International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099
VOL 3 ISSUE 1 (2018) PAGES 1 - 11
Received: 10/07/2018. Published: 27/07/2018

AN EFFICIENT KEY-POLICY ATTRIBUTE-BASED ENCRYPTION SCHEME IN CLOUD COMPUTING

D.B.Shanmugam[1], D.S.Sumitha[2], Dr.J.Dhillipan[3] , C.Karthi[4]
[1]*Associate Professor, Department of MCA, Sri Balaji Chockalingam Engineering College , Arni*
[1]*dbshanmugam@gmail.com*
[2]*M.Phil, Research Scholar, Dr.M.G.R.Chockalingam Arts College, Arni.*
[2] ***sumithadsmca@gmail.com***
[3]*Asst.Prof.,(S.G) & Head, MCA Department, SRM University, Ramapuram Campus, Chennai.*
[3]*Jd_pan@yahoo.co.in*
[4]*Assistant Professor, Department of MCA, Sri Balaji Chockalingam Engineering College , Arni*
[4]*cknmca@gmail.com*

ABSTRACT

In the current network era, cloud service providers offer infinite storage space and computing power for users to manage their data. To enjoy these services, individuals and organizations store their private data on cloud servers. However, in the case of security breaches, users' private data stored in the cloud are no longer safe. When users outsource their data to cloud servers, they expect complete privacy of their data stored in the cloud. Protecting the privacy and data of users has remained a very crucial problem for cloud servers. To avoid any inconvenience, users store their private data in encrypted form. The Attribute Based Encryption(ABE) cryptosystem enriches the flexibility of the encryption policy and the description of users' rights, and it changes from a one-one to one-many scenario during the encryption and decryption phases. ABE has been widely used in many scenarios, particularly in cloud computing In this Project, public key encryption with equality test is concatenated with key-policy attribute-based encryption (KP-ABE) to present key-policy attribute-based encryption with equality test (KP-ABEwET). The proposed scheme not only offers fine-grained authorization of ciphertexts but also protects the identities of users. The main technologies in this scheme include keypolicy attribute-based encryption (KP-ABE) and public key encryption with equality test (PKEwET). the concepts of public key encryption with equality test and identity-based encryption to obtain identity-based encryption with equality test. Inheriting the advantage of simplify the certificate management with all messages encrypted with the receiver's public identity Using this primitive someone with the trapdoor for its identity can delegate out the capability of equality test on its ciphertexts without requiring a central authority to act as a delegator.

1. INTRODUCTION

In the current network era, cloud service providers offer infinite storage space and computing power for users to manage their data. To enjoy these services, individuals and organizations store their private data on cloud servers. However, in the case of security breaches, users' private data stored in the cloud are no longer safe. When users outsource their data to cloud servers, they expect complete privacy of their data stored in the cloud.

Protecting the privacy and data of users has remained a very crucial problem for cloud servers. To avoid any inconvenience, users store their private data in encrypted form. For fine-grained sharing of encrypted data, Sahai and Waters presented attribute-based encryption (ABE) . ABE is a public key cryptosystem variant that allows users to access secret data based on their attributes. This cryptosystem enriches the flexibility of the encryption policy and the description of users' rights, and it changes from a one-one to one-many scenario during the encryption and decryption phases. The underlying cryptosystem combines the secret key and the access structure. Be then court et al. proposed cipher text-policy attribute based encryption (CP-ABE) traditionally, this type of expressive access control is enforced by employing a trusted server to store data locally.

The server is entrusted as a reference monitor that checks that a user presents proper certification before allowing him to access records or files. However, services are increasingly storing data in a distributed fashion across many servers. Replicating data across several locations has advantages in both performance and reliability.The drawback of this trend is that it is increasingly difficult to guarantee the security of data using traditional methods; when data is stored at several locations, the chances that one of them has been compromised increases dramatically. For these reasons we would like to require that sensitive data is stored in an encrypted form so that it will remain private even if a server is compromised.Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a 'cloud'. It greatly attracts attention and interest from both academia and industry due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the best of our knowledge. First of all, data confidentiality should be guaranteed.

The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control.

