ISSN:0975-9646

Richa Singh Dangi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (6) , 2015, 5284-5288

# An Effective Signcryption Based Authentication for Security in Cloud Computing

Miss. Richa Singh Dangi[1]
[1]Scholar

Mr. Amit Saxena[2]
[2]Associate Professor

Mr. Manish Manoria[3]
[3]Professor

[1,2,3]*Dept. Of Computer Science & Engg.*
*Truba Institute of Engg. & I.T,Bhopal (M.P)*

***Abstract*— Here a well-organized procedure is implemented for Mutual Authentication of data between various users of the cloud. The Proposed algorithm implemented here provides security from various attacks as well as provides load balancing monitoring at the virtual machines and message verification. The idea to create a cloud environment and allots various users and data centers at the virtual machine to send their data in a secure manner. First of all the data from various users are set up and load is computed at both culmination of the statistics centers and finally setup and key generation and finally encryption and decryption of the data. The planned procedure applied here provides less computational time and security from a variety of attacks as well as less power consumption and ability to balance load at the data centers and the virtual**

***Index Terms*— Public key, Cloud Computing, Public Key Encryption, Attacks, Data Sharing.**

## I. INTRODUCTION

The recent advancements in technology have changed the way how electronic data is stored and retrieved. Nowadays, individuals and enterprises are increasingly utilizing remote services (such as Dropbox [1], Google Cloud Storage [2] and Amazon Simple Storage Service [3]), mainly for economical benefits. These services not only permit information sharing but also ensure availability of data from anywhere at any time. However, the rising use of remote services raises serious privacy issues by putting personal data at risk, particularly when the server's offering such services are untrusted. Unfortunately, servers get straight admittance to the statistics they store and process. For protecting sensitive data from servers in untrusted environments, data could be encrypted before leaving trusted boundaries. Regardless of whether the data is encrypted or not, the server will need to decide who will increase admittance to it. For regulating access to the data, access control policies could be specified. These are access control policies that will describe who can gain access to the data. State-of-the-art policy-based systems can ensure application of these policies. However, the matter becomes complicated when sensitive policies, which may leak private information, have to be enforced in untrusted environments. Although around may immobile be some misperception as to what precisely Cloud Computing earnings, and no overall agreement on a definition for Cloud Figuring has remained reached [4, 5], for the possibility of this work we will accept the casual definition of Cloud Computing planned in [6] and testified under:

Cloud Computing is a prototypical for empowering opportune, on claim grid admittance to a collective puddle of configurable totaling properties (e.g., networks, servers, storage, applications, and amenities) that can be swiftly provisioned and unrestricted with negligible organization exertion or provision provider interaction.

## CLOUD COMPUTING

The underlying concept of cloud computing is the separation of applications from the operating systems and the hardware on which they run. Cloud computing convey applications via the internet, which are accessible from mesh browsers and desktop and moveable apps, while the software and data are stored on servers at a remote location.

Today, our data is migrating beyond the boundaries of our personal computers and all our data would still safely reside on the web, accessible from any Internet-connected computer, anywhere in the world because of cloud computing.

