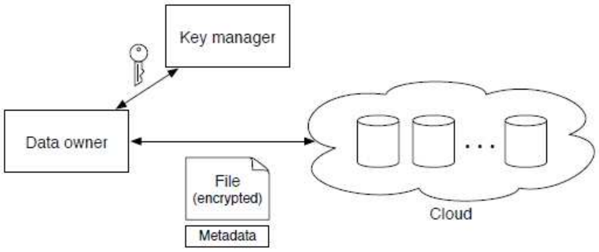

Figure 2: Fade Design For Out Sourced Encoded Data.

As a result, the primary safety belongings of document confident deletion is that regardless of the fact that a cloud company does no longer remove expired document copies from its garage, those documents live encrypted and unrecoverable.

Policy-based Deletion

We companion every record with a unmarried atomic report get entry to coverage (or policy for brief), or greater generally, a Boolean combination of atomic guidelines. Every (atomic) coverage is related to a control key, and all the manipulate keys are maintained via the crucial thing manager. just like time-primarily based completely deletion, the document content material is encrypted with a facts key, and the records secret's in addition encrypted with the manage keys similar to the coverage aggregate. While a coverage is revoked, the corresponding manage key can be eliminated from the important thing manager. therefore, whilst the policy aggregate related to a record is revoked and no longer holds, the records key and for this reason the encrypted content material of the record cannot be recovered with the manipulate keys of the recommendations. In this situation, we say the document is deleted.

Contributors in the System

Our tool is composed of three people: the facts proprietor, the vital component supervisor, and the storage cloud. They're described as follows.

Facts Proprietor: The records proprietor is the entity that originates record statistics to be saved at the cloud. it may be a file system of a pc, a consumer-diploma software program, a mobile device, or perhaps within the form of a plug-in of a purchaser software.

Key Manager: The critical thing manager continues the coverage-primarily based manage keys which may be used to encrypt statistics keys. It responds to the information owner's requests by way of performing encryption, decryption, renewal, and revocation to the manipulate keys.

Garage Cloud: The garage cloud is maintained by means of a 3rd-party cloud company (e.g., Amazon S3) and continues the facts on behalf of the information proprietor. We emphasize that we do no longer require any protocol and implementation adjustments at the storage cloud to help our system. Even a naive garage issuer that truly gives record upload/down load operations can be suitable.

A file is deleted (or permanently inaccessible) if its policy is revoked and becomes obsolete, right here, we expect that the manage key related to a revoked insurance is reliably eliminated by way of the vital element manager. Accordingly, via confident deletion of documents, we recommend that any present report copy which can be associated with revoked guidelines will continue to be completely encrypted and unrecoverable. The critical element manager may be deployed as a minimally trusted 1/3-birthday celebration provider. Thru minimally trusted, we imply that the essential issue supervisor reliably gets rid of the manipulate keys of revoked recommendations. But that may, it as crucial variable manager may be compromised. In this example, an attacker can get better the documents which might be associated with gift active guidelines. But, files which can be related to revoked guidelines though continue to be inaccessible, because the manage keys are removed. Ultimately, document confident deletion is accomplished.

4. HASBE ARCHITECTURE FOR ACCESS CONTROL POLICY

As depicted in Fig. 3, the cloud computing gadget beneath attention includes five forms of events: a cloud carrier provider, facts proprietors, information customers, some of place government, and a depended on authority. The cloud provider business enterprise manages a cloud to offer information storage provider. Information owners encrypt their facts documents and keep them inside the cloud for sharing with statistics purchasers. To access the shared facts files, statistics consumers down load encrypted statistics documents of their hobby from the cloud after which decrypt them. Every records proprietor/customer is administrated by using a domain authority. a domain authority is managed thru its parent domain authority or the depended on authority. Records proprietors, statistics customers, region authorities, and the relied on authority are organized in a hierarchical way as shown in Fig. 3

.

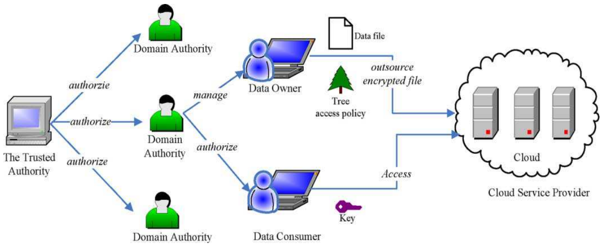

Figure 3: System Architecture For Access Control Policy.

