Survey on Dual Encryption with Attribute Authority in Cloud Computing

Kayalvili. S[1], Sowmitha. V[2]

[1]Dept. of CSE, Velalar College of Engineering &Technology, Tamilnadu, India,
[2]ME-CSE, Velalar College of Engineering &Technology, Tamilnadu, India,
Email: kayalvilis@gmail.com[1], sowmithav@gmail.com[2]

Abstract - Cloud computing enables users to accumulate their sensitive data into cloud service providers to achieve scalable services on-demand. Outstanding security requirements arising from this means of data storage and management include data security and privacy. And it requires the use of strong encryption techniques with fine-grained access control for data security in cloud computing. Attribute-based Encryption (ABE) is an efficient encryption system with fine-grained access control for encrypting out-sourced data in cloud computing. With the emergence of sharing confidential corporate data on cloud servers, data are generated by several organizations, and access policies can be defined by several authorities. Since data outsourcing systems require flexible access control approach Problems arises when sharing confidential corporate data in cloud computing. User-Identity needs to be managed globally. A trusty server is guilty of process and implementing access management policies. Simple trust relations have to be compelled to be fashioned by sharing the general public key between every attribute authority. In addition, fine-grained access control needs to be achieved. It can be done by dual encryption mechanism. Attributes need to be grouped. Each group should maintain own key. Users need to have one common group key and individual user key. RSA Encryption/Decryption Mechanism used in this project. Data is dual encrypted for more security and to maintain De-Centralization in Multi-Authority environment.

Keywords – ABE-Attribute Based Encryption; Trusted authority; revocation; outsourcing; Attribute level.

I. INTRODUCTION

Cloud computing is internet-based computing during which massive teams of remote servers square measure networked to permit sharing of data-processing tasks, centralized information storage, and on-line access to pc services or resources. Clouds are often classified as public, personal or hybrid. Cloud computing could be a kind of computing that depends on sharing computing resources instead of having native servers or personal devices to handle applications. The most sanctioning technology for cloud computing is virtualization. Virtualization software system permits a physical computer to be electronically separated into one or a lot of "virtual" devices, every of which might be simply used and managed to perform computing tasks. Cloud computing adopts ideas from Service familiarized design (SOA) which will facilitate the user break these issues into services which will be integrated to supply an answer. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained within the domain of SOA to permit international and simple access to cloud services in an exceedingly standardized means.

Cloud computing could be a quite cloud computing; it's evolved by addressing the QoS (quality of service) and dependableness issues. Cloud computing provides the tools and technologies to create data/compute intensive parallel applications with far more reasonable costs compared to ancient parallel computing techniques.

In basic ABE systems, the data shared is often at intervals one domain or organization. However, in reality, info likes drivers' licenses and registration info in universities area unit organized by totally different government departments. The management of attributes and key distributions can't be undertaken by an equivalent attribute authority. Moreover, access methods could also be distributed supported attributes of various authorities. Therefore, leveled multi-authority ABE cannot meet distribution demands. Distributive multi-authority ABE is employed to unravel the access downside during which user attributes belong to totally different authorities. Those authorities take issue from that for a leveled multi-authorized ABE, that the leveled multi-authority ABE has one trust root. There's no trust between organizations, and attribute management and key distribution continually area unit performed on an individual basis from one another.

For some specific work reasons like sharing confidential company information on cloud servers, trust relationships is created between organizations. Single-authority ABE primarily randomizes non-public keys, and

also the secret values area unit separated supported the half within the users' non-public keys (referring to a distinct attribute), and coding is performed by reconstructing the key values. In Single-authority ABE, every user's keys area unit generated victimization totally different random and on the QT shared values specified keys generated for various users can't be combined, that prevents collusion attacks. For distributive multi-authority ABE, the non-public keys of users are generated by totally different authorities that don't communicate. Thus, the crucial technical challenge for distributive multi-authority ABE is constructing a secret sharing price to resist collusion attacks.

