ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Secure Data Sharing in Cloud Environment Using Multi Authority Attribute Based Encryption

K.Divya[1], N.Sadhasivam[2]

PG Scholar, Department of CSE, Bannari Amman Institute of Technology, Sathyamangalam, India[1]

Assitant Professor(Senior Grade), Department of CSE, Bannari Amman Institute of Technology, Sathyamangalam, India[2]

ABSTRACT—Cloud computing, as associate rising computing paradigm, permits users to remotely store their knowledge during a cloud, thus on relish services on-demand. With fast development of cloud computing, additional and additional enterprises can source their sensitive knowledge for sharing during a cloud. To stay the shared knowledge confidential against untrusted cloud service suppliers (CSPs), a natural approach is to store solely the encrypted knowledge during a cloud. The key issues of this approach embody establishing access management for the encrypted knowledge, and revoking the access rights from users after they are not any longer licensed to access the encrypted knowledge. A progressive encoding theme supported elliptic curve encoding theme permits knowledge to be encrypted multiple times with completely different keys and produces a final cipher text that may be decrypted with one decoding key during a single decoding operation. This theme permits ever-changing the encoding key while not decrypting the info initial, so permits the re-encryption of information in associate Untrusted atmosphere. For secure sharing on the cloud encoding theme, permitting an information owner to store its encrypted data on a cloud and share with completely different users. The sharing is achieved by re-encrypting the info to the licensed users by the cloud supplier, sharing policies nominative by knowledge house owners, and preventing unauthorized access to knowledge.

KEYWORDS—cloud trust; trusted cloud storage; untrusted providers; data sharing; progressive encryption;

I. INTRODUCTION

Cloud computing promotes a model for providing IT capacities over the web as services and on a lease- based mostly and on-demand vogue. A group of technologies underpins the new computing paradigm, together with net Services, Virtualization, Utility Computing, and so on. Intensive analysis efforts are place into cloud com- putt and its connected technologies, leading to many well acknowledged cloud computing theories and technologies; together with Map scale back [3] and its implementation Apache Hadoop [5]. variety of cloud platforms and cloud infrastructures are rumored, together with Eucalyptus [4], Nimbus and a range of services area unit obtainable to the general public, like Amazon EC2 [1], Amazon straightforward Storage Service [2], and so on. Cloud computing is usually represented with a three layer stack, with every layer providing its own services, as illustrated in Figure one. The Cloud Infrastructure Service or the Infrastructure as a Service (IaaS) provides IT infrastructures as a service over pc networks. The Cloud Platform Service or the Platform as a Service (PaaS) delivers computing platforms as a service to sustain the cloud applications. The Cloud Application Services or code as a Service (SaaS) delivers code as a service over the network, permitting users to use applications while not having to put in and run code on their own computers. The readying models planned within the remainder of this text illustrate however applications will be deployed on the Cloud Platform and therefore the means applications act with one another.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

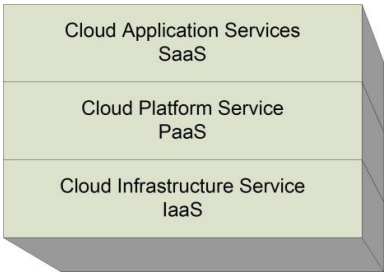

Fig.1. Cloud Technology Stack

With cloud computing, deployment of IT systems and data storage is shifted to off-premises third-party IT infrastructures. Deployment on off-premises third party IT Infrastructures has the subsequent characteristics.

- Data homeowners have solely restricted management over the IT Infrastructure, thus information homeowners should establish a mechanism to mandate the social control of their security policies to make sure information confidentiality and integrity.
- Cloud service suppliers have unnecessary rights. This allows cloud service suppliers to manage and modify users IT system and information.

The on top of 2 characteristics lead directly to a terribly low level of trust on keeping and sharing knowledge on a cloud, once comparison to that of typical infrastructures wherever users have a precise degree of management on the underlying infrastructures.

This work tries to determine a mechanism to handle this issue by permitting users to have sure knowledge storage and sharing over untrusted cloud storage suppliers. Having the ability to implement sure services on untrusted cloud storage suppliers permits users to manage their knowledge on any cloud storage suppliers, eliminating the desired trust on the suppliers.

