

ENHANCING DATA SECURITY IN CLOUD ENVIRONMENTS THROUGH ATTRIBUTE-BASED ENCRYPTION

¹**Vinayak. G**

¹Research Scholar, Department of Computer Science, Arunodaya University, Lekhi Village, Naharlajun, Itanagar – Dt: Papum Pari, Arunachal Pradesh - 791110

²**Dr. Annamali Giri**

²Assistant Professor, Department of Computer Science, Arunodaya University, Lekhi Village, Naharlajun, Itanagar – Dt: Papum Pari, Arunachal Pradesh - 791110

ABSTRACT

This study presents a new Secure Cloud File System (SCFS) that enhances the security of file sharing in cloud environments. It does this by utilising Cipher text-Policy Attribute-Based Encryption without Pairing (CP-ABE-WP). As cloud computing continues to gain popularity, there is an increasing demand for effective data management and access control. The suggested SCFS framework makes use of attribute computing to give users a dynamic and adaptable way to share data, allowing them to easily manage their access privileges and permissions according to specified attributes. Our security investigation shows that the CP-ABE-WP approach can resist chosen-plaintext attacks, so any sensitive data will remain protected. When compared to traditional attribute-based encryption methods, the CP-ABE-WP model significantly outperforms them in terms of computational cost while retaining strong security features. By providing a practical and extensible method for safe file sharing, this study contributes to the field of secure cloud computing, which aims to enhance user agency and confidentiality in cloud-based data management systems.

Keywords: Data Security, Cloud Environments etc.

INTRODUCTION

Now that cloud computing has arrived, companies may store, manage, and retrieve data from remote servers rather than using outdated on-premises systems. The scalability and flexibility of cloud services may help businesses of all sizes streamline their operations, cut costs, and improve resource management. The emergence of cloud providers like AWS, Microsoft Azure, and Google Cloud Platform has made it easier than ever for organisations to adjust their infrastructure to meet evolving demands without investing much in new hardware. As a result of this paradigm shift, innovation has been possible in previously unimaginable areas, such as data security, privacy, and regulatory compliance. The security risks associated with relying on cloud infrastructure are substantial. Organisations must ensure the security of sensitive information in environments over which they have no control when migrating to the cloud. Since traditional security measures target the physical assets and private networks of an organisation, they are useless in decentralised, shared-resource cloud systems. Hackers are increasingly taking advantage of vulnerabilities in cloud infrastructures to commit data breaches, unlawful access, and leaks, making it imperative to reevaluate data security procedures. Data security systems must be designed to be both effective and scalable if they are to maintain user confidence, comply with regulations, and safeguard sensitive information and intellectual property.

Attribute-Based Encryption (ABE)

Recently, Attribute-Based Encryption (ABE) has emerged as a promising alternative to traditional cloud encryption methods, which have their limitations. In contrast to the conventional methods that focus on identity-based access control, ABE allows data owners to implement access limitations based on user variables such as position, department, or region. When dealing with data shared among several users with different expectations, this form of access control is quite helpful in cloud settings since it offers a more flexible and granular approach. By associating decryption keys with certain properties, ABE allows users to access data if their characteristics match the access policy defined by the data owner. The two main types of ABE are Key-Policy Attribute-Based Encryption (KP-ABE) and

Ciphertext-Policy Attribute-Based Encryption (CP-ABE). Users can only decrypt data if their key attributes match the policy, as the access policy is contained in the decryption key in KP-ABE. In contrast, CP-ABE allows data owners to encrypt their data with access policies included in it, limiting access to just those individuals whose attributes fit the policy. Both methods allow businesses to strengthen security while streamlining key management through the definition of complex access controls based on user attributes rather than individual identities. Access control is improved by this.

The Value of ABE in Ensuring the Security of Cloud Data

Because data access requirements in cloud environments are often complex and dynamic, ABE is well-suited to these types of situations due to its versatility. Businesses may restrict data access to permitted individuals who meet specific criteria by implementing granular access control using ABE. Both the data and the risks associated with key distribution are mitigated by this strategy, which bases access on user traits instead of shared keys. It is critical to secure data in distant, multi-tenant cloud environments, and ABE enhances security by including attribute-based access control. Traditional encryption methods have scalability problems, however ABE solves some of those problems as well. Large businesses may find it exceedingly difficult to handle encryption keys for thousands of individuals when their jobs and access requirements change over time. Without reencrypting data or interrupting approved users' access, organisations may easily alter their access restrictions and attribute-based keys using ABE. Since of its scalability, ABE is attractive to organisations with large cloud operations since it helps them reduce administrative overhead while improving data security.