This is because when sensitive information or computation is outsourced to the cloud servers or another user, which is out of users' control in most cases, privacy risks would rise dramatically because the servers might illegally inspect users' data and access sensitive information, or other users might be able to infer sensitive information from the outsourced computation.

. Data storage centre in cloud computing can be reliable and secure, because the world's most advance data canter is helping the users save the data. The users must not concern about virus attack, data loss, and other problems when they used the cloud in correct form User with cloud computing can use the cloud services anywhere, everywhere, on-demand and based on pay per use principle.

ABE is a public key cryptosystem variant that allows users to access secret data based on their attributes. This cryptosystem enriches the flexibility of the encryption policy and the description of users' rights, and it changes from a one-one to one-many scenario during the encryption and decryption phases.

Computers have become an integral part of our life and we need computers everywhere, i.e. for computing work, research or in any related field. As the use of computers in our day-today life increases, the quantity of required computing resources is also rising up. Purchasing and managing

these big computing resources are easily manageable for giant IT companies like Google and Microsoft as and when they need. But, when it comes to smaller enterprises, affordability becomes a major component to think about. Apart from purchasing, problem related to the huge IT infrastructure is machine failure; hard drive crashes, software bugs, etc. This might be a big trouble for such small enterprise community.

So cloud computing provides a settlement to this situation for these start-up small companies. Cloud computing is a paradigm shift in which computing is shifting from personal computers and individual enterprise application server to a 'cloud' of computers. A cloud is a virtualized server pool which offers different computing resources to their clients as per their demands. So, users of this system need only be concerned with the computing service being asked for, not about the underlying details of how it is achieved i.e. hidden from the user. The data and the services provided reside in massively scalable data centers and can be ubiquitously accessed from any connected device all over the universe.

Cloud computing gained popularity around October 2007, when IBM announced collaboration with the Google in this sphere. Thereafter IBM's announced the "Blue Cloud" concept. Since then, the term "Cloud Computing" starts gaining the popularity. Cloud computing is a computing paradigm, in which massively scaled IT resources are supplied as a service across the internet to multiple external customers and are billed by consumption. Many cloud computing providers have popped up and there is a considerable increase in the use of this concept. Google, Microsoft, Yahoo, IBM and Amazon have started offering cloud computing services among which Amazon is the pioneer in this field. It's a blessing for small companies like Smug Mug, which is an online picture hosting site, has used cloud services for the storing all the data and answering some of its services.

Similarly cloud computing is finding importance in several fields like web hosting, parallel batch processing, graphics rendering, financial modeling, web crawling, genomics analysis, and so on So now developers with innovative minds of new cloud services, no longer command the heavy capital expenditures in hardware to deploy their service or the human expense to run it. Since "Cloud computing" simply provides the latest technologies, IT services and software products as per demand to the organizations connected on the Clouds. This provides the power of on-demand computing to the organizations as the other on-demand utilities such as electricity, water. Now, users use a diverse range of devices, including PCs, laptops, smart phones, and PDAs to access programs, storage, and application-development platforms over the Internet, via services offered by cloud computing providers. Cloud computing acceptance is growing really rapidly. Most IT departments spend a major amount of time, money and energy on its IT infrastructure implementation, maintenance, and up gradation. So that now gradually more, IT giants as well as middle size organizations are moving to cloud computing technology, which minimizes their set up cost & time required to install all digital infrastructure.

Instantly simply by adopting cloud computing, IT professional is needed simply to concentrate on strategies not on engineering sciences which will boost up their revenues. Cloud computing is an emerging area within the field of information technology (IT). It is turning upside down the way we realize computation by enabling the use of storage, processing, or higher level factors such software applications, not by owning them and having them installed on computers that we possess - but rather to employ these resources simply as a serving.

The term cloud computing causes confusion due to the multiple aspects of service that it may include. From a genetic point of thought, it could be stated that cloud computing is a form of computing where scalable, adaptable, and elastic IT capabilities are offered as a service to multiple users. The best thing about the cloud computing is that now computing resources will be accessed & charged according to its usage, which will accomplish the organization need at comparatively low price. Thus, the users would not demand to know about clouds functioning and on demand technical service delivery. This technology replaces the actual physical infrastructure through virtual infrastructure which will be delivered through the cyberspace and then that it allocates resources according to the demand with ease of scalability.