The overall plan of the proposal mechanism is to write in code the information before storing on the cloud. On sharing the information, the encrypted knowledge is re-encrypted while not being decrypted initial. The re-encrypted knowledge can then be cryptographically accessible to the authorize user solely.

The entire method doesn't reveal the clear knowledge to the cloud supplier at any stage, preventing the cloud supplier from accessing the knowledge. The re-encrypted knowledge would solely be accessible to the licensed user with the corresponding token, preventing the information being shared while not the permission from the information owner.

II. SECURITY REQUIREMENTS

Cloud computing provides storage services to users, wherever users will have access to terribly giant volume of storage. Knowledge unbroken on clouds also can be shared by users giving that the sharing is allowed by the info house owners.

The situation of secure sharing on the cloud is delineated as Figure 2. Alice includes a piece of knowledge that's unbroken on the cloud. Alice needs to share the info with Bob however doesn't need Trudy to possess access to the info. Trudy mustn't be able to access the info by eavesdropping or by deed Bob's authorization token because the authorization token is barely valid for Bob to use.

The specific security needs may be summarized as follows.

1. Knowledge hold on the cloud ought to be confidential. The cloud storage supplier that gives storage service mustn't have the potential of compromising the confidentiality of the information by any suggests that.
2. Sharing of the information may be achieved by the authorization by the information owner. With the given authorization, approved users will then access the information unbroken on the cloud. The authorization and therefore the access of information mustn't offer the cloud supplier any right to access the information.
3. Permissions given by knowledge owner cannot be transferred to others by the permission bearer. Users that aren't the permission holder won't be ready to exercise the permissions given by the information owner to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

access the information.

The challenge of meeting the necessities in the on top of situation is that secure knowledge sharing wants to be achieved via Associate in Nursing Untrusted cloud storage supplier. It's necessary that the cloud storage supplier helps to enforce the authorization policy for knowledge access however the social control mustn't reveal any info to the cloud storage supplier or modify the cloud storage supplier have excessive privileges to permit unauthorized access.

III. PROGRESSIVE ELLIPTIC CURVE ENCRYPTION SCHEME

This section presents progressive elliptic curve cryptography (PECE). The PECE theme permits a chunk of information to be encrypted multiple times victimization completely different keys such the ultimate cipher text may be decrypted during a single run with one key. The cryptography and decoding are each supported Elliptic Curve Cryptography.

The PECE scheme works in as follows.

Let m be a piece of data, U be a set of N users. For each $u_i \in U$, u_i has the secret key k_i.

Let q be a random number agreed by all $u_i \in U$.

The encryption is performed in the order of $u_1, \cdots, u_N$. For $u_i \in U$, it computes

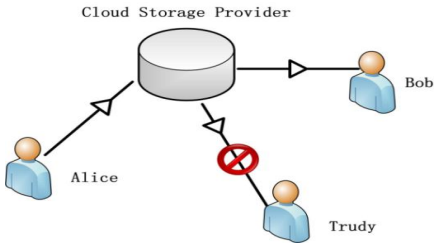

Fig.2. A Scenario of Secure Sharing on the Cloud

$$m_i = m_{i-1} + qk_iG \quad (1)$$

Where $m_0 = m$.

When all $u \in U$, has participated in the encryption process, the final encrypted data is as follows.

$$m_e = m_N \quad (2)$$

$$= m_{N-1} + (qk_NG) \quad (3)$$

$$= m_{N-t} + \sum_{i=N-t+1}^{N} (qk_iG) \quad (4)$$

$$= m_0 + \sum_{i=1}^{N} (qk_iG) \quad (5)$$

$$= m + \sum_{i=1}^{N} (qk_iG) \quad (6)$$

Let $k_c = \Sigma_{i=1}^{N} k_i$ then me can be decrypted by a single operation as follows.

$$m_p = m_e - qk_cG \quad (7)$$

$$= m_e - q\sum_{i=1}^{N} k_iG \quad (8)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

$$= m_e - \sum_{i=1}^{N}(qk_iG) \quad (9)$$

$$= m \quad (10)$$

With PECE theme, a bit of knowledge are often encrypted multiple times victimization completely different keys. The ultimate secret writing produces a cipher text which will be decrypted employing a single key with one spherical of decoding.