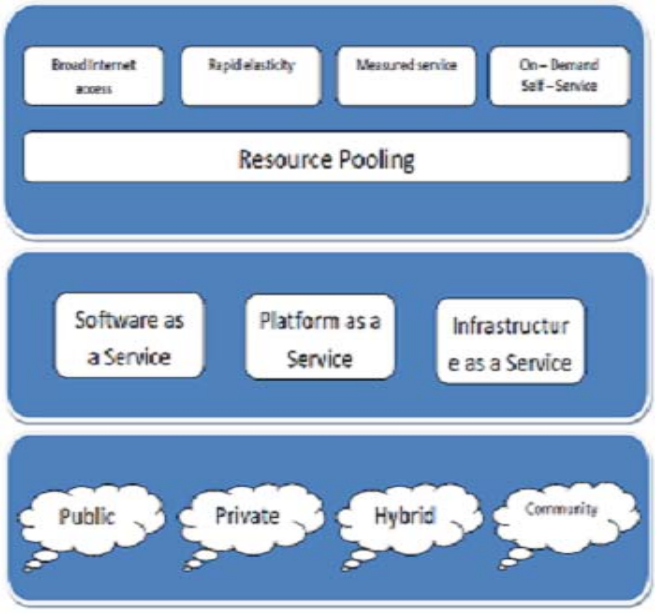


Figure 1: Cloud Computing

## SHARED KEY CRYPTOGRAPHY

In large networks, there would be many keys to be managed, and each user would have to securely manage a list containing the key pairs for each of his or her contacts. Distribution extended period clandestine keys amongst a amount of operators is an unreasonable and worrying supposition due to augmented susceptibility from the aging of keys, and lack of flexible user constellations due to the shared keys. Since this would require that a symmetric key is already shared between the distributor and the receiver.

**DATA SHARING**

Today's computing technologies have attracted more and more people to store their private data on third-party servers either for ease of sharing or for cost saving. Every people want that their data may be secure by the unauthorized user. In this figure we are performing data sharing. We are using three level of sharing important group midpoint, statistics proprietor and operator. In statistics storage midpoint all the data keep store in encrypted form.

Whenever user want to access this data then he or she gets a key by the KGC and with the help of this key user gets this data but the user is registered user otherwise he or she will not having this key. So by this we perform data sharing in small level.

Whenever we performing data sharing we have to maintain the data policies and time to time update these policies. One solution of this issue is using a policy which is good in performing encryption that is Cipher text policy attribute-based encryption (CP-ABE). This policy provides that every user had to define their own policy and enforce that policy on the data distribution.

**SIGNCRYPTION**

In cryptography, Signcryption is a public-key encryption scheme that performs the purposes of numerical name as well as of encryption simultaneously. The two fundamental cryptographic tools are Encryption and Digital signature which can guarantee confidentiality, integrity, and non-repudiation. Until the late early 2000s, both of them have been viewed as important but different basic requirement of various cryptographic systems. In community important arrangements, a outdated method is signature-then-encryption i.e. to digitally sign a communication then shadowed by an encryption. But it can intend us to two problems: Low efficiency and high cost, and the case that no arbitrary scheme can guarantee the security. Signcryption is a cryptographic method that achieves the functionalities and possessions of numerical name and encryption in a solitary rational stage i.e. together at the similar instance and can decrease the computational costs very effectively and it also decreases communication overheads when we liken it with the outdated signature-then-encryption arrangements.

Signcryption is a scheme that provides the properties and functionality of both encryption and digital signatures schemes in such a way so that it becomes more efficient than signing and encrypting separately one by one. The meaning of all this is that under a particular model of security at least some aspect of its efficiency (e.g. the computation time) is much better than any hybrid combination of digital signature and encryption schemes. Sometimes hybrid encryption can be applied in place of simple encryption, and a single session-key for several encryptions is reused to attain better overall efficiency for numerous name encryptions than a signcryption arrangement but the reuse of session key results in breach of security under even the relatively weak CPA model

Mr. Yuliang Zheng was the one who introduced signcryption for the first time in 1997 [7].An elliptic curve-based signcryption scheme was also proposed by Zheng which saves computational and communication costs by 58% and 40% respectively when it is compared to the outdated elliptic curve-based signature-then-encryption schemes. Meanwhile many other signcryption schemes are also proposed but there are many problems and limitations that each of them are having, on the other sidethe also offer different level of computational costs and security services.

## II. LITERATURE SURVEY

Since encryption can provide confidentiality of the message and digital signature can provide authentication and non repudiation of a message. To simultaneously provide two roles in reality, in 1997, Zheng [7] first proposed a new crypto graphical primitive: signcryption, by which digital signature and PKE can be performed in a logic step, at lesser communication overheads and lower computational cost than the above sign-then encrypt way. Meanwhile then, here are numerous signcryption schemes proposed. It is solitary newly that a proper refuge waterproof prototypical [8] is dignified only if sanctuary resistant for Zheng's scheme [12] in the haphazard revelation prototypical. By coalescing ID grounded cryptology [9] and signcryption, Malone-Lee projected a major ID-based signcryption arrangement. But Libert and Quisquater [10] piercing out that Malone-Lee's arrangement is not semantically safe, meanwhile the autograph of the communication is noticeable in the signcrypted communication. Chow et al [11] planned an ID-based signcryption arrangement that can deliver together community verifiability an onward security. In 2003, Boyen [12] future a safe identity-based signcryption arrangement with cryptograph manuscript secrecy and demonstrable safe in the chance oracle perfect. Their refuge resistant perfect is somewhat dissimilar from that of [8] which comprises the code manuscript secrecy. In 2004, Libert and Quisquater adapted Boyen's safety resistant perfect to nonidentity founded signcryption arrangement and future a signcryption arrangement [13].