Clouds appear to be a combination of clusters and Grids. However, this is not the case. Clouds are clearly next-generation data centers with nodes virtualized through hypervisor technologies such as VMs, dynamically "provisioned" on demand as a personalized resource allocation to satisfy a specific service-point understanding. Cloud computing has been built upon the development of distributed computing, grid computing and virtualization. Since the cost of each task in cloud resources is different to one another, scheduling of user tasks in the cloud is not the same as in traditional scheduling methods. So cloud computing, allowing organizations to reassess IT and reinvent the way they practice business. By adopting cloud philosophies, businesses can quickly incorporate and distribute services through cloud environments, increasing efficiency, improving business agility and turn down costs by 14%. Cloud service providers (CSPs) (e.g. Microsoft, Google, Amazon, Salesforce.com, GoGrid etc.) are applying the concept of virtualization for computing assets through the Internet.

In the study the main concerned of the organizations is the security which stood first among all the business organizations or corporate giants about cloud computing. The organizations & the IT professionals are mainly concerned about how security, privacy & reliability can be taken cared in Cloud Computing. Storing vital applications and important data to a shared cloud instead of preserving it in own place is a major decision for organizations those are adopting the cloud concept.

1.2 What exactly is Cloud Computing?

Everyone in this industry, from experts to cloud providers, owns their own definition about "cloud computing". There is not a common consensus for what precisely this term really stands for. Some of the existing definitions are analyzed which helps to clarify the term and what it implies.

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

"A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers".

1.3 Cloud Computing Evolution

Cloud computing is primarily an enhancement of distributed computing, utility computing and grid computing. The features of all above concepts are merged to provide the new business term. Basically, in cloud computing the computing tasks are passed out to many distributed computers, those may be local or remote hosts. Hence, the enterprises need to pay attention merely to the computing applications and can access the computer resources, software's and storage system according to its necessity.

So before we start with cloud computing, three concepts must be clearly understood those are

(i) Cluster computing

(ii) Grid computing

(iii) Utility computing

The History begins from the following technologies.

1.3.1 Cluster Computing

This is basically clustering of the coupled computers, to work in a group to achieve a single computing task by working closely equivalent of forging a single computer. In cluster computing, cluster stands for a group of interlinked local computers, those works together towards an exclusive end. The cluster components are not necessary, connected to each other through fast local area networks. This grouping of computers improves the public presentation, speed and availability as well as trimming the overall cost, instead of functioning over a super computer.

1.3.2 Grid Computing

Grid computing links various geographically distributed individual computers to establish a single large infrastructure. It merges the various computer assets from multiple administrative domains to fulfill a single computing task.

The primary differences between the grid computing from cluster computing are

(i) More loosely coupled

(ii) Heterogeneous

(iii) Geographically distributed.

The separate grids can be devoted to individual application; but a single grid can also be accessed from a mixture of different applications.

1.3.3 Utility Computing

Utility computing works to pay per use basis, i.e. paying for what you accessed and used from a shared pool of resources, e.g., storage system, software and servers like public utilities, water, electricity and gas etc. So utility computing is the wrapping up of computing resources as a metered service. This concept delivers the benefit of having negligible or no initial investment to access the various computing resources. Basically on this concept the computational resources are mainly rented as compared to the earlier scenario in which we wanted to purchase the products to avail the services.

This readiness of being helped as a utility became the foundation of the "On Demand" computing. The Utility Computing concept in well implemented in IT industry such as IBM, Microsoft, Sun and Amazon; provide CPU, computer memory media and virtual servers as a utility from last many years. IBM, HP and Microsoft were early giant leaders in the area of utility computing and they have put a great deal in the research work on working on the cloud architecture, payment arrangement and development challenges. Google, Amazon and others set out to take the lead in 2008, as they established their own utility services for computing, storage and applications. They have created virtual hosts and data center for IT systems to combine memory, I/O devices, and computer memory media to establish up a pool of scalable virtual resources.