The Global symbol (GID) and central authority originated to resolve the resist collusion attacks. All early schemes used central authority to deliver secret cacophonic, thereby reassuring collusion resistant below circumstances whereby authorities don't trust each other. However, a central authority ought to be globally trustworthy. Therefore, so as to avoid the protection weaknesses ensuing from the employment of central authorities, schemes that don't use central authorities are revealed. There's no reliance on single trust centre, and though every authority distributes its own attributes and keys, they still want common support parameters for distribution by connected organizations, or sophisticated trust relationships have to be compelled to be fashioned between every authority. User's GID is revealed globally in early schemes can breach the user privacy. So as to resolve the question, some schemes used anonymous key supply protocol to reinforce user privacy, however the protocols typically square measure advanced.

The main objective of this paper isn't to use a central authority to manage users and keys, and solely straightforward trust relations have to be compelled to be fashioned by sharing the general public key between every attribute authority (AA). User identities square measure distinctive by combining a user's identity with the identity of the AA wherever the user is found. Once a key request has to be created to associate authority outside the domain, the request has to be performed by the authority within the current domain instead of by the users, so, user identities stay personal to the AA outside the domain, which is able to enhance privacy and security.

In addition, the key supply protocol between AA is easy because the results of the trust relationship of AA. Moreover, extensibility for authorities is additionally supported by the theme given during this work and it ought to provide some enhancements by combining a user's identity with the identity of the Attribute Authority (AA) wherever the user is found. This results in distinctive user identifiers globally, and also the drawback of collusion resistance may also be solved. Here, once the user ought to requests associate attribute secret key, if the attributes square measure situated outside the domain, the request by the supply AA within the domain to the target AA is employed instead of by requests by users themselves. So, user identities stay personal to the AAs outside the domain, so avoiding privacy speech act. The key supply protocol between AAs is easy as results of the trust relationship of AAs. On the opposite hand, victimization the AA rather than users to initialize attribute requests will greatly improve potency and security.

II. RELATED WORKS

A. Data Outsourcing Architecture Combining Cryptography and Access Control

The recent adoption and diffusion of the information out-sourcing paradigm, wherever knowledge house owners store their knowledge on external servers, there are increasing general demands and issues for knowledge confidentiality. Besides well-known risks of confidentiality and privacy breaks, threats to out-sourced knowledge embody improper use of information: the server may use substantial components of a set of knowledge gathered and arranged by the information owner, doubtless harming the information owner's marketplace for any professional duct or service that comes with that assortment of data. The projected novel access management model and design that eliminates the necessity for a reference monitor and depends on cryptography to make sure confidentiality of knowledge hold on a server. Knowledge area unit encrypted because the knowledge owner stores them on associate in nursing external server. Authorizations and coding area unit united therefore permitting access management social control to b e outsourced beside the information. The nice advantage is that the information owner, whereas specifying the policy, wants not b e concerned in its social control.

B. Mediated Cipher text-Policy Attribute-Based Encryption and Its Application

Distributed data systems need versatile access management models that transcend discretionary, necessary and role-based access management. The recently projected models, like attribute-based access management, outline access management policies supported completely different attributes of the requester, setting, or the information object. On the opposite hand, the present trend of service-based data systems and storage outsourcing need enhanced protection of knowledge together with access management ways that area unit cryptographically implemented. The conception of Attribute-Based coding (ABE) fulfills the same necessities. It provides a chic manner of encrypting knowledge such the encryptor defines the attribute set that the decryptor has to posses so as to decrypt the cipher-text. Projected the fundamental ABE theme, many additional advanced schemes are developed, like most notably

Cipher text-Policy ABE schemes (CP-ABE). In these schemes, a ciphertext is related to associate in nursing access policy and therefore the user secret keys related to a collection of attributes. A secret key holder will decipher the cipher text if the attributes related to his secret key satisfy the access policy related to the cipher text.

