International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 12 – SEPTEMBER 2017.

A Secured Reinforced Attribute Based Data Sharing Model in Cloud Computing

R.Senthilkumar[#1] and G. Raja Raja Cholan[*2]

[#]*Department of Computer Science, Prist University, Vallam, Thanjavur,India*

[*] *Department of Computer Science, Prist University, Vallam, Thanjavur, India*

***Abstract*— Cipher-text-policy attribute-based encryption is a very promising encryption technique for secure data sharing in the context of cloud computing. Data owner is allowed to fully control the access policy associated with his data which to be shared. However, CP-ABE is limited to a potential security risk that is known as key escrow problem, whereby the secret keys of users have to be issued by a trusted key authority. Besides, most of the existing CP-ABE schemes cannot support attribute with arbitrary state. In this paper, we revisit attribute-based data sharing scheme in order to solve the key escrow issue but also improve the expressiveness of attribute, so that the resulting scheme is more friendly to cloud computing applications. We propose an improved two-party key issuing protocol that can guarantee that neither key authority nor cloud service provider can compromise the whole secret key of a user individually. Moreover, we introduce the concept of attribute with weight, being provided to enhance the expression of attribute, which can not only extend the expression from binary to arbitrary state, but also lighten the complexity of access policy. Therefore, both storage cost and encryption complexity for a cipher text are relieved. The performance analysis and the security proof show that the proposed scheme is able to achieve efficient and secure data sharing in cloud computing.**

***Index Terms*—Cloud Computing, Attribute based Encryption, CP-ABE, Cloud data sharing**

I. INTRODUCTION

The demand of outsourcing data has greatly increased in the last decade. To satisfy the need for data storage and high performance computation, many cloud computing service providers have appeared, such as Amazon Simple Storage Service (Amazon S3), Google App Engine, Microsoft Azure, Dropbox and so on. There are two obvious advantages to store data in Cloud Servers:

1) The data owners save themselves out from the trouble of buying extra storage servers and hiring server management engineers;

2) It is easier for the data owner to share their data with intended recipients when the data is stored in the cloud.

Despite of the above advantages of cloud storage, there still remain various challenging obstacles, among which, the privacy and security of users' data have become two major issues. Traditionally, the data owner stores his/her data in the trusted servers, which are generally controlled by a fully trusted administrator.

However, the cloud is usually maintained and managed by a semi-trusted third party (Cloud provider). As a result, traditional security storage technologies cannot be directly applied in the cloud storage scenario. While it is desirable for the data owner to share his/her private data with intended recipients, it presents an even more challenging problem since we have to make sure that except the intended recipients, nobody, including the cloud providers, can obtain any useful information from the encrypted data. The conventional approach to address the above mentioned problem is to use cryptographic encryption mechanisms, and store the encrypted data in the cloud. Authorized users can download the encrypted files and decrypt them with the given keys. But in this scenario, how to distribute and update session keys is one of the most important but hard problems. *Digital Envelope*[1] is used to address this task in [2], [3]: the data is encrypted with a randomly chosen session key by using symmetric encryption, and then the session key is encrypted with the public key of the specific user by using public-key encryption. For example, we assume that the user *A* wants to securely send a file *F* to the user *B*. First, The user *A* chooses a random session key *K*, and uses a symmetric encryption algorithm (such as *DES* and *AES*) to encrypt the file *FILE*: *{FILE}K*. Then user *A* uses an asymmetric encryption algorithm (such as *RSA*) to encrypt the session key *K*: *EPuKB*(*K*) (*PuKB* is *B*'s public key). Here, *EPuKB*(*K*) is named as a digital envelope, which can be transmitted in the open environment, and be decrypted only by the user *B*. However, in normal ways, if a file is shared to *N* specific authorized users, *N* digital envelopes are required to be generated. Therefore, the computing and communication overhead of generating digital envelopes is *O*(*N*) for one file. Meanwhile, the computational complexity and communication overhead of session key updating are both *O*(*N*). Moreover, we assume that one session key is required for each one sharing file. If the total number of shared files is *M* for *N* specific recipients, the overall overhead of digital envelope generation for all shared files is as large as *O*(*MN*).

