

Providing Cloud Security Using DROPS Technique

Nirmale Pooja S., Kore Pranjali P, Pratape Pradnya P., Patil Mayur H.

B. E Students, Dept. of Computer Engineering, JSPM'S ICOER, Wagholi, Pune, Maharashtra, India

ABSTRACT: Outsourcing information to an outsider authoritative control, as is done in distributed computing, offers ascend to security concerns. The data compromise may occur due to attacks by malicious users and nodes within the cloud. Therefore, high security systems are required to protect data within the cloud. Be that as it may, the utilized security technique should likewise consider the advancement of the information recovery time. In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and then replicate the fragmented data over the cloud nodes. Each of the nodes contains only a single fragment of a particular data file that ensures that even in case of a successful attack, no any meaningful information is disclose to the attacker. Furthermore, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to bar from an attacker of guessing the locations of the fragments. Moreover, the DROPS methodology does not depend on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally costly methodologies. We show that the eventuality to locate and compromise all of the nodes storing the fragments of a single file is extremely low. We also compare the performance of the DROPS methodology with ten other state-of-art schemes. The higher level of security with slight performance overhead was observed.

KEYWORDS: file fragmentation, file replication, attribute-based encryption, and outsourced key-issuing; outsourced decryption;

I. INTRODUCTION

The cloud computing paradigm has reformed the usage and management of the information technology framework. Cloud computing is characterized by on-demand self-services, ubiquitous network accesses, resource pooling, elasticity, and measured services. The aforementioned characteristics of cloud computing make it a conspicuous candidate for businesses, organizations, and individual users for adoption. However, the benefits of minimum cost, negligible management (from a users perspective), and greater elasticity come with increased security concerns. Security is one of the most crucial aspects among those forbidding the wide-spread adoption of cloud computing. Cloud security issues may stem due to the core technologies implementation (virtual machine (VM) escape, session riding, etc.), cloud service presenting (structured query language injection, weak authentication schemes, etc.), and arising from cloud characteristics (data recovery vulnerability, Internet protocol vulnerability, etc.). For a cloud to be secure, all of the participating entities must be secure. In any given system with multiple units, the highest level of the systems security is equal to the security level of the weakest entity. Therefore, in a cloud, the security of the assets does not completely depend on an individual's security measure. The neighboring entities may provide an opportunity to an attacker to detour the user's defenses. The sufficient amount of loss information present public data integrity auditing with division and replication of data in cloud system that judicially fragments user text files into small part and replicates them at strategic locations within the cloud.

We develop a scheme for outsourced data that takes into account both the security and performance. The proposed scheme fragments and replicates the data file over cloud nodes.

The proposed System scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

In ABE Attribute based encryption, We consider the case that the user Alice has a large number of data stored in the cloud. If Alice submits a request for accessing the encrypted data stored in the CSP, according to the traditional outsourced ABE scheme, the CSP downloads all the data, executes partial decryption and responses all corresponding data of Alice. This greatly increases the cost for communication and storage at Alice side. In this article, we organically integrate outsourced -ABE (OABE) with PEKS and present a novel cryptographic paradigm called outsourced attribute-based encryption scheme with keyword search function (KSF-OABE). In our system, when the user wants to outsource his sensitive information to the public cloud, he encrypts the sensitive data under an attribute set and builds indexes of keywords. As a result, the users can decrypt the ciphertext only if their access policies satisfy the corresponding attributes. By this way, when Alice submits the request with a trapdoor corresponding to a keyword "current", CSP downloads all the data intended for Alice and just returns a partial ciphertext associated with the keyword "current". Therefore, Alice can exclude the data what she does not hope to read. Then also Cloud computing is a new computation model in which computing resources is regarded as service to provide computing operations. This kind of computing paradigm enables us to obtain and release computing resources rapidly. So we can access resource-rich, various, and convenient computing resources on demand. The computing paradigm also brings some challenges to the security and privacy of data when a user outsources sensitive data to cloud servers. Many applications use complex access control mechanisms to protect encrypted sensitive information. Sahai and Waters addressed this problem by introducing the concept for ABE. This kind of new public-key cryptographic primitive enables us to implement access control over encrypted files by utilizing access policies associated with ciphertexts or private keys.