The depended on authority is the basis authority and chargeable for coping with top-degree area government. Every top-level domain authority corresponds to a top-level corporation, in conjunction with a federated enterprise company, even as each lower-degree domain authority corresponds to a lower-stage business enterprise, which includes an affiliated organization in a federated organization. Information proprietors/customers may additionally correspond to personnel in a corporation. Every location authority is answerable for managing the area authorities at the subsequent level or the records owners/clients in its domain. In our system, neither facts proprietors nor facts customers can be normally online. They arrive on line simplest even as important, even as the cloud company issuer, the relied on authority, and place authorities are continuously online. The cloud is concept to have plentiful garage capacity and computation energy. In addition, we count on that information customers can access statistics files for reading best.

Protection Version

We count on that the cloud server organization is untrusted in the experience that it can collude with malicious clients (brief for information proprietors/records customers) to harvest report contents stored within the cloud for its very own advantage. Within the hierarchical shape of the device clients given in Fig. 1, each birthday celebration is related to a public key and a personal key, with the latter being stored secretly by using the birthday celebration. The relied on authority acts as the idea of believe and authorizes the pinnacle-diploma region government. A website authority is relied on by the use of its subordinate area government or customers that it administrates, but can also try to get the personal keys of clients outdoor its area. Customers may additionally try to get admission to statistics documents both within and outside the scope of their access privileges, so malicious customers may also additionally collude with every other to get touchy documents beyond their privileges. Similarly, we assume that conversation channels between all events are secured the use of well-known protection protocols, collectively with SSL.

5. SYSTEM IMPLEMENTATION

We analyze the computation complexity for every system operation in our scheme as follows.
System Setup. Whilst the gadget is installation, the trusted authority selects a bilinear institution and a few random numbers. Whilst PK and MK0 are generated, there might be several PK exponentiation operations. So the computation complexity of machine Setup is O (1).

Pinnacle-level area Authority provide. This operation is finished by means of the trusted authority. The grasp key of a website authority is in The shape of

$$MK_i = (A, D, D_{i,j}, D^{'}_{i,j} fora_{i,j} \in A, E_i forA_i \in A)$$

, wherein is the key shape associated with a new area authority, is the set of A. Allow be the wide variety of attributes in , and be the range of devices in then the computation of includes exponentiations for every attribute in , and one exponentiations for every set in .
New person/vicinity Authority grant. In this operation, a brand new character or new domain authority is associated with a characteristic set, that's the set of that of the top level region authority. The precept computation overhead of this operation is randomizing the crucial component.

New Report Introduction

In this operation, the information proprietor wishes to encrypt a facts document the use of the symmetric key and then encrypt the usage of HASBE. The complexity of encrypting the information record with relies upon on the size of the information report and the underlying symmetric key encryption set of policies. Encrypting with a tree get right of entry to shape consists of exponentiations in step with leaf node in and one exponentiation in step with translating node in.

User Revocation

In this operation, an internet site authority just continues some use records of customers' keys and assigns new charge for expiration time to a consumer's key at the same time as updating it. Even as re-encrypting records documents, the records owner clearly needs two exponentiations for cypertext components related to the feature. So the computation complexity of this operation is i. File get entry to. In this operation, we speak the decrypting operation of encrypted facts files. a person first obtains with the set of rules after which decrypt statistics documents using . We're able to talk the computation complexity of the set of rules. The value of decrypting a cypertext varies relying on the vital thing used for decryption. Even for a given key, the manner to meet the associated get entry to tree can be various. The algorithm consists of pairing operations for each leaf node used to satisfy the tree, one pairing for every translating node at the route from the leaf node used to the foundation and one exponentiation for every node on the route from the leaf node to the basis. So the computation complexity changes depending upon the access tree and key structure. It have to be said that the decryption is completed on the facts clients; consequently, its computation complexity has little effect on the scalability of the general machine.

File Deletion

This operation is finished on the request of a information proprietor. If the cloud can affirm the requestor is the owner of the record, the cloud deletes the data report. So the computation complexity is . Computation complexity of each machine operation, in which denotes the wide variety of attributes inside the key shape, is the function set of the facts record, is the set of leaf nodes of the get admission to tree or policy tree, and is the set of translating nodes of the coverage tree.