II. RELATED WORKS

A. An intrusion detection system in adhoc networks

The nature of mobility for mobile networks needs additional mechanisms for providing security. These vulnerabilities do not exist in a fixed wired network. Therefore, the traditional way of protecting networks with

firewalls and encryption software is no longer sufficient. We need to develop new architecture and mechanisms to protect the wire-less networks and mobile computing applications. Hence, in this paper, we discuss how to identify the intrusion after an anomaly is reported. Simple rules are applied to identify the intruder information and detect the type of the attack. A node called the Monitor node carries the identification process. This node overhears the channel and detects the misbehavior nodes. There may be more than one monitor node in the whole network. Periodically the monitor nodes are elected in the network.

1) *Disadvantages:*

- First, a small window will result in false positives while a large window will result in irrelevant data as well as increase the chance of false negatives.
- Second, the net topology is only determined after considerable trial and error.
- The intruder can train the net during its learning phase.
- These statistical approaches can gradually be trained by intruders so that eventually, intrusive events are considered normal, false positives and false negatives are generated depending on whether the threshold is set too low or too high, and relationships between events are missed because of the insensitivity of statistical measures to the order of events.
- There are some drawbacks to the expert system approach too. For example, the expert system has to be formulated by a security professional and thus the system is only as strong as the security personnel who program it. This means that there is a real chance that expert systems can fail to flag intrusions.

B. *An Application-Specific Protocol Architecture for Wireless Micro sensor Networks*

ADVANCES in sensor technology, low-power electronics, and low-power radio frequency (RF) design have enabled the development of small, relatively inexpensive and low-power sensors, called *micro sensors* that can be connected via a wireless network. These wireless micro sensor networks represent a new paradigm for extracting data from the environment and enable the reliable monitoring of a variety of environments for applications that include surveillance, machine failure diagnosis, and chemical/biological detection. An important challenge in the design of these networks is that two key resources—communication bandwidth and energy—are significantly more limited than in a tethered network environment. These constraints require innovative design techniques to use the available bandwidth and energy efficiently. In order to design good protocols for wireless micro sensor networks, it is important to understand the parameters that are relevant to the sensor applications. While there are many ways in which the properties of a sensor network protocol can be evaluated, we use the following metrics. *Ease of Deployment* Sensor networks may contain hundreds or thousands of nodes, and they may need to be deployed in remote or dangerous environments, allowing users to extract information in ways that would not have been possible otherwise. This requires that nodes be able to communicate with each other even in the absence of an established network infrastructure and predefined node locations Networking together hundreds or thousands of cheap micro sensor nodes allows users to accurately monitor a remote environment by intelligently combining the data from the individual nodes. These networks require robust wireless communication protocols that are energy efficient and provide low latency. In this paper, we develop and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for micro sensor networks that combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. LEACH includes a new, distributed cluster formation technique that enables self-organization of large numbers of nodes, algorithms for adapting clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources. Our results show that LEACH can improve system lifetime by an order of magnitude compared with general-purpose multihop approaches

1) *Disadvantages:*

- Very high key Management storage, use symmetric algorithm.
- Lot of Cryptography problem occur in Cluster Based Wireless Sensor Network
- Require high Energy to transmit data to the GH.
- This method is prohibitively expensive in terms of communication overhead (or energy spent).
- Each node to send an authentication message to the base station.
- Falsified Attack.
- Tree-based aggregation approaches are not resilient to communication losses resulting from node and transmission failures, which are relatively common in WSNs

C. *Efficient Algorithms for Pairing-Based Cryptosystems*

The recent discovery of groups where the Decision Diffie-Hellman (DDH) problem is easy while the Computational Diffie-Hellman (CDH) problem is hard, and the subsequent definition of a new class of problems variously called the Gap Diffie-Hellman, Bilinear Diffie-Hellman, or Tate-Diffie-Hellman [6] class, has given rise to the development of a new, ever expanding family of cryptosystems based on pairings, such as: Short signatures .Identity-based encryption and escrow ElGamal encryption. Identity-based authenticated key agreement .Identity-based signature schemes. Tripartite Diffie-Hellman. Self-blindable credentials. The growing interest and active research in this branch of cryptography has led to new analyses of the associated security properties and to extensions to more general (e.g. hyperelliptic and superelliptic) algebraic curves **.**However, a central operation in these systems is computing a bilinear pairing (e.g. the Weil or the Tate pairing), which are computationally expensive. Moreover, it is often the case that

