Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 6, June-2018

TMACS

Monica Jadhav [1], Ashwini Belchada[2], Renuka Hiremath [3], Mritunjay Kumar[4].

[1]*Department of Computer Science, Dr. DY Patil Insititue of Engineering and Technology, Talegaon. Maharashtra, India*
[2]*Department of Computer Science, Dr. DY Patil Insititue of Engineering and Technology, Talegaon. Maharashtra, India*
[3]*Department of Computer Science, Dr. DY Patil Insititue of Engineering and Technology, Talegaon. Maharashtra, India*
[4]*Department of Computer Science, Dr. DY Patil Insititue of Engineering and Technology, Talegaon. Maharashtra, India*

Abstract — characteristic-based totally mystery writing (ABE) is taken into consideration a promising cryptological engaging in tool to make sure information owners' direct management over their facts publicly cloud garage. The sooner ABE schemes contain just one authority to attend to the whole characteristic set, which might deliver a single-factor bottleneck on every security and overall performance. Later, some multi-authority schemes are projected, during which multiple authorities in my view hold disjoint attribute subsets. However, the unmarried-point bottleneck downside remains unsolved. At some point of this paper, from any other attitude, we have a tendency to conduct a threshold multi-authority CP-ABE get entry to control theme for public cloud storage, named TMACS, at some stage in which more than one authorities prepare manipulate a homogenous attribute set. In TMACS, taking advantage (t; n) threshold secret sharing, the passe-partout may be shared amongst more than one authority, and a criminal person will generate his/her mystery key by way of interacting with any t government. Security and overall performance analysis results display that TMACS isn't completely verifiable secure as soon as however t government ar compromised, but conjointly sturdy as soon as no however t authorities are alive within the system. Moreover, by expeditiously combining the normal multi-authority topic with TMACS, we have a tendency to construct a hybrid one, that satisfies the scenario of attributes getting back from absolutely unique authorities in addition as attaining protection and gadget-degree lustiness.

Keywords—CP-ABE, (t; n) threshold secret sharing, multi-authority, public cloud storage, access control.

I. INTRODUCTION

Despite several benefits of cloud storage, there still stay numerous difficult obstacles, among which, privacy and security of users' information have become major problems, particularly publically cloud storage. Historically, information knowledge information} owner stores his/her data in trustworthy servers, that area unit typically controlled by a completely trustworthy administrator. However, publically cloud storage systems, the cloud is sometimes maintained and managed by a semi-trusted third party (the cloud provider). Data is no longer in information owner's trust worthy domains and also the information owner cannot trust on the cloud server to conduct secure knowledge access management. Therefore, the secure access management drawback has become a critical difficult issue publically cloud storage, during which ancient security technologies can't be directly applied.

Attribute-based secret writing (ABE) is thought to be one of the foremost suitable schemes to conduct information access control publically clouds for it will guarantee information owners' direct management over their information and supply a fine-grained access management service. Till now, there are unit many ABE schemes proposed, which might be divided into 2 categories: Key- Policy Attribute-based secret writing (KP-ABE), like and Cipher text-Policy Attribute-based encryption (CPABE), decipher keys area unit associated with access structures whereas cipher text area unit solely labeled with special attribute sets.

In this paper, we tend to propose a strong and verifiable threshold multi-authority CP-ABE access management scheme, named TMACS, to take care of the single-point bottleneck on each security and performance in most existing schemes. In TMACS, multiple authorities collectively manage the full attribute set however nobody has full management of any specific attribute.

In TMACS, we tend to redefine the key within the ancient CP-ABE schemes as master. The introduction of (t, n) threshold secret sharing guarantees that the master can't be obtained by any authority alone. TMACS isn't solely verifiable secure once but t authorities area unit compromised, however conjointly strong once no but t authorities area unit alive within the system.

II. PROBLEM STATEMENT

In existing access control systems for public cloud, there brings a single-point bottleneck on both security and performance against the single authority for any specific attribute.