II. RELATED WORK

1. "On the characterization of the structural robustness of data center networks,"

In this paper, Author studied the structural robustness of the state-of-the-art data center network (DCN) architectures [1]. Our results revealed that the DCell architecture degrades gracefully under all of the failure types as compared to the FatTree and ThreeTier architecture. Because of the connectivity pattern, layered architecture, and heterogeneous nature of the network, the results demonstrated that the classical robustness metrics are insufficient to quantify the DCN robustness appropriately. Henceforth, signifying and igniting the need for new robustness metrics for the DCN robustness quantification. We proposed deterioration metric to quantify the DCN robustness. The deterioration metric evaluates the network robustness based on the percentage change in the graph structure. The results of the deterioration metric illustrated that the DCell is the most robust architecture among all of the considered DCNs.

2. "Energy-efficient data replication in cloud computing datacenters,"

This paper reviews the topic of data replication in geographically distributed cloud computing data centers and proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system [2]. Moreover, the optimization of communication delays leads to improvements in quality of user experience of cloud applications. The performance evaluation is carried out using Green Cloud – the simulator focusing on energy efficiency and communication processes in cloud computing data centers. The obtained results confirm that replicating data closer to data consumers, i.e., cloud applications, can reduce energy consumption, bandwidth usage, and communication delays significantly.

3. "An analysis of security issues for cloud computing,"

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. Author presented security issues for cloud models: IaaS, PaaS, and SaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines [3].

4. “Fuzzy Identity-Based Encryption.

Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term “attribute-based encryption”. In this paper Author present two constructions of Fuzzy IBE schemes [4]. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

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

The Authors develop a new cryptosystem for one-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. Authordemonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption [5].

Sr.No	Author	Paper Name	Description	Year
1	K. Bilal, M. Manzano, S.U. Khan, E. Calle, K. Li, and A. Zomaya,	On the characterization of the structural robustness of data center networks	In this paper, Author studied the structural robustness of the state-of-the-art data center network (DCN) architectures. Our results revealed that the D-Cell architecture degrades gracefully under all of the failure types as compared to the FatTree and ThreeTier architecture.	2013
2	D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya,	Energy-efficient data replication in cloud computing datacenters	This paper reviews the topic of data replication in geographically distributed cloud computing data centers and proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system.	2013
3	K. Hashizume, D. G. Rosado, E. Fernandez-Medina, and E. B. Fernandez,	An analysis of security issues for cloud computing	We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users.	2013
4	A. Sahai and B. Waters	Fuzzy Identity-Based Encryption.	The Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. In this paper Author present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity.	2005

TABLE 1. STUDY OF DIFFERENT METHODS

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

III. PROPOSED ALGORITHM

Algorithm 1 Algorithm for fragment placement

Inputs and initializations:

$O = \{O_1, O_2, \dots, O_N\}$

$o = \{sizeof(O_1), sizeof(O_2), \dots, sizeof(O_N)\}$

$col = \{open_color, close_color\}$

$cen = \{cen_1, cen_2, \dots, cen_M\}$

$col \leftarrow open_color \forall i$

$cen \leftarrow cen_i \forall i$

Compute:

for each $O_k \in O$ do

select $S^i \mid S^i \leftarrow \text{indexof}(\max(cen_i))$

if $col_{S^i} = open_color$ and $s_i \geq o_k$ then

$S^i \leftarrow O_k$

$s_i \leftarrow s_i - o_k$

$col_{S^i} \leftarrow close_color$

$S^{i'} \leftarrow \text{distance}(S^i, T)$ \triangleright /*returns all nodes at

distance T from S^i and stores in temporary set $S^{i'}$ */

$col_{S^{i'}} \leftarrow close_color$

end if

end for

Algorithm 2 Algorithm for fragment's replication

for each O_k in O do

select S^i that has $\max(R_k^i + W_k^i)$

if $col_{S^i} = open_color$ and $s_i \geq o_k$ then

$S^i \leftarrow O_k$

$s_i \leftarrow s_i - o_k$

$col_{S^i} \leftarrow close_color$

$S^{i'} \leftarrow \text{distance}(S^i, T)$ \triangleright /*returns all nodes at

distance T from S^i and stores in temporary set $S^{i'}$ */

$col_{S^{i'}} \leftarrow close_color$

end if

end for

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

3. AES Algorithm

Step 1: Key Expansions

For each round AES needs a different 128-bit block of round key also one more.

Step 2: Initial Round

Add Round Key with a block of the round key, each byte of the state is combined using bitwise xor.