curves over fields of characteristic 3 are used to achieve the best possible ratio between security level and space requirements for super singular curves, but such curves have received considerably less attention than their even or (large) prime characteristic counterparts. Our goal is to make such systems entirely practical and contribute to fill the theoretical gap in the study of the underlying family of curves, and to this end we propose several efficient algorithms for the arithmetic operations involved the definition of point tripling for super singular elliptic curves over F3m, that is, over fields of characteristic 3. A point tripling operation can be done in O (m) steps (or essentially for free in hardware); as opposed to conventional point doubling that takes O (m2) steps. Furthermore, a faster point addition algorithm is proposed for normal basis representation. These operations lead to a noticeably faster scalar multiplication algorithm in characteristic 3. An algorithm to compute square roots over Fpm in O(m2 log) steps, where m is odd and p _ 3 (mod 4) or p _ 5 (mod 8). The best previously known algorithms for square root extraction under these conditions take O (m3) steps. This operation is important for the point compression technique, whereby a curve point P = (x, y) is represented by its x coordinate and one bit of its y coordinate, and its usefulness transcends pairing-based cryptography. A deterministic variant of Miller's algorithm to compute the Tate pairing that avoids many irrelevant operations present in the conventional algorithm whenever one of the pairing's arguments is restricted to a base field (as opposed to having both in an extension field). Besides, in characteristics 2 and 3 both the underlying scalar multiplication and the final powering in the Tate pairing experience a complexity reduction from O(m3) to O(m2) steps. All of these improvements are very practical and result in surprisingly faster implementations.

1) *Disadvantages:*

- Slow reaction on restructuring and failures.
- Network latency and network traffic.
- Total energy consumed for packet delivery.
- While centralized protocols have a single point of failure and high communication cost
- Self-healing mechanism designed for continuous iteration without significantly affecting the network performances, while achieving high clone detection rate

D. An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures: Implementation and Evaluation

Authentication in Wireless Sensor Networks (WSNs) can be divided into three categories, namely base station to sensor nodes, sensor nodes to other sensor nodes, and outside users to sensor nodes. The problem of authenticated broadcast by the base station has been widely addressed We focus on the other two categories, namely the authenticated broadcast/multicast by the sensor nodes and the outside user authentication. To handle these two problems, we proposed an authentication framework for WSNs in using Identity(ID)-based Cryptography and Online/Offline Signature (OOS) schemes. This framework is comprised of two authentication schemes; quick authenticated broadcast/ multicast by sensor nodes and outside user authentication. The first scheme allows every sensor node in the network to broadcast or multicast authenticated messages very quickly without the involvement of the base station. All potential receivers can verify a message sent by any sender node in the network. It also allows sensor nodes on the path from the sender node to the receivers to verify a valid message and drop false injected data. The second scheme enables all sensor nodes in the network to verify the legitimacy of any outside user without storing any user specific information. It allows a maximum possible number of legitimate users to access data from sensor nodes in a secure way. This scheme first authenticates a user and then establishes a session key for the secure exchange of user queries and sensor nodes data. The proposed framework uses an ID-based Online/Offline Signature (IBOOS) (an ID-based version of OOS) for the first scheme and an ID-based Signature (IBS) for the second scheme In Wireless Sensor Networks (WSNs), authentication is a crucial security requirement to avoid attacks against secure communication, and to mitigate against DoS attacks exploiting the limited resources of sensor nodes. Resource constraints of sensor nodes are hurdles in applying strong public key cryptographic based mechanisms in WSNs. To address the problem of authentication in WSNs, we propose an efficient and secure framework for authenticated broadcast/multicast by sensor nodes as well as for outside user authentication, which utilizes identity based cryptography and online/offline signature (OOS) schemes. The primary goals of this framework are to enable all sensor nodes in the network, firstly, to broadcast and/or multicast an authenticated message quickly; secondly, to verify the broadcast/multicast message sender and the message contents; and finally, to verify the legitimacy of an outside user. This paper reports the implementation and experimental evaluation of the previously proposed authenticated broadcast/multicast by sensor nodes scheme using online/offline signature on Tinos and MICA2 sensor nodes. Key words: Wireless Sensor Network**.**

1) *Disadvantages:*

- Scalability of network is low.
- Computation cost is high.
- Storage overhead is also high.
- These Scheduling Approaches save on the energy waste due to collisions.
- They can increase the energy waste due to overhead from control messages.