III. LITERATURE REVIEW

1) Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments

AUTHORS: Jeong-Min Do

To ensure data confidentiality and fine-grained access control in cloud computing environments, a recent study proposed system model using Key Policy-Attribute Based Encryption(KP-ABE) and Proxy Re-Encryption(PRE). But, existing work has effected the violation of data confidentiality through collusion attack of revoked user in system and cloud server. To resolve this problem, we propose system model that store and divide data file into header, body. In addition, our schemes selectively delegate decryption right using Type-based Proxy re-encryption.

2) How to share a secret

AUTHORS: Adi Shamir

We show how to divide data into pieces in such way that is easily reconstrutable from any pieces, but even complete knowledge of k-1 pieces revels absolutely no information about D. this technique enables the construction of robust key management schemes for cryptographic system.

3) Secure Data Access in Cloud Computing.

AUTHORS: Sunil Sanka

Data security and access control is one of the most challenging ongoing research work in cloud computing, because of users outsourcing their sensitive data to cloud providers. Existing solutions that use pure cryptographic techniques to mitigate these security and access control problems suffer from heavy computational overhead on the data owner as well as the cloud service provider for key distribution and management. This paper addresses this challenging open problem using capability based access control technique that ensures only valid users will access the outsourced data. This work also proposes a modified Diffie-Hellman key exchange protocol between cloud service provider and the user for secretly sharing a symmetric key for secure data access that alleviates the problem of key distribution and management at cloud service provider. The simulation run and analysis shows that the proposed approach is highly efficient and secure under existing security models.

4) Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage

AUTHORS: GIUSEPPE ATENIESE

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semitrusted proxy converts a cipher text for Alice into a cipher text for Bob *without* seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following recent work of Dodis and Ivan, we present new re-encryption schemes that realize a stronger notion of security and demonstrate the usefulness of proxy re-encryption as a method of adding access control

to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

5**) Capability-based Cryptographic Data Access Control in Cloud Computing**

AUTHORS: Chittaranjan Hota

Cloud computing has emerged as a popular model in computing world to support processing large volumetric data using clusters of commodity computers. It is the latest effort in delivering computing resources as a service. It is used to describe both a platform and a type of application. A cloud computing platform dynamically provisions, configures, and deprovisions servers as needed. Cloud computing also describes applications that are extended to be accessible through the Internet. Data security and access control is one of the most challenging ongoing research work in cloud computing, because of users outsourcing their sensitive data to cloud providers. Existing solutions that use pure cryptographic techniques to mitigate these security and access control problems suffer from heavy computational overhead on the data owner as well as the cloud service provider for key distribution and management. This paper addresses this challenging open problem using capability based access control technique that ensures only valid users will access the outsourced data. This work also proposes a modified Diffie-Hellman key exchange protocol between cloud service provider and the user for secretly sharing a symmetric key for secure data access that alleviates the problem of key distribution and management at cloud service provider. The simulation run and analysis shows that the proposed approach is highly efficient and secure under existing security models.

IV. EXISTING SYSTEM

Public cloud storage there brings a single-point bottleneck on every security and performance against the only authority for specific attribute. Authority is compromised, associate adversary will acquire the only-one-authority's key, then he/she will generate personal keys of any attribute set to decipher the particular encrypted knowledge. Only-one-authority is crashed; the system fully cannot work well. CP-ABE schemes are still far from being wide used for access management publicly cloud storage.

V. PROPOSED SYSTEM

Robust and verifiable threshold multi-authority CP-ABE access management scheme named as TMACS. In TMACS, multiple authorities collectively manage the whole attribute set but no one has full management of any specific attribute. Combining of (t, n) threshold secret sharing and multi-authority CP-ABE theme, we tend to propose and realize a robust and verifiable multi authority access control system publically cloud storage, in which multiple authorities collectively manage a uniform attribute, set.

VI. MATHEMATICAL MODEL

Let S be the Whole system S= {I,P,O}
I-input
P-procedure
O-output

Input I={DO,CSP,F }
Where,
F- Files F = {f1,f2,…..,fn}
DO- Data owner,
CSP- Cloud service provider,
Procedure (P),
We present a complete model for secure communication between different entities and secure access to data. There are four algorithms in the proposed scheme.