Step 3: Rounds

- Sub Bytes- in this step each byte is replaced with another byte.
- Shift Rows- for a certain number of steps, the state's last three rows are moved cyclically.
- Mix Columns- on the columns of the state a mixing operation operates, in each column combining the four bytes.

Step 4: Add Round Key

Step 5: Final Round (no Mix Columns)

- Sub Bytes
- Shift Rows
- Add Round Key.

IV. PROPOSED SYSTEM

To design a system for Division and replication of data in cloud with Attribute based encryption. Division and Replication of Data in the Cloud that judiciously fragments user files into pieces and replicates them at strategic locations within the cloud.

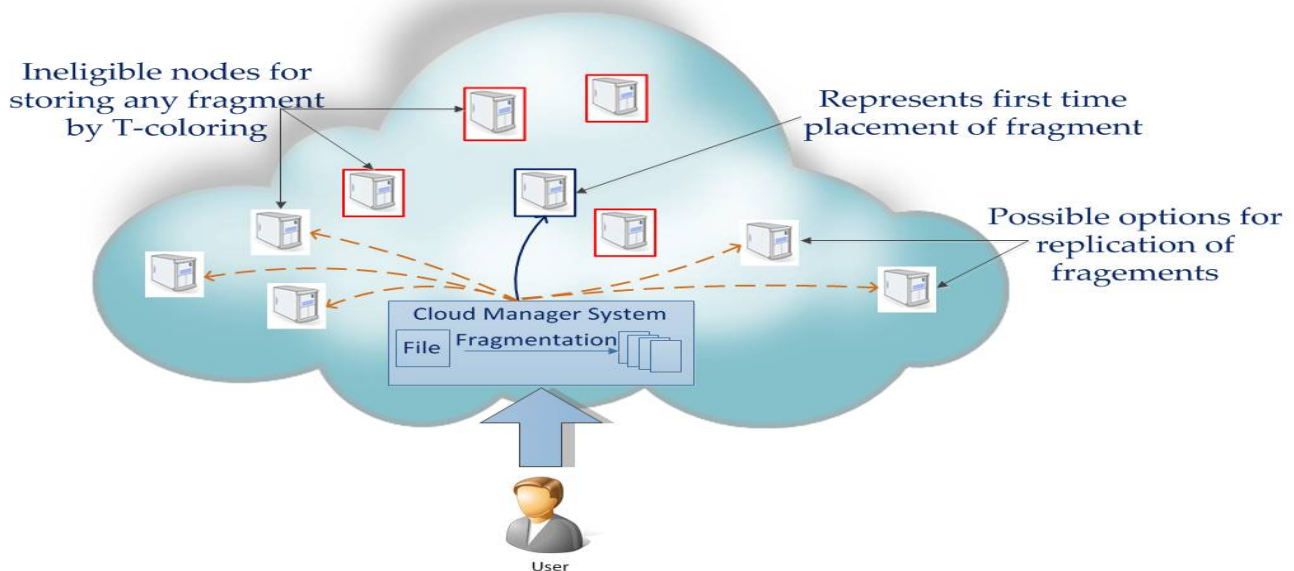


Figure 1: System Architecture

In proposed system, we collectively approach the issue of security and performance as a secure data replication problem. The division of a file into fragments is performed based on a given user criteria. Divided File can store in different nodes. Attribute based encryption (ABE) technology has been used to design fine-grained access control system, which provides one good method to solve the security issues in cloud setting.

In this paper, we collectively rules the issues of security and performance as a secure the file. Division and Replication of Data in the Cloud storage that fragments user files into small part and replicates them at strategic locations with into the cloud storage nodes. The division of a file into fragments is performing based on the giving input criteria such that

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

as the individual fragments do not contain any meaningful data. Each of the cloud node (we use the term node to represent storage capacity, physical, and the virtual machines) contains will be distinct fragment to increase the more data security on cloud.