1.3.4 Cloud Computing

Cloud computing permits users and systems to access their applications without any investment and installation and give them the ability to access their personal data on any computer by simply having an internet connection. This technology ensures additional computing power to the user by centralizing storage devices and server, which facilitate them a lot more processing speed. This technology just uses the net connection and centralized remote servers.

Yahoo mail, Gmail and other social networks the simplest and widely accepted example of cloud computing. We generally do not to worry about the implementation of any server to access them. The consumers just need an internet connection and you can start accessing the electronic mail inbox. All the management, including of servers and emails is done under the supervision of cloud service providers Yahoo, Microsoft, Google, etc. The consumer gets only to practice the software

interface and all remaining management will be attained by the cloud service provider itself. The users simply enjoy the benefits.

2 SCOPE OF THE RESEARCH:

In individuals and organizations store their private data on cloud servers. they expect complete privacy of their data stored in the cloud Protecting the privacy and data of users has remained a very crucial problem for cloud servers. numerous cryptographers presented many research works based on ABE Soon after its conceptualization, ABE reached prime importance in our daily life (for example, in television payment systems, personal health record systems . The legitimate users access data according to their attributes and can decrypt their ciphertexts or test the ciphertexts. If the legitimate users satisfy the access structure for the test, they can get the test results of the ciphertexts from the cloud server. If the legitimate users satisfy the access structure for the decryption, they can decrypt the ciphertexts. cryptosystem enriches the flexibility of the encryption policy and the description of users' rights.

3 AIM AND OBJECTIVE:

This project presents a new primitive called key-policy attribute-based encryption with equality test (KP-ABEwET). Our objective is to achieve a fine-grained authorization of ciphertexts. The main technologies in our scheme include keypolicy attribute-based encryption (KP-ABE) and public key encryption with equality test . Within the information security community, a lot of research efforts have been dedicated to cryptographic techniques supporting operations on encrypted data.

4 PROPOSED METHODOLOGY:

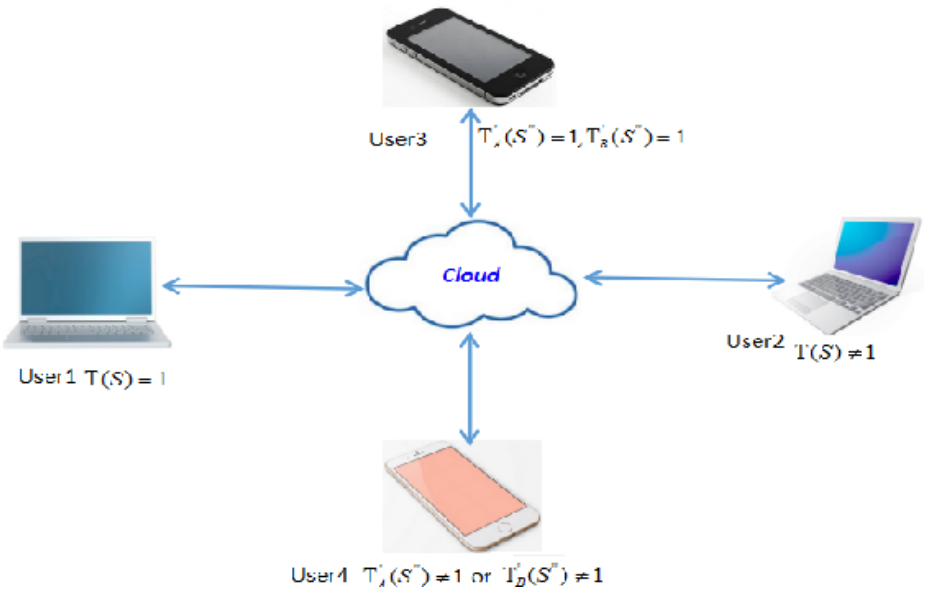
Key-Policy Attribute-Based Encryption With Equality Test (KP-ABEwET). It is a combine concepts of PKEwET and KP-ABE is to achieve a fine-grained authorization of ciphertexts. The main technologies in our scheme include keypolicy attribute-based encryption (KP-ABE) and public key encryption with equality test (PKEwET). It s supports performing the fine-grained test of ciphertexts and changes from one-one to one-many for users in the testing algorithm.