The significance of establishing strong data security protocols

With record-high cloud usage comes an extreme focus on data availability, integrity, and secrecy. Cloud storage has become an integral part of modern enterprises, housing a wide variety of data types such as customer records, financial records, vital intellectual property, and medical records. There is no way to overstate the need of robust data protection for industries handling highly sensitive data, such as healthcare, finance, and government. In addition to the evident danger to data integrity, organisations confront regulatory, legal, and reputational concerns in the case of a breach. Regulatory frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) impose stringent requirements on organisations to safeguard personal information and impose severe fines for violating these standards. There has been a lot of use for symmetric and asymmetric encryption, two of the first methods of data protection. These tactics are important, but they can't handle the various users and frequent changes that cloud systems bring. Traditional encryption solutions do not offer enough support for granular access control when several users with different needs share data. Because it gets much more complex to maintain track of encryption keys and user permissions, security flaws become more obvious as cloud systems increase. This gap has been filled by Attribute-Based Encryption (ABE), which is suitable for multiuser, widely distributed cloud environments.

REVIEW OF LITERATURE

Apurva R. Naik (2016) Social networking and growing popularity of cloud services have made everyone to communicate each other in an easiest way. File sharing and distribution are the frequently used services provided by cloud service providers, although these facilities reduce cost of data sharing but at the same time data security and access control is the major problem. Many renowned service providers have faced the challenges to secure data and provide better access control, and we know once the data is leaked we cannot recover the data loss. Thus in order to ensure better security we need to focus on the two major problems, and those are access control and encryption policy. Cipher text policy attribute based encryption is the most effective solution for access control in real time scenarios where owner can actually decide the access rights for the enduser, but it comes with key escrow problem. We are proposing our modified escrow-free key issuing protocol to solve the problem of key escrow and our Modified Attribute Based Encryption scheme to achieve all security requirements to get a robust and secure system. Further we evaluate our model on the basis of results and lastly we conclude the paper.

Zhu Shuaishuai (2015) When compared to current cloud-based solutions, traditional file systems are woefully inadequate in terms of flexibility, granular access control, and robust security. Here, we

provide a method for safe file sharing that is based on attribute control. In order to construct a working cloud file system utilising Attribute-Based Encryption (ABE), we offer a systematic approach to cloud attribute computing. We provide a Ciphertext-Policy ABE (CP-ABE-WP) scheme that integrates into a secure and fast file system and eliminates the requirement for pairing, therefore facilitating safe and efficient data transfer in the cloud. The findings show that the approach is fast, selectively secure against plaintext assaults, and meets all the requirements for cloud file-sharing.

Raya Lakshmi G.V (2014) Cloud computing is a new paradigm that offers a variety of IT services; yet, there are significant obstacles to its spread related to security and privacy. Use of cloud services for real-time, mission-critical applications is disproportionately affected by these difficulties. The first step of this research is to examine and contrast the various Attribute-Based Encryption (ABE) methods. An new ABE-based encryption system that utilises digital signatures, asymmetric encryption, and hash functions is next proposed as a means to further enhance cloud security. Our approach provides a streamlined yet effective strategy for cloud applications that are mission-critical.

OBJECTIVE OF THE STUDY

1. To Strengthening cloud data security via Attribute-Based Encryption (ABE).
2. To Data Security in the Cloud: An Analysis of Attribute-Based Encryption

METHODOLOGY

This approach shows how to use CP-ABE-WP to show how to use attribute-based encryption (ABE) to share files securely in the cloud. To improve security, we have streamlined licence administration, given priority to three types of data exchange, and substituted efficient polynomial operations for bilinear pairings. The model outperforms conventional ABE systems.