6. EXPERIMENTAL EVALUATION

We've got implemented a multilevel HASBE toolkit primarily based on the toolkit (http://acsc.csl.sri.com/cpabe/) superior for CP-ABE [18] which makes use of the Pairing-based Cryptography library (http://crypto.stanford.edu/percentage/). Then complete experiments are executed on a laptop with dual middle 2.10-GHz CPU and a couple of-GB RAM, walking Ubuntu 10.04. We make an assessment on the experimental statistics and provide the statistical data. Similar to the toolkit, our toolkit also affords a range of command line gear as follows:

Hasbe-setup: Generates a public key PK and a master key MK

Hasbe-keygen: Given PK and MK, generates a non-public key for a key shape. The critical thing shape with depth 1 or 2 is supported.

Hasbe-keydel: Given PK and MK of DA, delegates some components of DA's personal keys to a state-of-the-art person or DA in its region. The delegated secret is equivalent to producing personal keys through the basis authority.

Hasbe-Keyup: Given PK, the non-public key, the brand new function and the subset, generates a brand new personal key which includes the trendy attribute.

Hasbe-Eni: Given PK, encrypts a file underneath an access tree coverage laid out in a policy language.

Hasbe-Dec: Given PK a non-public key, decrypts a record. Hasbe-rec: Given, a non-public key and an encrypted file, re-encrypt the file. Phrase that the non-public key ought with the intention to decrypt the encrypted document.

The time required to setup the device for a one-of-a-kind intensity of key form. Our scheme can be extended to assist any depth of key shape. The cost of this operation will increase linearly with the important thing structure intensity, and the setup can be completed in consistent time for a given depth. Except for this check, all other operations are tested with the critical aspect shape depth of, top-stage area Authority grant is completed with the command line device. The fee is decided thru the range of subsets and attributes inside the key shape. At the same time as there may be simplest one subset in the key shape, the rate grows linearly with the quantity of attributes at the same time as the variety of attributes within the key shape is constant to be 50, the fee moreover will increase linearly with the quantity of subsets. Results of those two figures agree to the theoretic evaluation. With the command, a site authority DA can perform new man or woman/location Authority supply for a modern man or woman or each different area authority in his domain. The price is predicated upon on the range of subsets and attributes to be delegated. Count on the area authority DA has a non-public key with 50 attributes. At the same time as DA wants to delegate 45 of the attributes, the fee grows linearly with the quantity of subsets to be delegated. The comparison outcomes perform green valuables with admire to variety of key structure as shown in table 1.

Number of Arts in Key Structure	FADE	HASBE
1	1.254	0.945
2	1.568	0.856
3	1.785	1.245
4	2.145	1.956
5	2.845	2.145
6	3.452	2.405

Table 1: Comparison Results Of FADE And HASBE With Respect To Key Structure.

Customer Revocation operation consists of steps: Key replace and facts Re-encryption. Key update is applied with the command. The foundation authority or area authority can assign a new feature to the user or location authority. which include a modern-day attribute to at the least one subset of private key can be completed in constant time because the complexity due to processing values as shown event generations in facts and its graphical representation as proven in discern four . If the latest function needs to be assigned to numerous subsets, the price is linear with the extensive type of the subsets. Statistics Re-encryption is performed with the command.

No. of Attributes	HASBE	FADE
10	0.095	0.24
20	0.2	0.78
30	0.75	0.98
40	0.98	1.24
50	1.51	1.85
60	2.13	2.34

Figure4: Comparison Results With Respect To Key Generation And Arts In Key Structure

.

The data proprietor can re-encrypt the information record. for instance, there may be an encrypted file named that is encrypted with a policy and the statistics owner re-encrypts it with the command - then the new encrypted records file is related to a policy and, whilst a consumer is revoked, the associated facts document may be re-encrypted in this manner, and the new attributes can be assigned to valid person with command. Table 2 shows comparison results with respect to time in user proceedings.

The value of operation statistics Re-encryption relies upon on the number of attributes at the get admission to tree, that's same because the encryption operation, so we do no longer provide the evaluation right here.

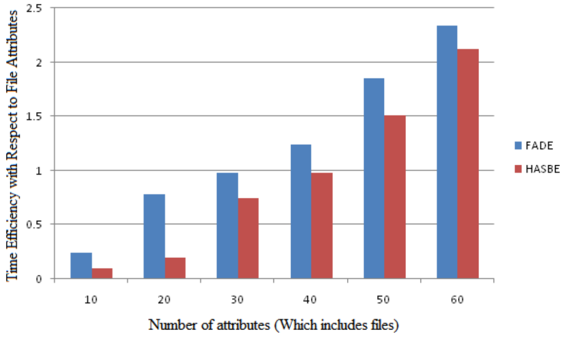

Figure 5: Time Comparison Results With Respect To File Attributes.