Advantages:

- Efficient user revocation for cloud Storage.
- Reduces communication overhead.

The security model of authorization is provided, and the security of authorization based on the ABE(Attribute based Encryption).

International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099
VOL 3 ISSUE 1 (2018) PAGES 1 - 11
Received: 10/07/2018. Published: 27/07/2018



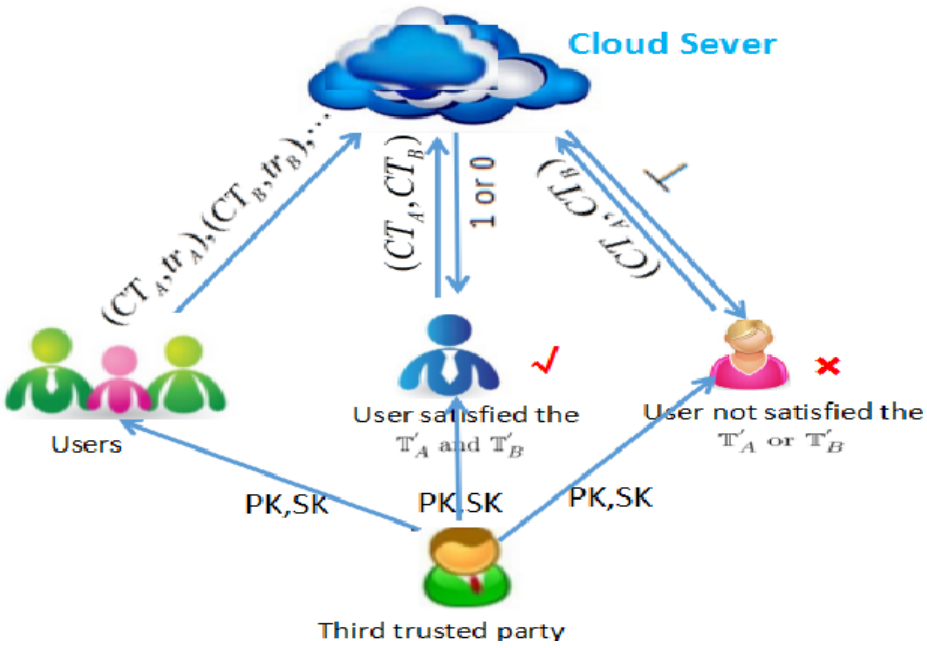
Example for KP-ABEwET

5 PROPOSED RESOURCE ALLOCATION METHOD:

The customer will evaluate a prospective service provider based on three main parameters: pricing approach, QoS, and utilization period. The pricing approach describes the process by which the price is determined.