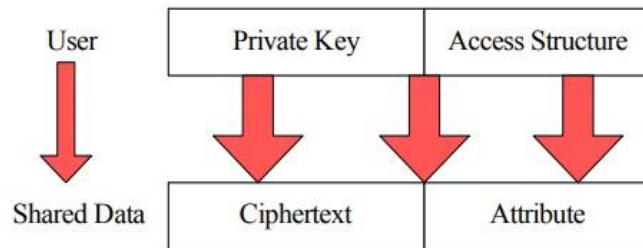
A new paradigm for exchanging files on the cloud

First, there is fragmented data, which consists of private information exchanged between friends; second, anonymous data, which is data shared between users all over the globe; and third, sustaining data, which allows users to access databases from anywhere in the world. Conventional methods of access control are ineffective when dealing with cloud data due to its dynamic nature. An option that has been proposed involves assigning individuals access rights based on specific qualities. When users share, they send these sets to a central server, which then allows access to capabilities like safe decryption.

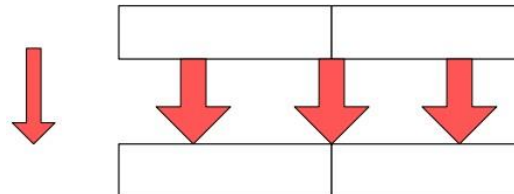
Table: 1 Files stored and shared online

| Instance | Data Sharing Type |
|-------------------|-------------------|
| P2P Software | Fragmentary Data |
| Social Network | Anonymous Data |
| data warehouse | Sustaining Data |
| Cloud Environment | |

In a cloud environment, the two most common kinds of objects are entities and data; to describe the relationships between these, access restrictions and attributes are utilised. Both characteristics, which characterise the states of objects, and access control, which defines the relationships between items, allow for the safe transfer of data. The static attributes, security settings, and activity descriptions that are part of each user's license serve as identifying and control information. In contrast to the older key-policy ABE, which associates user keys with access structures, the newer ciphertext-policy ABE associates characteristics with ciphertext. This idea enables creating, managing, and sharing files on the cloud a safe proposition by merging attribute computing with ciphertext-based access control.



(a) The linked KP-ABE structure



(b) This structure associated with KP-ABE Definitions and Security Model:

1. **Result: 1** The ciphertext is connected to the access structure, and a user's private key is linked to their attributes in ciphertext-based access control.
2. **To elaborate:** Attribute obtain, attribute disseminate, attribute deduce, and attribute revoke are the four primary ways of attribute computing in a cloud environment that are used to produce and control the actions of entities.

The chosen-plaintext attack is prevented by this system's security paradigm, which is based on the selected attribute set notion. To communicate with a challenger, an attacker selects a set of qualities and then utilises a series of key queries and encryption. One way to win is for your opponent to guess which side your challenger will choose. An ABE approach can be considered safe if the opponent's advantage is limited.

Initiative: CP-ABE-WP This pairing-free ABE system enhances performance in attribute-based encryption by evading bilinear pairings on a prime-order cyclic group (G), a generator (g), and a bilinear map (e).

$$\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}, i \in Z_p$$

that is, the Lagrange coefficient, and

$$S \subset Z_p. \text{ Let } H: \{0,1\}^* \rightarrow G$$

Serve as a hash algorithm

(K) is the access tree threshold, which controls the amount of users permitted into the shared group. Method for setting up: To determine this, take the set (\mathbb{Z}_p) and randomly select two values, (α) and (β):"

$$PK = (G, g, h = g^\beta, t = g^\alpha)$$

$$MK = (\alpha, \beta)$$

To encrypt (PK, m, T), begin at the root node of the access tree T and assign a polynomial q_x with a degree of $dx = k_x - 1$. Here, k_x is the threshold of node x . Select s from the set of all permutations of p in the set of all permutations of \mathbb{Z}_p , and then set $q_R(0) = s$ for the root node. Using the formula $q_x(0) = q_{parent(x)}(0)$, give each child node x a starting value for q_x . Then, pick values at random for the remaining q_x coefficients. The term Y is defined as a set of T leaf nodes. Then, we determine the ciphertext E_T by using the T structure and the provided polynomials.

$$E_T = (T, C' = m \cdot t^s, C = h^s, \forall y \in Y :$$

$$C_y = (t \cdot h)^{q_y(0)}, C' = H(att(y))^{q_y(0)})$$

The algorithm KeyGen (γ) will create a secret key for the user that is associated with the characteristics in (γ) when given a set of attributes (γ) and a master key (MK).