Here in this paper [14] author has proposed a new arbitrated certificateless encryption method without pairing process for strongly distribution sensitive information in open clouds. Here they use Mediated certificateless public key encryption (mCL-PKE) explains the key escrow difficulty in identity based encryption and certificate revocation difficulty in public key cryptography. On the other hand, existing mCL-PKE methods are also in-competent because of utilize of costly pairing process or susceptible beside incomplete decryption attacks. With the intention of concentrate on the presentation and protection concerns, here in this paper they apply their mCL-PKE method to build a realistic explanation to the difficulty of sharing sensitive information in public clouds. The cloud is utilized as a protected storage space and a key generation center. In their method the data owner encrypts the susceptible statistics by the mist produced users' public key supported on its right to use manage policies and uploads the encoded statistics to the cloud storage space. Due to unbeaten permission, the cloud moderately decrypts the encrypted data for the cloud consumers. The cloud consumers consequently completely decrypt the in some

measure decrypted data using their own private keys. The privacy of the content and the keys is protected regarding the cloud, for the reason that the cloud cannot entirely decrypt the information. They also suggest an expansion to the exceeding approach to get better the competence of encryption at the data owner on cloud. Experimental result shows that proposed system has it's enhance security and performance and that schemes are proficient and practical use in real time application.
This building can be watched as a Uniqueness Founded Encryption of a communication under several attributes that compose a (fuzzy) identity [15, 16].

## III. PROPOSED METHODOLOGY

The practice applied here for provided that Lively Data at Statistics middles with Multi Receiver Identity based Signcryption. The proposed methodology implemented will consists of following phases:

1. First of all create a cloud Environment.
2. The cloud Environment Setup consists of 'N' number of Cloudlets 'Ci', Data Centers 'DCi', Virtual Machines 'VMi', Brokers 'Bi'.
3. Now the user of the cloud starts sharing of data to other users of the cloud.
4. During the sharing of data over cloud environment four steps are performed initialized with Setup Phase and Key Generation Phase and Encryption Phase and Decryption and Verification Phase.

### Cloud Environment Setup

Here the cloud environment is setup and simulate using Cloud Simulator in which first of all Cloudlets and Data Centers and Virtual Machines and Brokers are created.

a) If 'N' be the number of Requests to be send from Cloudlets 'Ci' to the Data Centers 'DCi' through Brokers 'Bi'.
b) Let us suppose 'Ri' number of resources to used during the sharing of data from Cloudlets 'Ci' to Data Centers 'DCi'.
Ci → Bi → DCi
c) For each of the Resource to be shared to data Centers
Ri → DCi
d) End

### Security Algorithm

The technique implemented for the Secure Data Sharing uses Multi Receiver Identity Based Signcryption using Elliptic Curves which consists of Following Phases:

### Setup

During the setup phase of the Signcryption methodology implemented here for data security. Here in the setup phase Elliptic Curves are created using the equation:

$$y^2 = ax^3 + bx + c$$

Where,

$$4a^3 + 27b^2 \neq 0$$

Elliptic Curve Cryptography contains the following Parameters over the finite field

| Symbol | Description |
|---|---|
| q | The prime number of the order of p |
| a,b | The curve coefficient |
| B | is the base point or the common point ( , ) |
| n | Is the order of the base point B. |
| h | $\frac{E(F_q)}{n}$ |
| Sk1 | The secrete key of first user with (X,Y) Co-ordinates. |
| Sk2 | The secrete key of other user with (X, Y) Co-ordinates. |
| P1 | Is the generated public key of first user. |
| P2 | Is the generated public key of other user. |
| * | Is the point multiplication |