IV. SECURE DATA SHARING USING ELLIPTIC CURVE CRYPTOGRAPHY

To secure sharing a piece of knowledge over cloud storage, that can be provided by untrusted cloud service suppliers, a protocol has been devised supported the progressive elliptic curve encoding theme projected in Section III.

A. Secure Sharing Scheme

The protocol may be represented with the state of affairs with 3 principles as mentioned earlier. The method may be concisely summarized into 5 steps as illustrated in Figure three. At Step (A), Alice encrypts her information and keeps the info on a service provided by a Cloud Storage supplier. At Step (B), Bob sends a request to Alice asking for access permission to the info. Alice, at Step (C), sends a document to the Cloud Storage supplier for the re-encryption of the information and sends a document for Bob to decipher the re-encrypted data along with his non-public key at Step (D). At Step (E), the Bob acquires the re-encrypted information from the Cloud Storage supplier and decrypts it.

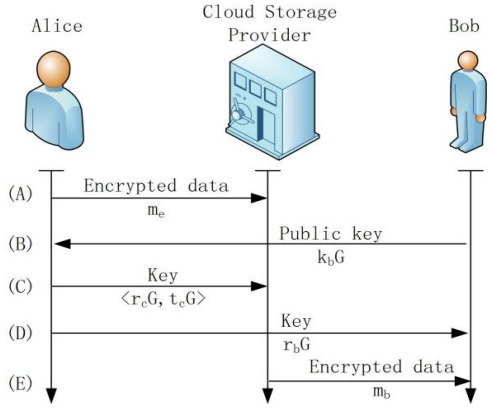

Fig.3. Secure Sharing over Cloud Storage

Assuming that Alice has the private key k_a and the public key k_aG, Bob has the private key k_b and the public key k_bG, and the Cloud Storage Provider has the shared private key k_c with Alice and the public key k_cG.

For a piece of data m, the storing and sharing is as follows.

1) Alice picks two random number r and t, and encrypts m such that

$$m_e = m + rk_cG + tG \quad (11)$$

2) Bob sends a request to Alice with his public key k_bG.

3) Alice chooses random number r_c and r_b. Alice calculates

$$t_cG = -r_bk_bG - r_ck_cG = rk_cG - tG \quad (12)$$

4) Alice sends (r_cG, t_cG) to the Cloud provider, and r_bG to Bob.

5) Cloud provider re-encrypts the data m_e as follows.

$$m_c = m_e + r_ck_cG + t_cG \quad (13)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

6) Bob receives m_c from the Cloud Provider and performs the following computation to generate m_b.

$$m_b = m_c + r_b k_b G \quad (14)$$

Algorithm Proof

The final text m_b generated by Bob is actually identical to m. It can be proved as below.

$$m_b = m_c + r_b k_b G \quad (15)$$

$$= \left(m_e + r_c k_c G + t_c G\right) + r_c k_c G \quad (16)$$

$$= \left(\left(m + rk_c G + tG\right) + r_c k_c G + \left(-r_b k_b G - r_c k_c G - rk_c G - tG\right)\right) + r_b k_b G \quad (17)$$

$$= m \quad (18)$$

B. Summary

The above proposed protocol and algorithm allows sharing of data over a cloud storage service. The sharing depends on the access control from the data owner and will not disclose any information to the cloud storage service provider.

V. SECURITY ANALYSIS

Security attacks to the proposed scheme include accessing the data without authorization, disclosing information during sharing, and sharing the data with others without data owner's permissions.

A. Unauthorized Access To Data

The proposed secure sharing scheme, discussed in Section IV, authorizes users to have access to data by issuing credentials to the authorized users. The issuing of credentials can only be conducted by the data owner. Without the credentials, neither the Cloud Storage Provider nor the users can have access to the data. As the access to the data depends on the data owner's issuing of the authorization credentials, even though the Cloud Storage Server is out of the control of the data owner and is even malicious and untrusted, the enforcement of the access control policy is guaranteed.