Step one is to randomly select an integer (r from \mathbb{Z}_p). Furthermore, for every attribute (j in γ), choose an integer at random from the collection \mathbb{Z}_p . To determine the secret key, one must follow these steps:

$$SK = \left(D' = g^{(\beta+r)s}, \forall j \in \gamma: D_j = \left(g^{(r+r_j)} \cdot H(j) \right)^{q_x(0)}, D'_j = g^{r_j} \right)$$

The goal of this iterative process is to use the secret key SKSKSK and the set of properties γ to decode the encrypted message ETETET. This method will return \perp unless the condition $TK(\gamma) \geq 0$ is met, in which case it will output the message mmm. The inner workings of the algorithm are detailed below. The recursive function may be defined as $Dec_Node(ET, SK, x)$, where xxx is a node in the access tree. This function converts input into a GGG group value. Assuming x is a leaf node, let iii be the property that guarantees i is a member of γ . The decryption algorithm may be calculated in this way:

$$Dec_Node(ET, SK, x) = \begin{cases} \frac{D_i \cdot C_x}{D'_i \cdot C'_x} = \frac{g^{(r+r_i)q_x(0)} \cdot H(i)^{q_x(0)} \cdot h^{q_x(0)} \cdot g^{\alpha \cdot q_x(0)}}{g^{r_i \cdot q_x(0)} \cdot H(i)^{q_x(0)}} = g^{(\alpha+r+\beta) \cdot q_x(0)} \\ \perp \end{cases}$$

If x is not a leaf node, then for every child node z in the set of child nodes, we compute $F(z, ET, SK) = Dec_Node(ET, SK, z)$. The given function $F(z, ET, SK)$ is equal to the text $\{Dec_Node\}(ET, SK, z)$. Applying the formula $Dec_Node(ET, SK, z)$ yields $F(z, ET, SK)$.

The index of node xxx is represented as $index(x)$ if the set $SX \subseteq Z$ is such that $SX \cap X = kX$. The definition of Set S_x should be $\{index(z): z \in SX\}$. The index of the set S_x equals the value of z. This operation produces the set $S_x = \{index(z): z \in SX\}$. This is the procedure for performing the calculation:

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_z^{\Delta_{i, S_x}(0)} \\ &= \prod_{z \in S_x} \left(g^{(\alpha+r+\beta) \cdot q_z(0)} \right)^{\Delta_{i, S_x}(0)} \\ &= \prod_{z \in S_x} \left(g^{(\alpha+r+\beta) \cdot q_{parent(z)}(index(z))} \right)^{\Delta_{i, S_x}(0)} \\ &= \prod_{z \in S_x} \left(g^{(\alpha+r+\beta) \cdot q_z(0)} \right)^{\Delta_{i, S_x}(0)} \\ &= g^{(\alpha+r+\beta) \cdot q_x(0)} \end{aligned}$$

If we know the square root of T, we can find C Dec. $\square\square\square_ \square\square(\) , , r s$
 Find the value of m at the node (E T SK x) and at the intersection of g T and r s.

Implementing Attribute Computing for Cloud File Security (SCFS)

An optimisation for cloud contexts, Secure Cloud File System (SCFS) retains key characteristics of traditional file systems, including data management, access control, and resource allocation. Despite its greatness, cloud file systems like GFS and HPFS may lack some characteristics necessary for safe data transport. To provide a more versatile data-people mapping, our method employs attribute computing in conjunction with the CP-ABE-WP scheme.

Important parts of the SCFS comprise:

Public parameters are created by the authoritative server using the setup () function, and users are assigned PKs and namespace rules during system initialisation. The sender uses $encrypt(PK, m, T)$ to encrypt data before uploading it to a cloud storage provider.

The authoritative server can retrieve the static characteristics of the sender and recipient using $Attribute_Get(IDs, IDr)$.