E. A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Networks

Continued advances of MEMS and wireless communication technologies have enabled the deployment of large scale wireless sensor networks (WSNs) .The potential applications of WSNs are highly varied, such as environmental monitoring, target tracking and military surveillance. Sensors in such a network are equipped with sensing, data processing, and radio transmission units, while the power is highly limited. Due to the sensors' limited power, innovative techniques that improve energy efficiency to

prolong the network lifetime are highly required. Thus energy-aware design has been a hot research area at all layers of the networking protocol stack. Data gathering is a common but critical operation in many applications of WSNs, where data aggregation and hierarchical routing mechanism are commonly used techniques. Data aggregation can eliminate data redundancy and reduce communication load. Hierarchical (clustering) mechanisms are especially effective in increasing network scalability and reducing data latency, and have been extensively exploited. We propose and evaluate an energy efficient clustering scheme (EECS) for periodical data gathering applications in WSNs. In the *cluster head election* phase, the cluster head is elected by localized competition, which is unlike LEACH, and with no iteration, which differs from HEED. The optimal value of competition range produces a good distribution of cluster heads. Further in the *cluster formation* phase, plain nodes join clusters not only taking into account its intra-cluster communication cost, but also considering cluster heads' cost of communication to the BS.EECS is autonomous and more energy efficient, and simulation results show that it prolongs the network lifetime much more significantly than the other clustering protocols.

1) Disadvantages:

- Unbalanced energy depletion.
- Performance of data transmission is too low.
- Here several cluster head is elected which is lead to damage entire system.
- The Random Access Category, high-rate wireless sensor networks service that can lead to packet loss.

Local protocols do not detect replicated nodes that are distributed in different areas of the network.

III. PROPOSED SYSTEM MODEL:

A. Model:

Case Study and Data Collection .We consider a case study of a web-based collaboration application for evaluating performance. The application allows users to store, manage, and share documents and drawings related to large construction projects. The service composition required for this application includes: Firewall (x1), Intrusion Detection (x1), Load Balancer (x1), Web Server (x4), Application Server (x3), Database Server (x1), Database Reporting Server (x1), Email Server (x1), and Server Health Monitoring (x1). To meet these requirements, our objective is to find the best Cloud service composition

1) Group Leader

The group leader opens up a sharing area in the cloud to form a group application. Then, he/she grants the group members the right to implement data management. All the data in this group are available to all the group members, while they remain private towards the outsiders of the group including the cloud provider. The group leader can authorize some specific group members to help with the management of the group, and this privilege can also be revoked by the group leader. When a member leaves the group, he/she will lose the ability to download and read the shared data again.

2) File Upload

The group leader can upload the file for the group members. And the files are encrypted.

3) Re-encrypt

The group leader should re-encrypt the members file.

4) Select Admin

The group leader can authorize some specific group members to help with the management of the group, and this privilege can also be evoked by the group leader.

5) Accept Request

The group leader also accept the new member request.

B. Admin Authentication

The group leader can authorize some specific group members to help

with the management of the group, and this privilege can also be evoked by the group leader. And the Admin can accept the New user request.

C. Group Member

Each group member can implement file download and upload operations in the authenticated group. Each *GM* can get some related public information from Cloud Servers and compute the specific set of security parameters, such as group key pair.

D. Share Data

The group members can share their data into another members in same group the data will translated by encrypted data.

E. Upload Data

The group members can upload the file to group leader. And the group leader can re-encrypt the data

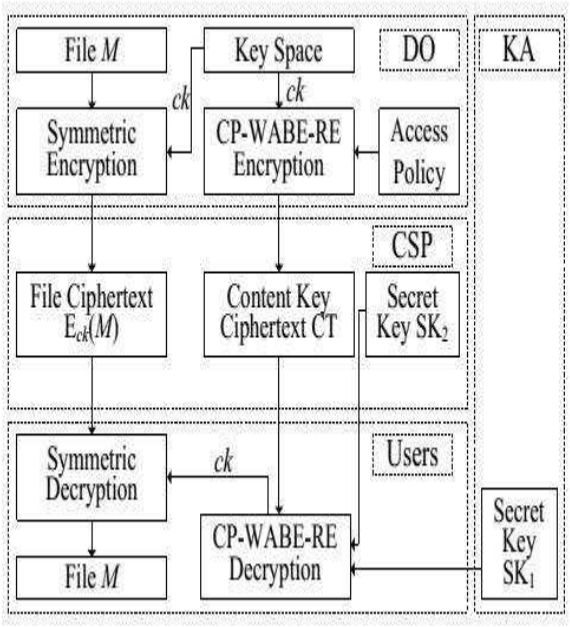
F. Download File

The group members also download the group leader file.