Unauthorized access to data can be implemented by the following two scenarios.

1) The assaulter acquires papers which will rewrite the info while not the assistance of the Cloud Storage supplier. To acquire such a papers, the assaulter can want the information of $rK_cG + tG$, or the information of the 3 secrets of r, kc and t. As m, r, kc , and t ar all unbroken secretly, the information of $rK_cG + tG$, or the information of the 3 secrets of r, kc and t, don't seem to be attainable. so it's impractical for Associate in Nursing assaulter to accumulate a papers which will rewrite the info while not the assistance of the Cloud Storage supplier.

2) The offender acquires credentials that may decode the info with the assistance of the Cloud Storage supplier. To acquire such a credential, the attacker must have the knowledge of r_b, k_b, or the knowledge of $r_b k_b G$. As r_b is delivered to Bob in the form of $r_b G$, it is not possible for the attacker to calculate r_b from $r_b G$. k_b could be a secret that is unbroken in camera by Bob, thence the offender may not acquire k_b . In summary, it's unfeasible for the offender to accumulate credentials that may decode the info with the assistance of the Cloud Storage supplier.

B. Information Disclosure During Sharing

During sharing, the info is often in its encrypted type, at completely different stage it's going to be encrypted with different keys. There's no single stage that the info is decrypted into its clear type before it's delivered to the licensed users. This ensures that the total sharing method won't disclose the knowledge of the info to any parties. To acquire the clear data during the sharing, an attacker must either have the decryption key for m_e , m_c or m_b .The above discussion proves that the attacker cannot decrypt m_e or m_b. To rewrite m_c, the wrongdoer wants the data of $r_c k_c G$.kc is that the personal secret unbroken by the Cloud Storage supplier, the wrongdoer may be able to calculate rc k_c G from rc G.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VI. RELATED WORK

C. Elliptic Curve Cryptography (ECC)

It is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public and private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithms may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in Elliptic Curve Cryptography are an example of such constants.

D. Cryptography

This introduction covers all the terms, and definitions that are needed to understand Elliptic Curve Cryptography and Cryptography in general. Traditionally, ciphers have used information contained in secret decoding keys to code and decode messages. The process of coding plaintext to create cipher text is called encryption and the process of decoding cipher text to produce the plaintext is called decryption. There are two types of encryption: symmetric key encryption and public (asymmetric) key encryption. Symmetric key and public key encryption are used.

E. Public Key Encryption

Encryption algorithms that use different keys for encrypting and decrypting information are most often called public-key algorithms but are sometimes also called asymmetric key algorithms. Public key encryption requires the use of both a private key and a public key .A user's public key, for example, can be published in the directory so that it is accessible to other people in the organization. The two keys are different but complementary in function. Information that is encrypted with the public key can be decrypted only with the corresponding private key of the set. The algorithm used is RSA.

F. Cryptographic Message Wrapping

RFC 2634 [10] defines the wrapping of secure emails. The wrapping allows a piece of data to be encrypted multiple times in any combinations. For example, a piece of data can be encrypted two or three times. In this case, the wrapping mechanism works as follows. Let a message m be first encrypted into an encrypted message $m_1 = enc(m, k_1)$, where enc be an encryption function and k_1 be the encryption key. m_1 is then used to construct a new piece of data, $m_{e1} = \{m_1, k'_1\}$, of a specific data of a specific data structure, called, Enveloped Data, where k'_1 be the encrypted text of k_1. Then m_{e1} is treated as a data block and encrypted again as m_2.m_2 will then be used to construct m_{e2} of the Enveloped Data structure. This operation can be performed repeatedly. Instead, it is only a way of packing encrypted data using the same data structure for multiple times with different encryption keys. There is no way to decrypt the double/triple wrapping encrypted data in a single decryption. To extract the final clear text, decryption must be conducted at each individual wrapping layer.