C. Persona: An Online Social Network with User-Defined Privacy

These net-works help users share information with their friends. However, users entrust the social network provider with such personal information as sexual preferences, political and religious views, phone numbers, occupations, identities of friends, and photographs. Although sites over privacy controls that let users restrict how their data is viewed by other users, sites provide insufficient controls to restrict data sharing with corporate affiants or application developers. Not only are there few controls to limit information disclosure, acceptable use policies require both that users provide accurate information and that users grant the provider the right to sell that information to others.

D. Fuzzy Identity-Based Encryption

In this paper, discussed the use fullness of using biometric s in Identity-Based and then discuss their contributions. Using biometrics in Identity- Based Encryption in many situations, using biometric–based identity in an IBE system has a number of important advantages over "standard" IBE. They argued that the use of biometric identities fits the framework of Identity-Based Encryption very well and is a very valuable application of it. First, the process of obtaining a secret key from an authority is very natural and straightforward. In standard Identity-Based Encryption schemes a user with a certain identity, for example, "Bob Smith", will need to go to an authority to obtain the private key corresponding to the identity. In that process the user will need to "prove" to the authority that he is indeed entitled to this identity. That will typically involve presenting supplementary documents or credentials. The type of authentication that is necessary is not always clear and robustness of this process is questionable (the supplementary documents themselves could be subject to forgery). Typically, there exists a trade-off between a system that is expensive in this step and one that is less reliable.

E. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

There is a trend for sensitive user data to b e stored by third parties on the Internet. For example, personal email, data, and personal preferences are stored on web portal sites such as Google and Yahoo. The attack correlation center, dshield.org, presents aggregated views of attacks on the Internet, but stores intrusion reports individually submitted by users. Given the variety, amount, and importance of information stored at these sites, there is cause for concern that personal data will be compromised.

III. METHODOLOGY

In this paper, each AA has public and secret keys, private key of attribute do not require, which reduce the quantity of key. Only when the system is set up, the public key of each AA and the basic parameters are distributed, which simplifies the process of trust establishment. The key issuing protocol for privacy only needs to use the public key of AA to realize the trust between AA. Modern data outsourcing systems require flexible access control approaches. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles. Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. Cipher text-policy attribute-based encryption is a promising cryptographic solution to these issues for enforcing access control policies defined by a data owner on outsourced data.

However, the problem of applying the attribute-based encryption in an outsourced architecture introduces several challenges with regard to the attribute and user revocation. So the project also proposes an access control mechanism using cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. This work demonstrates how to apply the proposed mechanism to securely manage the outsourced data. The analysis results indicate that the proposed scheme is efficient and secure in the data outsourcing systems.

The data outsourcing scenario challenges the approaches of traditional access control architectures such as reference monitor, where a trusted server is in charge of defining and enforcing access control policies. This assumption no longer holds in modern data outsourcing systems, because users want to be able to share private contents with a group of people they selected and to define some access policy and enforce it on the contents. Thus, it is desirable to put the access policy decisions in the hands of the data owners.

Recently proposed access control models, such as attribute-based access control, define access control policies based on different attributes of the requester, environment, for the data object. In addition, the current trend of storage outsourcing requires increased protection of data including access control methods that are cryptographically enforced.

The concept of attribute-based encryption (ABE) is a promising approach that fulfills these requirements. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the cipher text.

Thus, different users are allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access. However, the problem of applying the ABE to the data outsourcing architecture introduces several challenges with regard to the attribute and user revocation. The revocation issue is even more difficult especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, it is referred to such a collection of users as an attribute group). This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group.

It may result in bottleneck during rekeying procedure or security degradation in the system. This project attempts to solve these problems in attribute-based data access control using CP-ABE for data outsourcing systems. Recently, several attribute revocable ABE schemes have been proposed. They realize revocation by revoking attribute itself using timed rekeying mechanism, which is implemented by setting expiration time on each attribute. A coarse-grained revocation is called because the immediate rekeying on any member change could not be possible.