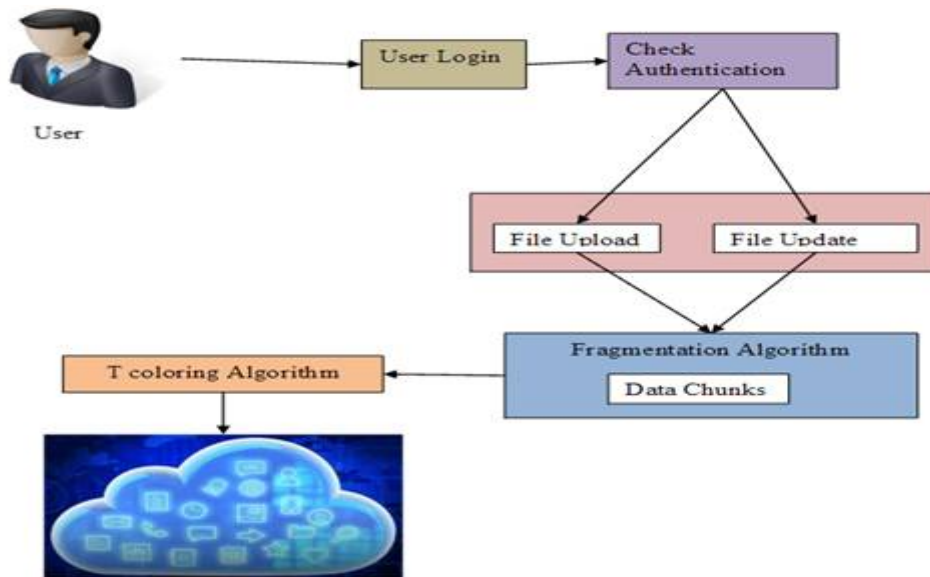


Figure 2: Fragmentations of File

V. EXPERIMENTAL RESULT

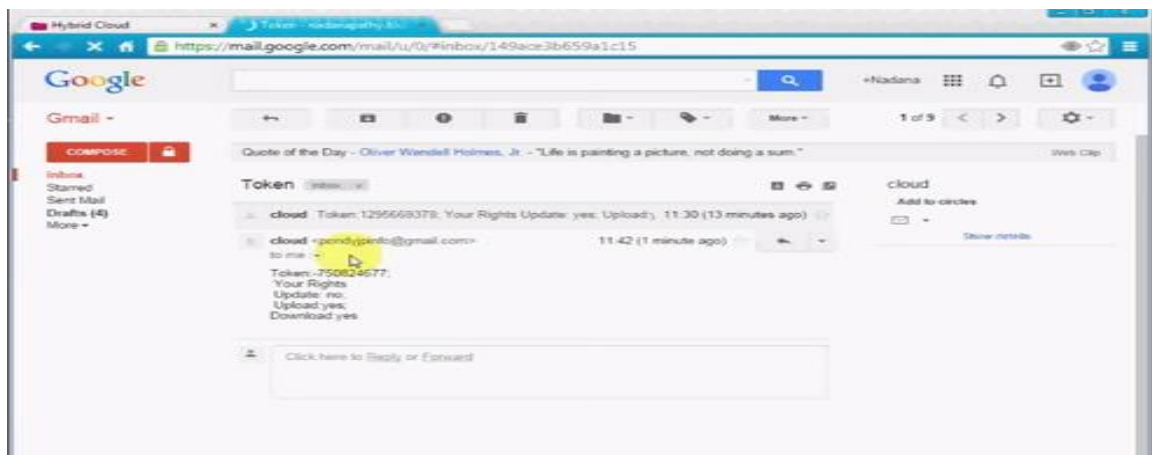


Fig3. Token send on mail.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017



Fig. 4 User Login

User can enter token key and upload or download file.