IV. THEORETICAL ANALYSIS

A. Key Escrow and Weighted Attribute:

Table I shows the problem of key escrow, feature of weighted attribute and application in cloud computing for each scheme. The key escrow in CP-WABE-RE scheme can be removed by using an improved key issuing protocol for cloud computing. Hur uses escrow-free key issuing protocol to solve the issue. On the contrary, both don't solve the problem of key escrow. In addition, the weighted attribute in CP-WABE-RE scheme can not only support arbitrary-state attribute instead of the traditional binary state, but also simplify access policy associated with a ciphertext as opposed. Unfortunately, can only express arbitrary-state attribute, and cannot simplify the access structure. In Table I, we can find that only CP-WABE-RE scheme can simultaneously support all the three functions. Hur solves the problem of key escrow so it can satisfy environment of cloud system as ours. However, both cannot remove key escrow. Thus the both schemes cannot be directly applied in cloud computing.

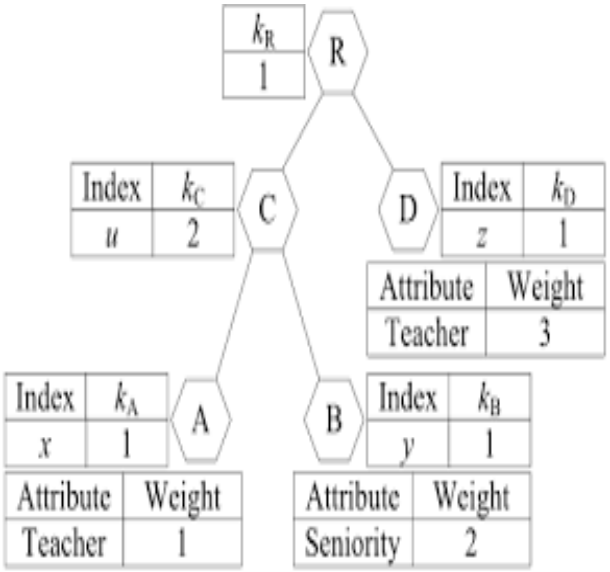


B. Efficiency:

We compare efficiency of the above four schemes on storage overhead and computation cost in theory. To simplify the comparisons, access structure, data re-encryption of, and dynamic membership management (that is, user joining, leaving, and attribute updating) of are not included in the following analysis. In addition, the cost of transmission isn't involved when implementing the interactive protocols in both and our proposed scheme. In the schemes are compared in terms of CT size, SK size, PP size and MSK size. CT size represents the storage overhead in cloud computing and also implies the communication cost from DO to CSP, or from CSP to users. SK size denotes the required storage cost for each user. PP and MSK sizes represent the storage overhead of KA and CSP in terms of public parameter and master secret key.

C. Weighted Access Tree

Let T be a weighted access tree, where root node of the tree is R. To facilitate description of the access tree, several functions and terms are defined as follows.



V. RESULTS AND DISCUSSION:

A. Experimental Results:

Domo is implemented in visual studio 2010 and sqlserver2008.In this paper we proposed a dynamic secure group sharing framework in public cloud computing environment. In our proposed scheme, the management privilege can be granted to some specific group members based on proxy signature scheme, all the sharing files are secured stored in Cloud Servers and all the session key are protected in the digital envelopes.

We use Cloud Servers' aid based enhanced *TGDH* scheme to dynamical updating group key pair when there're group members leaving or joining the group. Even though not all the group members are online together, our scheme can still do well. In order to providing forward secrecy and backward secrecy, digital envelopes should be updated based on proxy re-encryption, which can delegate most of computing overhead to Cloud Servers without disclosing any security information. From the security and performance analysis, the proposed scheme can achieve the design goal, and keep a lower computational complexity and communication overhead in each group members' side