The information proprietor can use the command to encrypt a file to create a brand new encrypted record.

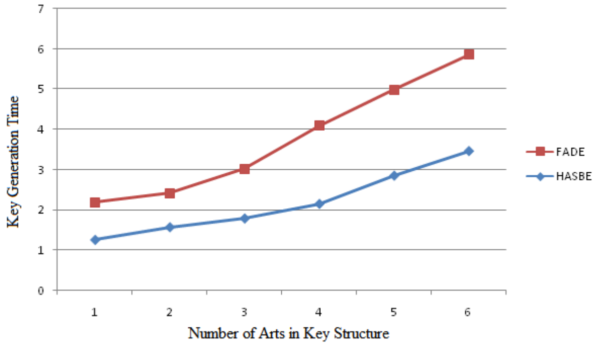

Table 2: Time Comparison Results With Respect To File Attributes.

The time for this operation relies upon at the get proper of access to tree form. In line with the huge type of leaf nodes and the extent of the get right of entry to tree coverage to get right of access to the record, decryption ought to be performed with the command. The time of decryption is unique relying at the access tree and key structure. Proper here we assume that there's just 1 subset with 50 attributes inside the key shape associated with the private key.

7. CONCLUSION

We present the layout of coverage-based record confident deletion, in which files are usually deleted and made unrecoverable through all of us at the same time as their associated file get right of entry to rules are revoked. We present the essential operations on cryptography keys as a way to achieve policy-primarily based file confident deletion. For presenting efficient get proper of access to control insurance in outsourced statistics , in this paper, we delivered the HASBE scheme for information scalable, flexible, and fine-grained get proper of entry to manage in cloud computing. The HASBE scheme seamlessly contains a hierarchical shape of device customers via utilizing a delegation set of regulations to ASBE. HASBE now not handiest facilitates compound attributes due to flexible attribute set combos, however also achieves green consumer revocation due to multiple price assignments of attributes. We officially proved the safety of HASBE primarily based on the security of CP-ABE through the usage of Bettencourt et al.. in the long run, we carried out the proposed scheme, and achieved comprehensive standard performance assessment and evaluation, which showed its performance and blessings over existing schemes.

REFRENCES:

[1] Yang Tang†, Patrick P. C. Lee†, John C. S. Lui†, and Radia Perlman, “FADE: Secure Overlay Cloud Storage with File Assured Deletion”, proceedings in Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.

[2] Zhiguo Wan, Jun’e Liu, and Robert 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, APRIL 2012.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee,D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the Clouds: A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.

[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik. Scalable and Efficient Provable Data Possession. In Proc. of SecureComm, 2008.

[5]R. Geambasu, T. Kohno, A. Levy, and H. M. Levy. Vanish: Increasing Data Privacy with Self-Destructing Data. In Proc. of USENIX Security Symposium, Aug 2009.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Proc. of ACM CCS, 2006.

[7] JungleDisk. http://www.jungledisk.com/.

[8]S. Kamara and K. Lauter. Cryptographic Cloud Storage. In Proc. of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization, 2010.

[9] LibAWS++. http://aws.28msec.com/.

[10]A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, Oct 1996.

[11] MyAsiaCloud. http://www.myasiacloud.com/.

[12]S. Nair, M. T. Dashti, B. Crispo, and A. S. Tanenbaum. A Hybrid PKI-IBC Based Ephemerizer System. IFIP International Federation for Information Processing, 232:241–252, 2007.

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

[14] T. Yu and M. Winglets, “A unified scheme for resource protection in automated trust negotiation,” in *Proc. IEEE Symp. Security and Privacy*, Berkeley, CA, 2003.

[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, “Attribute-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. Bettencourt, A. Sahai, and B. Waters, “Cypertext-policy attribute based encryption,” in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, 2007.

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

[20] A. Sahai and B. Waters, “Fuzzy identity based encryption,” in *Proc. Acvances in Cryptology—Euro crypt*, 2005, ol. 3494, LNCS, pp. 457–473.

[21] 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.