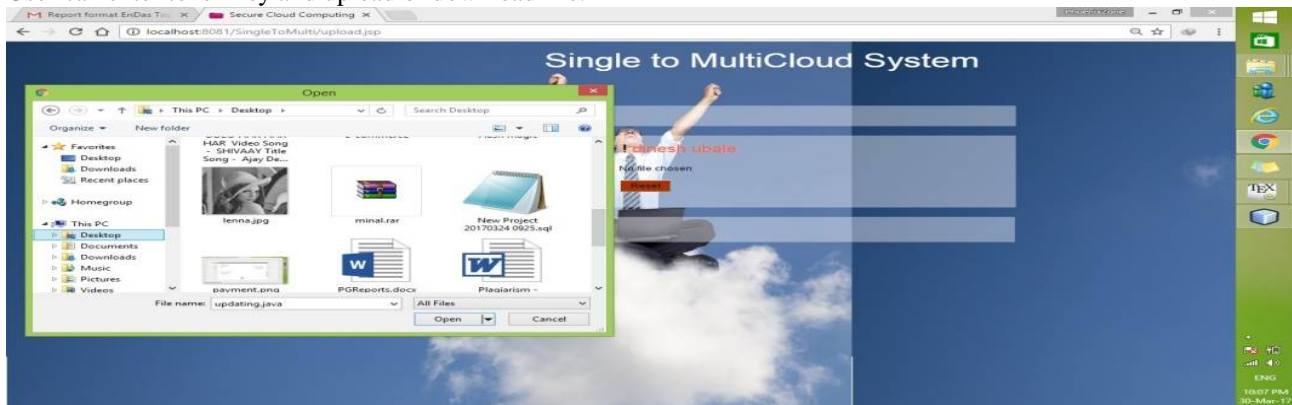


Fig5. Upload file

User can enter token key and upload file. User can select file and upload file.

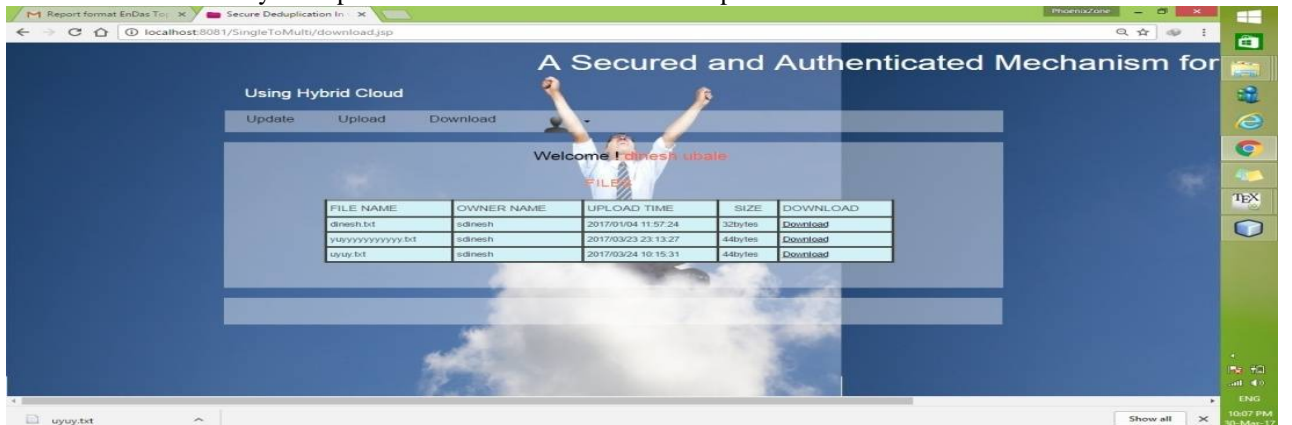


Fig6. Show details

Who can upload file or download file show in this table.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

VI. CONCLUSION

In this paper, the proposed that Division and replication of data in cloud with Attribute based encryption. The proposed system, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. And CP-ABE scheme that provides outsourcing key-issuing, decryption and keyword search function. Our scheme is efficient since we only need to download the partial decryption cipher text corresponding to a specific keyword. In our scheme, the time-consuming pairing operation can be outsourced to the cloud service provider, while the slight operations can be done by users. Thus, the computation cost at both users and trusted authority sides is minimized. The Division and replication of data in cloud with Attribute Based Encryption. With help of trapdoor provider work is reduces.

REFERENCES

- [1].K. Bilal, M. Manzano, S.U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.
- [2].D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446-451.
- [3]. J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. of IEEE INFOCOM 2014, Toronto, Canada, Apr. 2014, pp. 2121-2129.
- [4]. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," EUROCRYPT'05, LNCS, vol. 3494, 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. 13th ACM Conference on Computer and Communications Security (CCS'06), pp. 89-98, 2006, doi:10.1145/1180405.1180418.
- [6] J.G.Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol.23, no.11, pp. 2150-2162, Nov.2012, doi: 10.1109/TPDS.2012.50.
- [7] T. Okamoto and K. Takashima, "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption," CRYPTO'10, T. Rabin, ed., LNCS 6223, Berlin: Springer-Verlag, pp. 191-208, 2010.
- [8] W.R.Liu, J.W.Liu, Q.H.Wu, B.Qin, and Y.Y.Zhou, "Practical Direct Chosen Ciphertext Secure Key-Policy Attribute-Based Encryption with Public Ciphertext Test," ESORICS'14, LNCS 8713, Berlin: Springer-Verlag, pp. 91-108, 2014.