Step 1 describes secure communication of data between DO and CSP moreover this insures data confidentiality and, authentication of DO and CSP.
Step 2 describes procedures which DO and CSP apply after a new file creation in respect.
Step 3 describes about secure communication of data between CSP and user. In this step user's authorization is also checked.
Step 4 describes the threshold cryptography technique for decryption of a user's file.

Output(O)- Step 4 is applied at user side where number of keys is reduced (one key corresponding to one group) and no threat of collusion attack as in group-key scheme.

VII. ALGORITHM

AES Algorithm Steps

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data? The data to be encrypted. This array we call the state array.

You take the following AES steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.

Note: **AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds.**

A. BLOCK DEIAGRAM OF SYSTEM

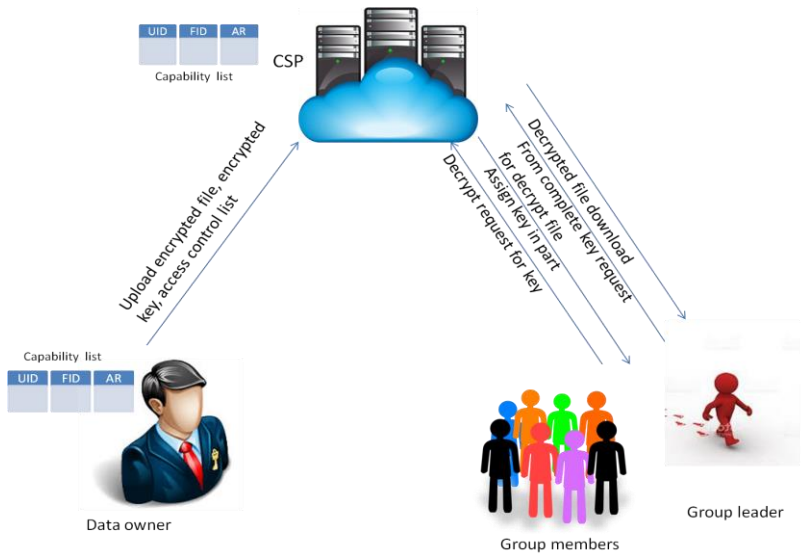


Figure 4.1. Block diagram of Identity based

Modules:

Original data holder
Data holder contain a capability list in which it will store (UID, FID,AR). Data holder upload data on cloud, holder may update the data, holder can view user related data, the data should be encrypted with a key. If any request is send by the user then cloud send notification to the holder.

System application users
Users will send request for accessing the data, cloud give response to register first then user send registration request to data holder then user will get response of data which is in encrypted form. If any error occurs then notification directly send to data holder

Cloud storage Provider
Cloud will contain copy of capability list and encrypted list. Capability list is a copy of data holder capability list and in encrypted list contain FIB, base address. And send notification to holder and give response to users.