In 2005, Sahai and Waters introduced fuzzy identity-based encryption (IBE), which is the seminal work of attribute-based encryption (ABE). After that, two variants of ABE were proposed: key-policy ABE (KPABE) CP-ABE depending on if a given policy is associated with either a ciphertext and a key. Later, many CP-ABE schemes with specific features have been presented in the literature. For example, presented a novel access control scheme in cloud computing with efficient attribute and user revocation. The computational overhead is significantly eliminated from O(2N) to O(N) in user key generation by improving CP-ABE scheme, where N is the number of attributes. The size of ciphertext is approximately reduced to half of original size. However, the security proof of the scheme is not fully given. Most of the existing CP-ABE schemes require a full trusted authority with its own master secret key as input to generate and issue the secret keys of users. Thus, the key escrow issue is inherent, such that the authority has the "power" to decrypt all the ciphertexts of system users. Chase and Chow presented a distributed KP-ABE scheme to solve the key escrow problem in a multi-authority system. In this approach, all authorities, which are not colluded with each other, are participating in the key generation protocol in a distributed way, such that they cannot pool their data and link multiple attribute sets belonging to the same user. Because there is no centralized authority with master secret information, all attribute authorities should communicate with others in the system to create a user's secret key. But, a major concern of this approach is the performance degradation. It results in O(N2) communication overhead on both the system setup phase and any rekeying phase. It also requires each user to store O(N2) additional auxiliary key components in addition to the attribute keys, where N is the number of authorities in the system. Chow later proposed an anonymous private key

generation protocol for IBE where a KA can issue private key to an authenticated user without knowing the list of the user's identities. It seems that this approach can properly be used in the context of ABE if attributes are treated as identities. However, this scheme cannot be adopted for CP-ABE, since the identity of user is a set of attributes which is not publicly unknown In 2013, provided an improved security data sharing scheme based on the classic CP-ABE. The key escrow issue is addressed by using an escrow-free key issuing protocol where the key generation center and the data storage center work together to generate secret key for user. Therefore, the computational cost in generating user's secret key increases because the protocol requires interactive computation between the both parties. Besides, Liu et al. presented a finegrained access control scheme with attribute hierarchy, where are built on top of respectively. In the schemes, the attributes are divided into multiple levels to achieve fine-grained access control for hierarchical attributes, but the attributes can only express binary state. Later, Fan et al. proposed an arbitrary-state ABE to solve the issue of the dynamic membership management. In this paper, a traditional attribute is divided to two parts: attribute and its value.

VI. CONCLUSION

In this paper, we redesigned an attribute-based data sharing scheme in cloud computing. The improved key issuing protocol was presented to resolve the key escrow problem. It enhances data confidentiality and privacy in cloud system against the managers of KA and CSP as well as malicious system outsiders, where KA and CSP are semi-trusted. In addition, the weighted attribute was proposed to improve the expression of attribute, which can not only describe arbitrary state attributes, but also reduce the complexity of access policy, so that the storage cost of ciphertext and time cost in encryption can be saved. Finally, we presented the performance and security analyses for the proposed scheme, in which the results demonstrate high efficiency and security of our scheme. Although the parameter can be downloaded with ciphertexts, it would be better if its size is independent of the maximum number of ciphertext classes. On the other hand, when one carries the delegated keys around in a mobile device without using special trusted hardware, the key is prompt to leakage, designing a leakage-resilient cryptosystem yet allows efficient and flexible key delegation is also an interesting direction

REFERENCES

[1] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.

[2] A. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," Inf. Sci., vol. 276, no. 4, pp. 354– 362, Aug. 2014.

[3] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham, "Randomizable proofs and delegatable anonymous credentials," in Proc. 29th Annu. Int. Cryptol. Conf., 2009, pp. 108–125.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.

[5] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, 2004.

[6] M. Chase, "Multi-authority attribute based encryption," in Proc. 4th Conf. Theory Cryptogr., 2007, pp. 515–534.

[7] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute- based encryption," in Proc. 16th ACM Conf. Comput. Commun. Secur., 2009, pp. 121–130.

[8] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 456–465.

[9] S. S. M. Chow, "Removing escrow from identitybased encryption," in Proc. 12th Int. Conf. Pract. Theory Public Key Cryptogr., 2009,pp. 256–276.

[10] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[11] A. De Caro and V. Iovino, "JPBC: Java pairing based cryptography," in Proc. 16th IEEE Symp. Comput. Commun., Jun./Jul. 2011, pp. 850–855.

[12] H. Deng et al., "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," Inf. Sci., vol. 275, no. 11, pp. 370–384, Aug. 2014.