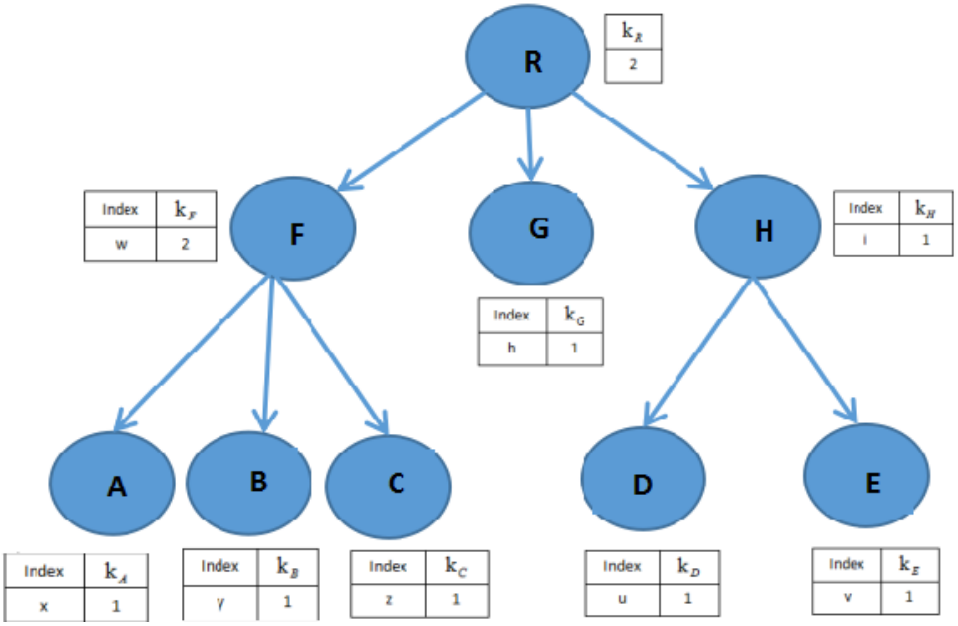
The pricing approach could be one of the following : fixed priced regardless of volume, fixed price plus per-unit rate, assured purchase volume plus per-unit price rate, per-unit rate with a ceiling, and per-unit price. The fixed price regardless of volume charges the customer a fixed price regardless of the volume of the service or product utilized. The fixed price plus per-unit charges the customer a fixed price plus a unit rate. In the assured purchase volume plus per-unit price rate, the customer pays a fixed price for a certain quantity. If the customer's utilization exceeds that quantity, the customer has to pay a fixed rate per unit for the extra utilization. In the per-unit rate with a ceiling approach, the customer pays the per-unit rate up to a certain limit. The provider will not charge the customer above that limit. In the price per unit approach, the customer is charged a different price per unit.

International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099
VOL 3 ISSUE 1 (2018) PAGES 1 - 11
Received: 10/07/2018. Published: 27/07/2018



Third Trusted Party

The quality of service describes the requirements for what a service provider should provide to his customers. QoS requirements include the availability of service, security, privacy, scalability, and integrity of the service provider. If the service provider ensures that these requirements are maintained at a high level, the quality of the service offered will increase. This will increase the number of customers and loyalty to the service provider.



Example Access Tree T

6 CONCLUSION

In this paper, we have constructed a new KP-ABE scheme supporting any monotonic access structure with constant-size ciphertext and proved that the proposed scheme is semantically secure in selective-set model based on the general Diffie-Hellman exponent assumption. The downside of the proposed KP-ABE scheme is that private keys have multiple size growths in the number of attributes in the access structure. One interesting open problem would be to construct a KP-ABE scheme with constant-size ciphertexts that is secure under a more standard assumption or which achieves a stronger full security notion. Another challenging problem is to construct a KP-ABE scheme with constant ciphertext size and constant private key size.

7 REFERENCES

[1] P. Mell and T. Grance, "The NIST denition of cloud computing," Special Publication 800-145, 2011. View at Google Scholar

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proceedings of the 5th ACM Symposium on Information, Computer and Communication Security (ASIACCS '10), pp. 261–270, April 2010. View at Publisher · View at Google Scholar · View at Scopus

[3] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494 of Lecture Notes in Computer Science, pp. 457–473, Springer, 2005.

[4] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," in Proceedings of the Annual International Cryptology Conference (CRYPTO '01), vol. 2139 of Lecture Notes in Computer Science, pp. 213–229, Springer, 2001.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89–98, November 2006. View at Publisher · View at Google Scholar · View at Scopus

[6] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 195–203, November 2007. View at Publisher · View at Google Scholar · View at Scopus

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of IEEE Symposium on Security and Privacy (SP '07), pp. 321–334, May 2007. View at Publisher · View at Google Scholar · View at Scopus

[8] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 456–465, November 2007. View at Publisher · View at Google Scholar · View at Scopus

[9] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proceedings of the 35th international colloquium on Automata, Languages and Programming, Part II (ICALP '08), vol. 5125 of Lecture Notes in Computer Science, pp. 579–591, Springer, 2008.

[10] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Proceedings of the International Conference on Practice and Theory in Public Key Cryptography (PKC '11), vol. 6571 of Lecture Notes in Computer Science, pp. 53–70, Springer, 2011.

[11] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," Journal of Computer Security, vol. 18, no. 5, pp. 799–837, 2010. View at Publisher · View at Google Scholar · View at Scopus.