**Table 1.** Various Notations Used

### Key Generation

If User'Ui' of the Cloudlet 'Ci' wants to share data with other users of the Cloud then during the setup of the elliptic curves both the users of the cloud shared a Common Base Point of the elliptic Curve 'B'. Now one User chooses a random point over the elliptic curve that would be the secrete key of the first user as 'Sk1'. The Chosen Secrete Key is the combination of 'X' and 'Y' axis parameters as Sk1(X, Y). Similarly other user of the cloud also shares random point over the elliptic Curve of another secrete key as Sk2. The Chosen Secrete Key is the combination of 'X' and 'Y' axis parameters as Sk2(X, Y). With the help of the Secrete Key Public Key Parameters are generated using.

$$P1(X,Y) = Sk1(X,Y) * B(X,Y)$$
$$P2(X,Y) = Sk2(X,Y) * B(X,Y)$$

Here Point Multiplication '*' used here is the combination of point addition and point doubling.
Point Addition is the addition of two point

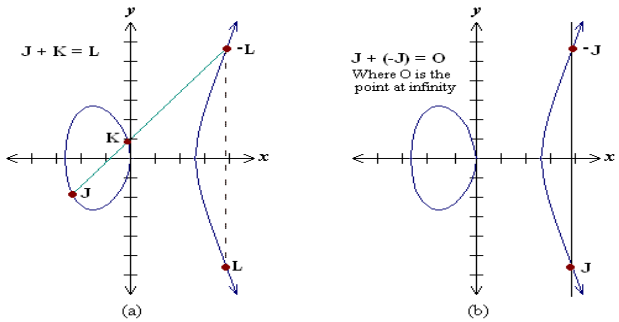


Figure 2. Point Addition

Point Doubling is the addition of point J to itself to obtain another point .

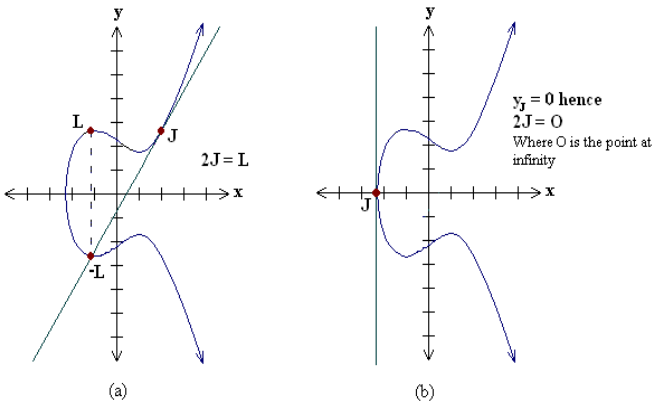


Figure 3. Point Multiplication

**Signcryption Phase**

The signcryption algorithm implemented here uses the Identity of the other users 'ID1'.

1. First of all select a random Integer 'r', $r \in R[1, n-1]$
2. Compute P ← [k] B
3. T ← [k] Sk1
4. Generate a set of keys from the key Derivation Function (k1||k2) ← KD(T,l)
5. Generate Cipher Text using the first Key c ← Ek1(m)
6. Generate Signature using the other key using Message Authentication Code Sg ← MACk2(c).
7. Sends the signcrypted text (P, C, Sg) to receiver.

| Symbol | Description |
|---|---|
| R | Selected random integer. |
| R | Prime order number |
| P | Is the public key selected from the elliptic curve. |
| Sk1 | Is the generated Secrete key of the first user |
| K | Generated private key of the user |
| KD | Is the Key Derivation Function. |
| B | Is the Common Base Point |
| E | Is the Encryption Algorithm |
| M | Message to be encrypted |
| k1 | Key 1 |
| k2 | Key 2 |
| C | Cipher text |
| Sg | Generated Signatures |
| MAC | Message Authentication Code Hash Function. |

Table 2. Various Annotations Used

**UnSigncryption Phase**

As soon as the signcrypted message (P, C, Sg) is received to the Receiver with Identity 'IDi'.