The license for access control is created by using the static attribute sets of the sender (γ') and the receiver (γ).

$$\left(\gamma', \gamma'', t_1, t_0, PK, \dot{SK} \right),$$

in which $\dot{SK} = (D', \forall i \in \gamma' : D_i, D'), t_0$ The file request will be processed by the authority server, who will then generate and provide the licence. A file's expiration time ($t_1 = 0$) will not be enforced if it is free. The receiver requests a license to decrypt data during the Attribute Deduce method. Once validated, the receiver can view the decrypted communication in the cloud. In the case that the current time ($t_c > t_1 > 0$) is greater than zero, Attribute Revoke disables the license, prohibiting the receiver and anybody else with the same license from continuing the decryption process.

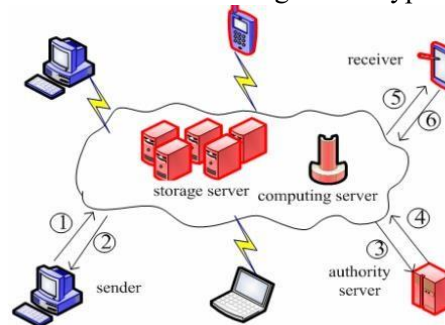


Figure: 1 SCFS Structure

THEORETICAL ANALYSIS

A selective ID model proves that the decisional BDH problem is hard, which is the basis for the CPABE-WP system's security. In the event that a competitor figures out the approach, the BDH problem is likely to be solved by a simulator. The antagonist (A) approaches the hero (Ch) in a challenge game and requests the hidden keys to certain sets of qualities as part of their interaction. During the challenge phase, (A) transmits two messages and (Ch) randomly selects one to encrypt. After more enquiries, (A) makes a well-informed guess as to which message was encrypted. Based on the CPA security criteria of the selected model, the approach is deemed secure since (A) maintains a little advantage in this game.

$$P(\text{Event 1}) = \frac{C_0}{C - n - q};$$

$$P(\text{Event 2}) = \left(1 - \frac{C_0}{C} \right) \cdot \frac{C - (n + q)}{C_1};$$

$$P(\text{Event 3}) = P(\text{DBDH Problem}).$$

Very little probability exists that Event 3 will take place, as it involves solving the discrete logarithm issue.

$$\begin{aligned} P[b' = b] &= P(\text{Event 1}) + P(\text{Event 2}) \\ &= \frac{C_0}{C - n - q} + \left(1 - \frac{C_0}{C} \right) \cdot \frac{C - (n + q)}{C_1} \\ &\leq \frac{C_0}{C - (|R_1| + |R_2|)} + \frac{C - (|R_1| + |R_2|)}{C} \\ &= \frac{CC_0 + C_1(C - (|R_1| + |R_2|))}{(C - (|R_1| + |R_2|))C} \\ &\leq \frac{1}{2} + \frac{C_0}{C} - \frac{(|R_1| + |R_2|)}{C_1} \end{aligned}$$

Then, one may find out the enemy's advantage, which is represented as $\epsilon(A)$.

$$\begin{aligned} \left| P[b' = b] \frac{1}{2} \right| &= \frac{1}{2} + \frac{C_0}{C} - \frac{(|R_1| + |R_2|)}{C_1} - \frac{1}{2} \\ &= \frac{C_0}{C} - \frac{(|R_1| + |R_2|)}{C_1} \end{aligned}$$

Theoretically, adversary AAA has a very low chance of picking the right ID since the selective ID model cannot possibly traverse all sets of user characteristics.

Testing

The file-sharing method was tested in a cloud scenario with a data centre, an authority server, 20 terminals. The data centre made use of Intel Xeon E5353 CPUs, DDR2 2 GB RAM, and 1000 Mbit/s, while the terminals made use of two IBM blade servers. The terminals' CPUs were 2.1 GHz, and they came with 1 GB of RAM and 100 Mbit/s. Utilising NetBeans 7.4, the scheme was tested on a VMware Exsi 5.1 server running Ubuntu 12.04 LTS after being constructed with jpbcc-1.2.1 and libcpabe-1.0.0. We compared KP-ABE, CP-ABE, and CP-ABE-WP during the phases of license manufacture and distribution and file encryption (using 256-bit AES). There were two exponential computations added by CP-ABE-WP, while four pairings and recursive computations were required by KP-ABE and CP-ABE. The average results are presented in the table below.