G. Distributed Key Management

Zhao et al. [9] proposed a distributed key management scheme based on RSA. The proposed scheme allows a RSA key be split into multiple shares. Each entity holds one of the shares. If all of them work on the same plaintext for encryption, a cipher text can be generated, which is the same as the cipher text produced by encrypting the plaintext using the original RSA key. Similarly, if all of them work on the same cipher text for decryption, a plaintext can be produced, which is the same as the plaintext produced by decrypting the cipher text using the original RSA key.

The difference between Zhao et al.'s scheme [9] and the scheme proposed by this paper is that, for encryption, Zhao et al.'s scheme [9] needs to work on the plaintext, and it is based on the RSA algorithm. The scheme proposed by this work needs only to work on the plaintext initially, and all further encryption will be applied on the previously produced cipher text.

H. Threshold Cryptography

Threshold cryptography [11] proposed by Shamir is a cryptography scheme based on secret sharing. It shares the encryption/decryption secret among n users, with each user keeping only part of the secret. The scheme allows any k or more users out of the n users to cooperate together to perform encryption/decryption operations. The operations will have the same effect as using the complete secret. When k is set to n, threshold

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

cryptography is very similar to the scheme proposed in this paper. But threshold cryptography, depending on the specific implementation and schemes, is likely to require working on the plaintext and also involve interactive and complicated communication among the participating users. The scheme proposed in this paper does not require interactive communication among the participating users.

I. Homomorphism Encryption

Homomorphism encryption is a cryptography scheme that, by applying algebraic operations on the cipher text, one can perform algebraic operations on the plaintext. This allows multiple parties to cooperatively generate a piece of cipher text without knowing the plaintext that others work on. The process can be formalized as follows. Let e be an encryption function and m_1 and m_2 be a plaintext.

$$c_1=e(m_1) \quad (19)$$

$$c_2=e(m_2) \quad (20)$$

$$c_1 \times c_2=e(m_1+m_2) \quad (21)$$

Where × and + are two algebraic operations

Homomorphism encryption is different from the scheme proposed in this paper. Homomorphism encryption investigates the algebraic relationship between the algebraic operations on plaintext and the algebraic operations on cipher text. The scheme proposed in this paper is to investigate the relationship between the algebraic operation on the cipher text and the algebraic operations on the encryption keys.

J. Incremental Encryption

Incremental encryption [7],[8] proposed an incremental cryptography scheme. The scheme allows the computation of the final cipher text based on the initial cipher text and the change of the plaintext. To be specific, let m be a plaintext, the initial cipher text be $c = f(m, k)$ where k be the encryption key. If m is modified to $m + m_\delta$, the final cipher text $c_f = f((m + m_\delta, k)$ can be computed as $c_f = g(c, h(m_\delta, k))$, where h is a function that calculates the effect of the change of the plaintext, and g is a function that calculates the final cipher text based on the effect of the plaintext change and the initial cipher text. This scheme is different from the scheme proposed by this paper is that, incremental encryption scheme [7], [8] is re-processing the cipher text for the purpose of generating a different plaintext on decryption. This is useful to apply changes of plaintext onto the previously generated cipher text. While the proposed scheme in the paper is trying to reprocess the cipher text to allow decrypting with another decryption key.

K. Elliptic Curve Cryptography

Conventional ECC encrypts the data m to the user w, who has the private key k_W and public key $k_W G$ as follows.

1) A random number r is picked.
2) Calculate $m_C = m + r\, k_W G$
3) Calculate $k_r = rG$

Then the message (m_C, k_r) is sent to the user w. On receiving the message (m_C, k_r), the user w decrypts the message as follows.

1) Calculate $p = k_W k_r = k_W r\, G = r\, k_W G$.

Calculate $m_p = m_C - p = (m + rk_W G) - rk_W G = m$.

L. Cloud Security

Armbrust et al. [6] identified ten obstacles to growth of cloud computing, arguing that these were the most ten important obstacles. The known obstacles embody availableness of service, knowledge lock-in, knowledge confidentiality and audit ability, knowledge transfer bottlenecks, performance unpredictability, climbable storage, bugs in massive distributed systems, scaling quickly, name fate sharing, and package licensing. Various security connected problems and issues in cloud computing are known and square measure beneath study, as well as information privacy [6], [14], information protection [11], access management , [13], [6], authentication [12], and so on. Many banks have expertise with security infrastructure provided as cloud computing services. Boiling Springs Savings Bank and Ulster Savings Bank relied on a security on- demand provider's security services to take care of their internal networks' security. Each bank according that the next level of security had been achieved with lower price.