1) Generate a message String T using T ← [x] P
2) Generate a set of Key pairs using Key Derivation Function
(k1||k2) ← KD(T,l)
3) Decrypt the message using Key k1, m ← Dk1(c).
4) Generate Signature using the other key using Message Authentication Code Sg1 ← MACk2(m).
5) Now verify the message by checking if the generated signatures from the user Sg == Sg1
6) If equal then message is verified message else invalid.

## IV. Result Analysis

The Table shown below is the analysis and comparison of prevention from various attacks during the authentication between user and server. The existing methodology implemented here for the authentication between user and server using Elliptic Curves provides security from various attacks while the mutual authentication technique implemented is still vulnerable to certain attacks.

| S. No. | Security Attacks | Existing Work | Proposed Work |
|---|---|---|---|
| 1 | Password Impersonation | No | Yes |
| 2 | Password Guessing Attack | Yes | Yes |
| 3 | Confidentiability | No | Yes |
| 4 | Public Verifiability | Yes | Yes |
| 5 | DoS Attack | Yes | Yes |
| 6 | Insider Attack | No | Yes |
| 7 | Denning Sacco Attack | Yes | Yes |
| 8 | DDoS Attack | No | Yes |
| 9 | Outsider Attack | Yes | Yes |
| 10 | Online Dictionary Attack | Yes | Yes |
| 11 | Offline Dictionary Attack | Yes | Yes |
| 12 | Server Masquerade Attack | Yes | Yes |
| 13 | Integrity | Yes | Yes |
| 14 | Unforgeability | Yes | Yes |
| 15 | Non-Repudiation | Yes | Yes |
| 16 | Forward Secrecy | Yes | Yes |
| 17 | Additional Authentication | No | Yes |

Table 3 Analysis of Prevention from Various Attacks

The table shown below is the analysis and comparison of existing mutual authentication based technique and the proposed methodology applied for authentication between user and server on cloud computing. The existing Mutual Authentication Technique implemented provides in total 12hash functions for the encryption to occur while proposed methodology only provides 1hash function for the encryption to occur for the Registration Phase. The various steps involved in Existing Mutual Authentication Technique take 1, 8, 3 Hash functions at the user side and 5, 0, 9 hash functions at the server end. While the proposed methodology takes 1, 0, 1 hash function at user side and 1, 0, 1 hash functions at the server side. The existing methodology in total takes 12 hash function at the user end

and 14 hash functions at the server end while the proposed methodology takes 2 hash functions at the user end and 2 hash functions at the server end. Since the proposed methodology implemented takes less hash function hence the overall cost will be less as compared to the existing methodology.

| Scheme | Existing Work | | Proposed Work | |
|---|---|---|---|---|
| | User | Server | User | Server |
| Registration | 1xh | 5h | 1h | 1h |
| Login | 8h | | | |
| Authentication | 3h | 9h | 1h | 1h |
| Total | 12h | 14h | 2h | 2h |

Table 4. Comparison of Cost

The figure shown below is the analysis and comparison of Signcryption and Un-Signcryption in Milli Second of the proposed methodology. The Signcryption time is computed for various bits on 112, 160, and 256 bits.

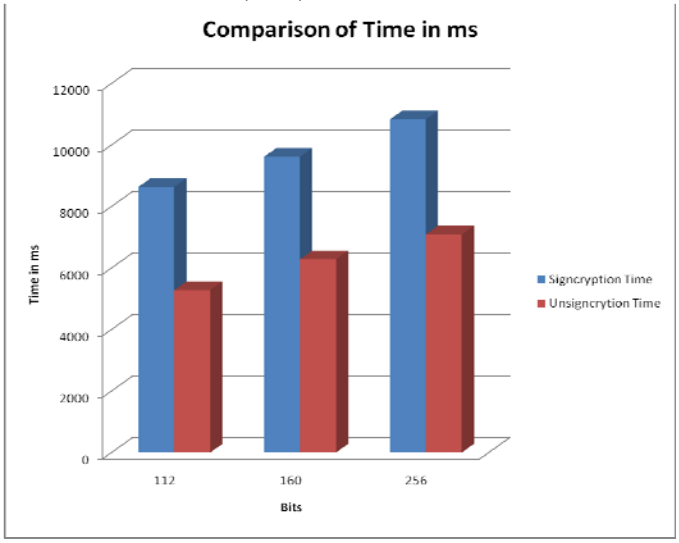


Figure 4. Comparison of Signcryption & UnSigncryption Time in ms

The figure shown below is the analysis and comparison of Storage Cost between Existing and proposed methodology. The proposed methodology implemented takes less Storage cost as compared to existing methodology implemented Mutual Authentication.