Indeed, these approaches have two main problems. First problem is the security degradation in terms of the backward and forward secrecy. An attribute is supposed to be shared by a group of users in the ABE systems by nature. Then, it is a considerable scenario that membership may change frequently in the group that shares an attribute. Then, a new user might be able to access the previous data encrypted before he comes to hold the attributes until the data are re-encrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). On the other hand, a revoked user would still be able to access the encrypted data even if he does not hold the attribute any more until the next expiration time (forward secrecy). Such an uncontrolled period is called the window of vulnerability.

The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time slot so that all of the nonrevoked users can update their keys. This could be a bottleneck for both the key authority and all nonrevoked users. It is observed that this is deteriorated due to the fact that the previous revocations were done without any consideration of the scalable distribution of the updated attribute keys to the group of users who share the attributes. Thus, it is argued that it is still a pivotal open problem to design a scalable and fine-grained revocation mechanism in the data outsourcing architecture using ABE, which is one of the problems.

Cipher Text-Policy Attribute-Based Encryption with User Revocation

A. Step 1: The setup algorithm is executed which is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public key PK and a master key MK.

B. *Step 2:* The attribute key generation algorithm is executed which takes input the master key MK, a set of attributes $\Lambda \subseteq \Lambda$, and a set of user indices $Y \subseteq \upsilon$ as parameters. It outputs a set of private attribute keys ΣK for each user in that identifies with the attributes set.

C. Step 3: The key encrypting key (KEK) generation algorithm is executed in this module, which takes a set of user indices $Y \subseteq \upsilon$ as input, and outputs $KEK\sigma$ for each user in , which will be used to encrypt attribute group keys $K_{\lambda\iota}$ for each $\Gamma\iota \in \Gamma$.

D. Step 4: An encryption algorithm (which is a randomized algorithm) that takes as input the public parameter PK, a message M, and an access structure 'A' over the universe of attributes. It outputs a cipher text CT such that only a user who possesses a set of attributes that satisfies the access structure will be able to decrypt the message.

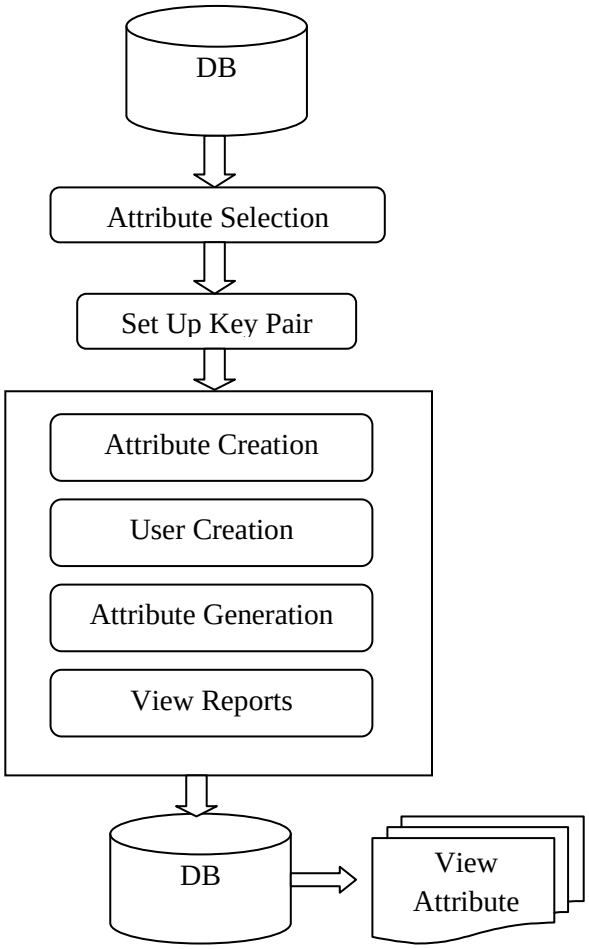

Fig. 1 Attribute Selections

E. Step 5: The re-encryption algorithm is a randomized algorithm that takes as input the cipher text CT including an access structure 'A', and a set of attribute groups G. If the attribute groups appear in 'A', it re-encrypts CT for the attributes; else, returns. Specifically, it outputs a re-encrypted cipher text CT' such that only a user who possesses a set of attributes that satisfies the access structure and has a valid membership for each of them at the same time will be able to decrypt the message.