B. HARDWARE REQUIREMENT

i) System Processors: Core2Duo

ii) Speed: 2.4 GHz

iii) Hard Disk :150 GB

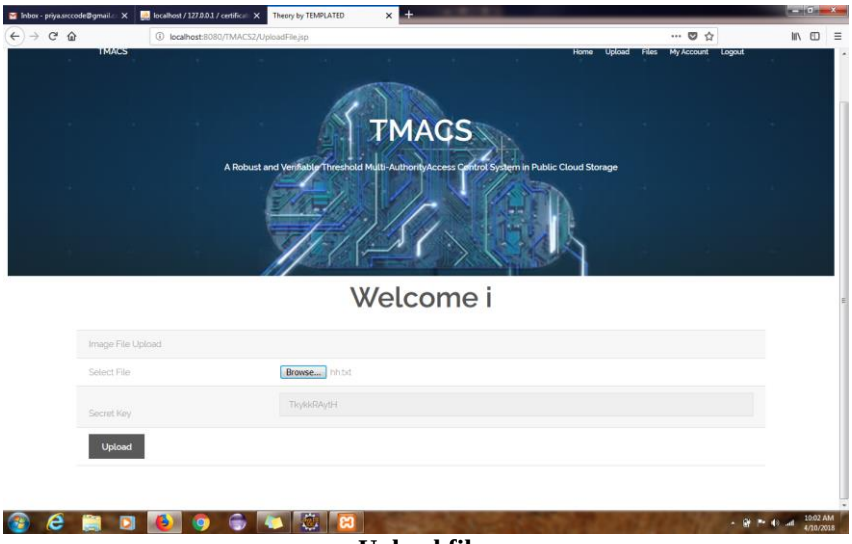
VIII. ADVANTAGES

In our system we are focusing especially on performance and security.
Considering the bottle neck we proposed TMACS as solution purpose.

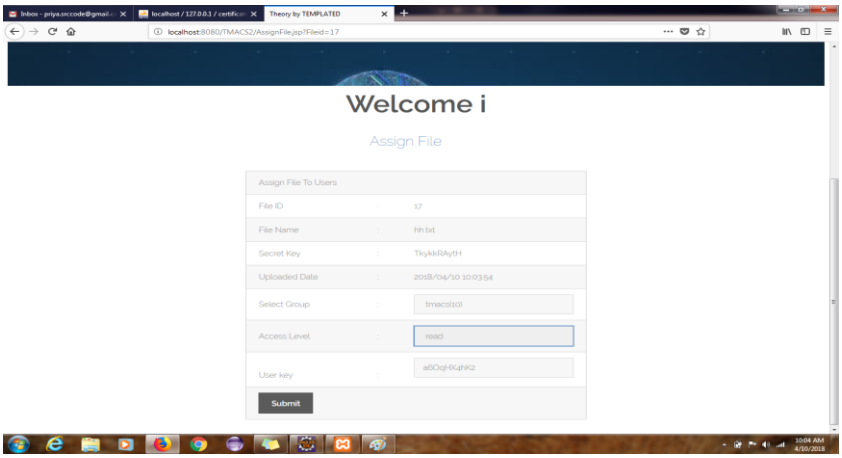
IX. APPLICATION

i) Encryption decryption system
ii) Enterprise or any organization can use this application for securely share data within their network.
iii) Cloud providers can also this system to avoid data leakage.