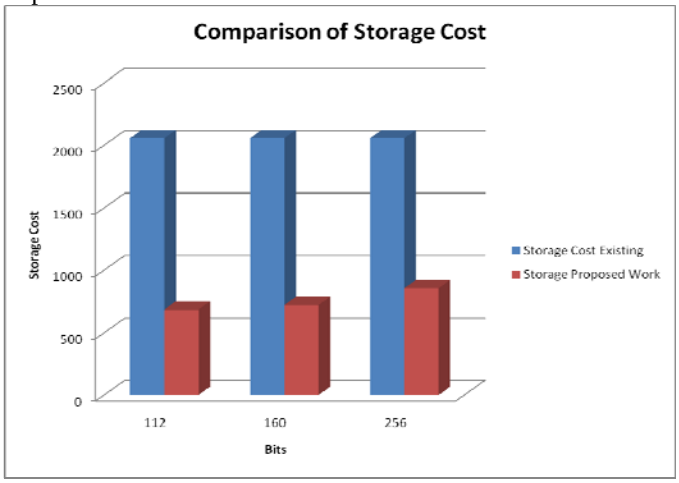


Figure 5 Comparison of Storage Cost

## V. Conclusion

The proposed methodology implemented here for the efficient data sharing by providing mutual authentication between users of the public clouds. The methodology implemented here provides efficient computational cost and time for encryption and decryption as well as provides secure data communication over public clouds.

## References

[1] "Dropbox." https://www.dropbox.com/ . October 30, 2013.
[2] Google, "Google cloud storage pricing." https://cloud.google.com/pricing/cloud-storage, February 2013.
[3] Amazon, "Amazon simple storage service (Amazon S3)." http://aws.amazon.com/s3/#pricing, February 2013.
[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Commun. ACM, 53:50–58, April 2010.
[5] Q. Zhang, L. Cheng, and R. Boutaba. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1:7–18, 2010. 10.1007/s13174-010-0007-6.
[6] P. Mell and T. Grance. The NIST Definition of Cloud Computing (Draft)–Recommendations of the National Institute of Standards and Technology. Special publication 800-145 (draft), Gaithersburg (MD), Jan. 2011.
[7] Y.Zheng. "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+cost(encryption)", Crypto'97, LNCS 1294, pp. 165-179, Springer-Verlag, 1997.
[8] J.Baek, R.Steinfeld, and Y.Zheng, "Formal proofs for the security of signcryption", PKC'02, LNCS 2274, pp. 80-98, Springer-Verlag, 2002.
[9] A. Shamir, "Identity-based cryptosystems and signature schemes", Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53, 1984.
[10] Libert and J.Quisquater, "Efficient signcryption with key privacy from gap Diffie-Hellman groups", PKC'04, LNCS 2947, pp. 187-200, Springer-verlag, 2004.
[11] Chi-How TAN, "On the Security of Signcryption Scheme with key Privacy", IEICE TRANS. FUNDAMENTALS, Vol E88-A, No.4, pp. 1093-1095, 2005.
[12] X.Boyen, "Multipurpose identity-based signcryption: A Swiss ary knife for identity-based cryptology", Crypto'03, LNCS 2729, pp. 383-399, Springer verlag, 2003.
[13] S.M.Chow, S.M.Yiu, L.Hui, and K.Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity", ICISC 2003, LNCS 2971, pp. 352-369, 2003.
[14] Seung-HyunSeo, Mohamed Nabeel, Xiaoyu Ding,Elisa Bertino,"An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 26, September 2014.
[15] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption", *Proceedings International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt '05)*, pp. 457-473, 2005.
[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data", *Proceedings of ACM Conference on Computer and Communication Security*, pp. 89-98, 2006.