F. Step 6: The decryption algorithm is executed which takes as input the cipher text CT' which contains an access structure 'A', a private key SK, and a set of attribute group keys K_Λ for a set of attributes Λ. The decryption can be done if Λ satisfies 'A' and K_Λ is not revoked for any $\lambda \in \Lambda$.

G. *Step 7:* If the data contains most important information and in order to protect the data security, more privileged service providers view most of the data and less privileged service providers view limited data.

IV. ENCRYPTION MODEL

A. Encryption Form

This module is used to encrypt the text using public key for the purpose of other users who do not know the given message. So, the public key is extracted using get key command button and displayed in the label control, the message is entered in the textbox control then the given encrypted message is displayed in the label control. The encrypted message is saved in the application using creates cipher text and save command button event.

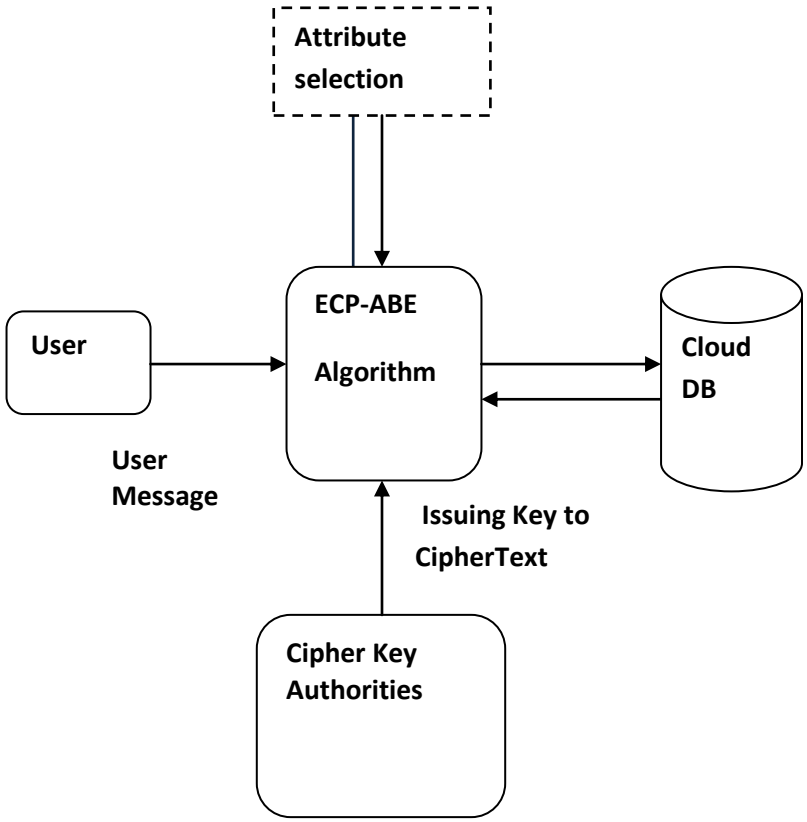

Fig. 2 Encryption Form

B. Decrypt Cipher Text

Decrypt cipher text retrieves the plain data in the application. The given cipher text is entered the data is showed to the user. In this form user identity number and cipher texts are selected from the combo box control, group identity is displayed in the label controls. The message is decrypted in the cipher text grid view control using the decrypt command button event.