Table: 2 Test results

| Scheme | Phase1 (ms) | Phase 2 (Mbytes/s) |
|-----------|-------------|--------------------|
| KP-ABE | 399.14 | 26.71 |
| CP-ABE | 322.91 | 28.56 |
| CP-ABE-WP | 171.23 | 27.07 |

We outperform the prior two ABE methods by a significant margin because we build the required structure using exponential expressions rather than pairing computations. In the access control system of KP-ABE and CP-ABE, there absolutely must be $(\lfloor \log_M \lfloor \lfloor 2M^n \rfloor - 1 \rfloor)$ pairings, where (M) is the number of child nodes and (n) is the degree of the access tree. Up to (M^{n-1}) , the number of possible pairings can be. Our method cuts computation costs in half by maintaining a steady distribution for the attribute set.

CONCLUSION

The Secure Cloud File System (SCFS) incorporates Cipher text-Policy Attribute-Based Encryption without Pairing (CP-ABE-WP), which significantly enhances the safety of file exchanges in cloud environments. It allows for dynamic data sharing and gets over the limitations of conventional data management by using attribute computing for access control. The CP-ABE-WP system stands strong against chosen-plaintext attacks, ensuring that sensitive information remains protected from unauthorised access. Performance testing showed that compared to traditional ABE systems, it utilises less processing resources, encrypts data more efficiently, and manages licenses more effectively. When it comes to cloud file sharing, SCFS with CP-ABE-WP is tops. It empowers users and sets a new standard for secure data management.

REFERENCES

1. Bethencourt, J., Sahai, A. and Waters, B. (2007) 'Ciphertext-policy attribute-based encryption', IEEE Symposium on Security and Privacy, IEEE Computer Society, Los Alamitos, pp.321–334.
2. Blaze, M. (1993) 'A cryptographic file system for Unix', The 1st ACM Conference on Communications and Computing Security, Fairfax, VA.
3. Chen, X., Li, J. and Susilo, W. (2012a) 'Efficient fair conditional payments for outsourcing computations', IEEE Transactions on Information Forensics and Security, Vol. 7, No. 6, pp.1687–1694.
4. Chen, X., Li, J., Ma, J., Tang, Q. and Lou, W. (2012b) 'New algorithms for secure outsourcing of modular exponentiations', ESORICS'2012, Vol. 7459, Springer-Verlag, pp

5. Duncan, R. (1989) 'Design goals and implementation of the new high performance file system', *Microsoft Systems Journal*, Vol. 4, No. 5, pp.1–13.
6. Garg, S., Gentry, C., Halevi, S., Sahai, A. and Waters, B. (2012) 'Attribute-based encryption for circuits from multilinear maps', *Advance in Cryptology*, Vol. 8043, pp.479–499.
7. Ghemawat, S., Gobioff, H. and Leung, S-T. (2003) 'The Google file system', *The 19th ACM Symposium on Operating Systems Principles*, Lake George, NY.
8. Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006) 'Attribute based encryption for finegrained access control of encrypted data', *Proceedings of ACM Conference on Computer and Communications Security (ACM CCS)*, pp.89–98.
9. Herranz, J., Laguillaumie, F. and Rafols, C. (2010) 'Constant size ciphertexts in threshold attribute-based encryption', *PKC'2010*, Vol. 6056, pp.19–34.
10. Kumar, Saravana & G.V, Raya & Balamurugan, Balamurugan. (2014). Enhanced Attribute Based Encryption for Cloud Computing. *Procedia Computer Science*. 46. 10.1016/j.procs.2015.02.127.
11. Latham, R., Miller, N. and Carns, P. (2004) 'A next-generation parallel file system for Linux cluster', *Mathematics and Computer Science*, Vol. 2, No. 1, pp.15–32.
12. Lewko, A., Okamoto, T., Sahai, A., Takashima, K. and Waters, B. (2012) 'Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption', *Advances in Cryptology (CRYPTO'2012)*, Vol. 6110, pp.62–91.
13. Naik, Apurva & Damahe, Lalit. (2016). Enhancing Data Security and Access Control in Cloud Environment using Modified Attribute Based Encryption Mechanism. *International Journal of Computer Network and Information Security*. 8. 53-60. 10.5815/ijcnis.2016.10.07.
14. Pirretti, M., Traynor, P., McDaniel, P. and Waters, B. (2006) 'Secure attribute-based systems', *Proceedings of ACM Conference on Computer and Communications Security*, pp.99–112.