Singh et al. [15] planned associate categorization theme which will build indices with access management data for looking out encrypting information, to implement access management on the looking out of encrypted outsourced information unbroken on a cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VII. CONCLUSION AND FUTURE WORK

In this work a progressive encryption scheme based on elliptic curve encryption. The proposed progressive encryption scheme allows data to be encrypted multiple times with different keys and produces a final cipher text that can be decrypted with a single decryption key in a single decryption operation. This scheme allows changing the encryption key without decrypting the data first, thus enables the re encryption of data in an Untrusted environment. The protocol is devised based on the proposed progressive encryption scheme, allowing a data owner to store its encrypted data on a cloud and share with different users.

The sharing is achieved by re-encrypting the data to the authorized users by the cloud provider. The proposed scheme can mandatory enforce sharing policies specified by data holders, and avoiding unlicensed access to data. Future work of this research includes Multi Attribute Authority is responsible for creating the private credentials used for decryption. In Attribute Authority is an independent attribute authority that is responsible for revoking attributes to users according to their role or identity in its domain.

In every attribute is associated with a single Attribute Authority, but each Attribute Authority can manage an arbitrary number of attributes. In practice, attributes belong to different authorities can be identified by encoding the attributes with different prefix. In this approach Every Attribute Authority has full control over the structures and semantics of its attributes, and preserves a state and a reversal list for each attribute in its domain. Each Attribute Authority is responsible for issuing secret keys to users when they are entitled attributes in its domain and publishing update keys for each attribute in its domain at each time slot to reflect the users' possessions of the attribute at the time slot.

REFERENCES

[1] Amazon Elastic Compute Cloud (EC2), 2009, http://www.amazon.com/ec2/.

[2] Amazon Simple Storage Service, 2009, http://aws.amazon.com/s3.

[3] J. Dean and S. Ghemawat, "MapReduce: simplified data processing on large clusters," Commun. ACM, vol. 51, no. 1, pp. 107–113, 2008.

[4] Eucalyptus, 2009, http://eucalyptus.cs.ucsb.edu/.

[5] Apache Hadoop, 2009, http://hadoop.apache.org/.

[6] L. Kaufman, "Data security in the world of cloud computing,"IEEE SECURITY & PRIVACY, vol. 7, no. 4, July-August2009.

[7] M. Bellare, O. Goldreich, and S. Goldwasser, " Incremental cryptography: The case of hashing and signing," in CRYPTO '94: Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, 1994, pp. 216–233.

[8] "Incremental cryptography and application to virus protection," in STOC '95: Proceedings of the twenty-seventh annual ACM symposium on Theory of computing. New York, NY, USA: ACM, 1995.

[9] G. Zhao, S. Otenko, and D. Chadwick, "Distributed key management for secure role based messaging," in Proceeding of The IEEE 20th International Conference on Advanced Information Networking and Applications (AINA2006), Vienna, Austria, April 2006.

[10] P. Hoffman, "RFC 2634 - Enhanced Security Services for S/MIME," Network Working Group, Request For Comment, June 1999.

[11] A. Shamir, "How to share a secret," Comm. ACM, vol. 22, no. 11, 1979. Available: http://portal.acm.org/citation.cfm?id=359168.359176

[12] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in The First International Conference on Cloud Computing, 2009,166.

[13] L. Hu, S. Ying, X. Jia, and K. Zhao, "Towards an approach of semantic access control for cloud computing," in The First International Conference on Cloud Computing, 2009, pp. 145–156.

[14] A°. A. Nyre and M. G. Jaatun, "Privacy in a semantic cloud: What's trust got to do with it?" in The First International Conference on Cloud Computing, 2009,

[15] A. Singh, M. Srivatsa, and L. Liu, "Search-as-a-Service: Outsourced Search over Outsourced Storage," ACM TRANSACTIONSON THE WEB, vol. 3, no. 4, September 2009.