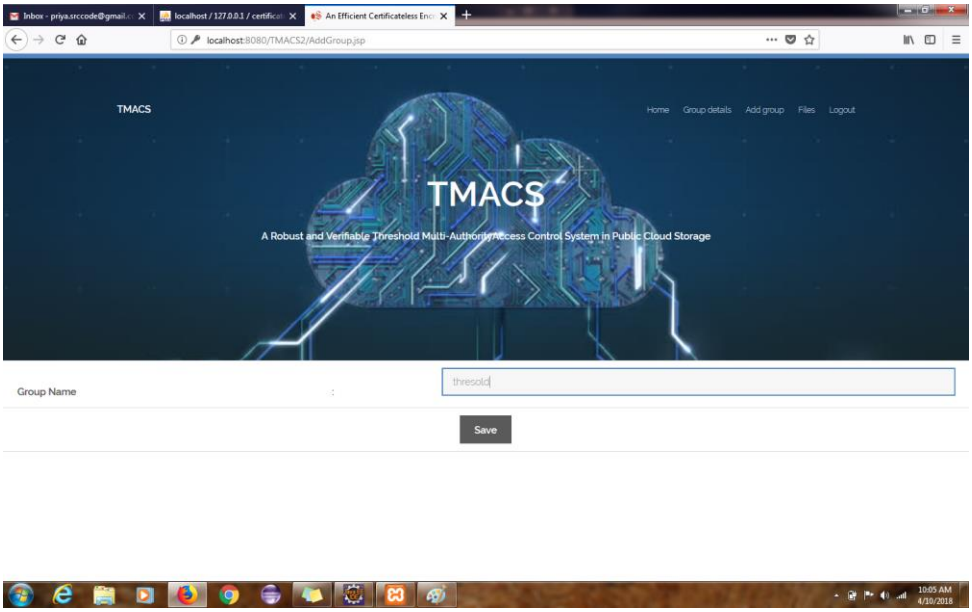
X. RESULT



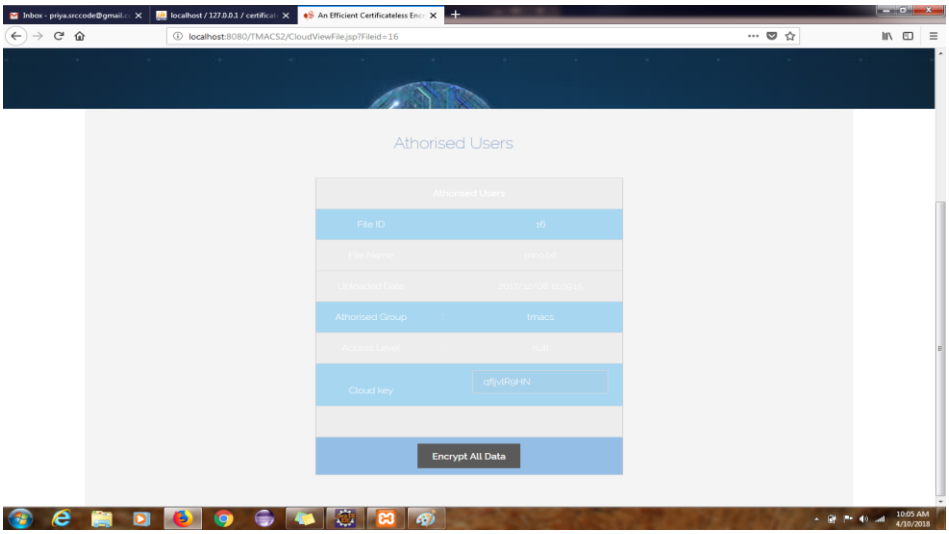
Upload files



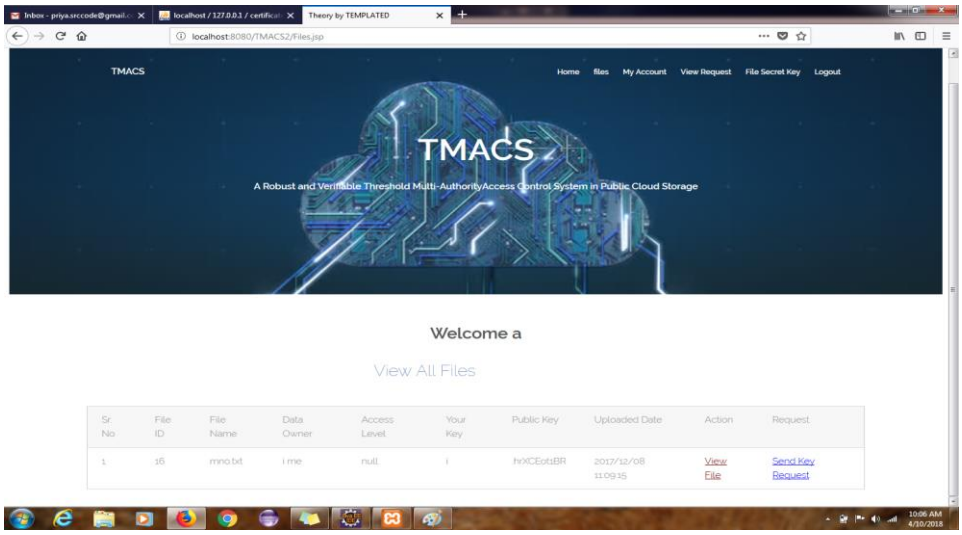
Assign file to group



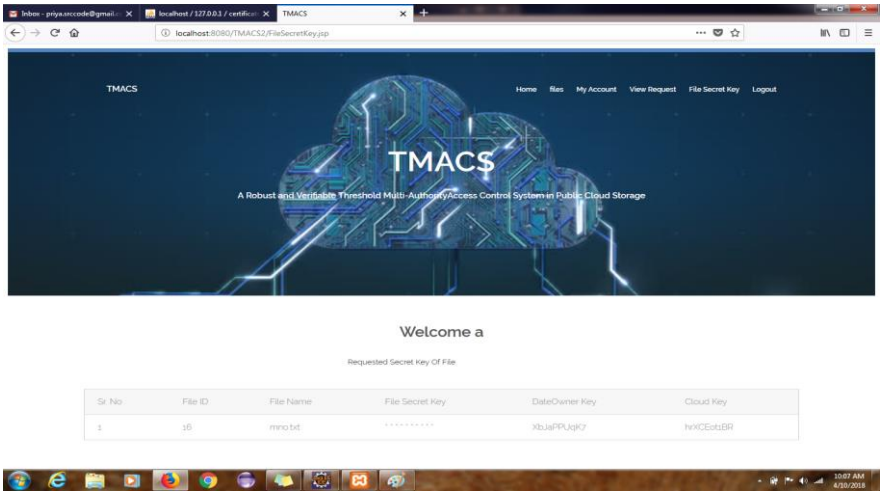
Add new group



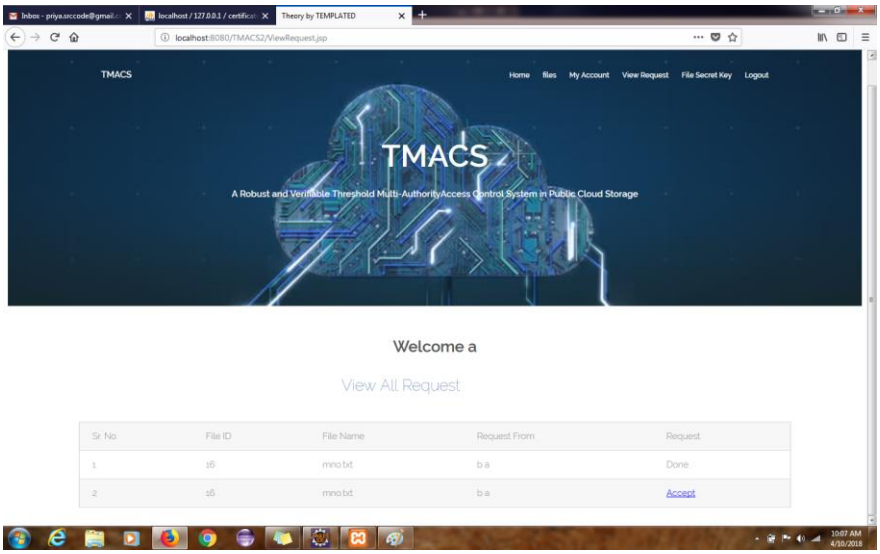
Encrypt all data to access file by user



Send key request by user



File secret key, data owner key and cloud key



Accept or decline request by user

XI. CONCLUSION AND FUTURE SCOPE

In this paper, we tend to tend to propose a replacement threshold multi-authority CP-ABE access management theme, named TMACS, in public cloud storage, at intervals that all AAs jointly manage the whole attribute set and share the key α. Taking advantage of (t, n) threshold secret sharing, by interacting with any t AAs, a legal user will generate his/her secret key. Thus, TMACS avoids anybody AA being a single-point bottleneck on each security and performance. The analysis results show that our access management scheme is powerful and secure. We will merely notice acceptable values of (t, n) to form TMACS not alone secure when however t authorities are compromised, however conjointly sturdy once no however t authorities are alive within the system.

ACKNOWLEDGMENT

Authors want to acknowledge Principal, Head of department and guide of their project for all the support and help rendered. To express profound feeling of appreciation to their regarded guardians for giving the motivation required to the finishing of paper.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, vol. 53, no. 6, p. 50, 2009.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th Financial Cryptography and Data Security. Springer, 2010, pp. 136–149.

[3] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2005, pp. 457–473.

[5] R. Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2014, pp. 195–203.