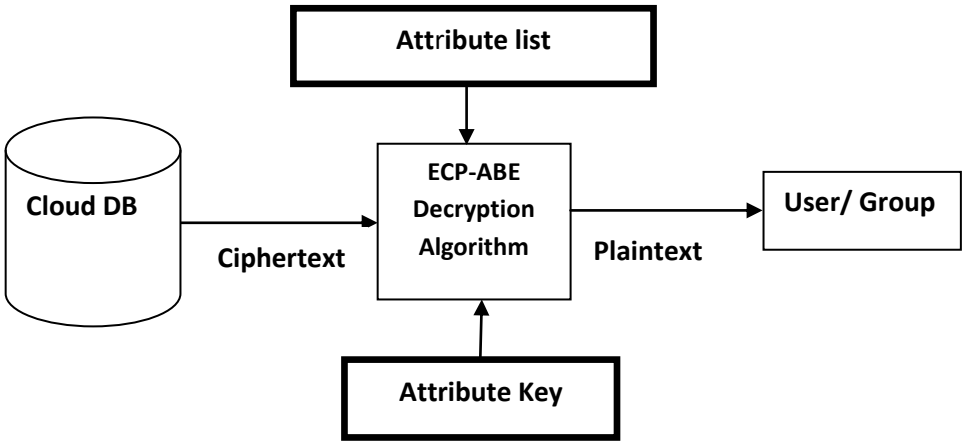

Fig. 3 Attribute Decryption Model

V. CONCLUSION

- Authorization policies and the support of policy updates are studied.
- Proposes a cryptographic approach for communication between users and attribute authorities.
- Allows a data owner to define the access control policy and enforce it on his outsourced data.
- Efficient and scalable to securely manage the outsourced data.

The future of the research work will be as follows. It allows a data owner to define the access control policy and enforce it on his outsourced data. It also features a mechanism that enables more fine-grained access control with efficient attribute and user revocation capability. The proposed scheme will be efficient and scalable to securely manage the outsourced data. The new system become useful if the below enhancements are made in future. The new system is designed such that those enhancements can be integrated with current modules easily with less integration work and it becomes useful if the above enhancements are made in future.

REFERENCES

[1] S. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "A Data Outsourcing Architecture Combining Cryptography and Access Control," Proc. ACM Workshop Computer Security Architecture, Nov. 2007.

[2] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application," Proc. Int'l Workshop Information Security Applications, pp. 309-323, 2009.

[3] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: An Online Social Network with User-Defined Privacy" Proc. ACM SIGCOMM '09, Aug. 2009.

[4] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Eurocrypt '05, pp. 457-473, 2005.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[6] J. Anderson. Computer security planning study. Technical Report 73-51, Air Force Electronic System Division, 1972.

[7] J. Saltzer and M. Schro eder. The protection of information in computer systems. Communications of the ACM, vol. 17, no. 7, 1974.

[8] N. Provos . Encrypting virtual memory. In Proc. of the 9th USENIX Security Symposium, Denver, Colorado, USA, August 2000.

[9] A. Harrington and C. Jensen. Cryptographic access control in a distributed system. In Proc. of the 8th SACMAT, Como, Italy, June 2003.

[10] S. Akl and P. Taylor. Cryptographic solution to a problem of access control in a hierarchy. ACM TOCS, vol. 1, no. 3, 2007.

[11] J. Crampton, K. Martin, and P. Wild. On key assignment for hierarchical access control. In Proc. of the 19th IEEE CSFW'06 , Venice, Italy, July 2006.

[12] G. Miklau and D. Suciu. Controlling access to published data using cryptography, In Proc. of the 29th VLDB Conference, Berlin, Germany, September 2003.

[13] H. Hacig Äum Äus, B. Iyer, and S. Mehrotra. Providing database as a service, In Proc. of 18th ICDE, 2002.

[14] R. Agrawal, J. Kierman, R. Srikant, and Y. Xu. Order preserving encryption for numeric data, In Proc. of ACM SIGMOD 2004, Paris, France, June 2004.

[15] E. Damiani, S. De Capitani di Vimercati, S. Foresti, S. Ja jo dia, S. Parab oschi, and P. Samarati. An exp erimental evaluation of multi-key strategies for data outsourcing, In Proc. of the 22nd IFIP International Information Security Conference, 2007.

[16] A. Sahai and B. Waters. Fuzzy identity-based encryption. In Advances in Cryptology, vol. 3494, pp. 457-473, 2005.

[17] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption, Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp. 321-334, 2007.