Multi Attribute based cloud Security using re-encryption

Madhavi Adodariya[1], Dr Vipul Vekariya[2], Prof. Shradhdha Bhalodiya[3]
[1]PG Scholar, [2] Principal, Noble Group of Institution, [3]Assistant Professor, Noble Group of Institution,
[1] Noble Group of Institution, Junagadh,
Gujarat, India

Abstract : As of late, numerous clients have transferred information to the cloud for simple stockpiling and offering to different clients. In the meantime, security and protection worries for the information are developing.Attribute-based encryption (ABE) enables both data security and access control by defining users with attributes so that only those users who have matching attributes will decrypt them. But if any attacker track the single attribute then it can be possible to attack to cloud. So in our proposed system multi attribute based multi level encryption (MABLE) then after completing attribute based encryption we will apply re-encryption with MABE so no one can decrypt. During implementations, ABE is used in fusion with a symmetric encryption scheme such as the advanced encryption standard (AES) where data is encrypted with AES and the AES key is encrypted with ABE. We will strengthen our client side encryption system and focus on retrieval of appropriate data.

IndexTerms **– Identity based encryption, MABLE, Reencryption,Security**

I. INTRODUCTION

In recent years, cloud storage has become a well-liked means that for straightforward knowledge storage and sharing with different users. The bigger the quantity and kinds of knowledge keep in cloud by several users, the bigger the safety and privacy issues for the information. Attribute-based encoding (ABE) is AN encoding theme 1st planned by Sahai and Waters [1] that achieves each knowledge security and access management by granting completely different decipherment rights to users supported attributes like the user's department and position. 2 main schemes exist for ABE: key-policy ABE (KPABE) [2] and ciphertext-policy ABE (CP-ABE) [3].

In these 2 schemes, AN access structure known as "policy" is employed to denote the decipherment condition exploitation AND and OR operations, for example: . In KP-ABE, knowledge is encrypted with a collection of attributes whereas a user's secret secret is generated supported a policy. In CP-ABE, knowledge is encrypted with a policy whereas a user's secret secret is generated supported

a set of attributes. CP-ABE is usually thought of for cloud service applications as knowledge is directly encrypted with the decipherment condition, implementing stronger access management over the information. Revocation of users or their attributes is an imperative feature of ABE for real-world applications. In real-world things, users and their attributes amendment over time withinthe system. for instance, users could also be found to be malicious, could merely leave the system, or their attributes could amendment. Therefore, revoking users or their attributes consequently so they'll not rewrite knowledge is very important. Existing revocation ways of ABE [13, 14, 15] square measure planned basedon the notion of exploitation ABE to write the information entirely, whereas in actual implementations, hybrid encoding of ABE and trigonal encoding, specifically the advanced encoding customary (AES), square measure used for potency. In hybrid encoding, knowledge is encrypted with AES and also the AES secret is encrypted with ABE. as a result of existing revocation ways have an effect on solely ABE ciphertext, this reality introduces a haul within which users will keep the AES key before revocation and use it to rewrite knowledge even once the users square measure revoked. Therefore, though existing revocation ways will be applied to revoke users from ABE, re-encrypting knowledge with a replacement AES secret is necessary so the recent AES key will not be used.

The additional attainable analysis directions of knowledge encoding technologies square measure as follows:

Data encryption combined with the distributed computing analysis. to write down in code and rewrite large data stream amount of your time in a {very} very distributed setting like cloud computing, it's necessary to vogue associate encryption formula which is able to be used effectively in a {very} very distributed setting. encryption combined with search technology. The because of search the information needed chop-chop among the cipher text still must be researched. encryption combined with processing technologies. data generally have choices of giant amount, high-dimensional data and high redundancy. The thanks to dig out useful data for encryption among data.

II. RELATED WORK

In this paper, they projected AN attribute-based proxy re-encryption methodology that uses ABE in hybrid with the symmetrical proxy re-encryption theme projected by Syalim et al. Potential future works embrace the following: i) in AN extremely future experiment, we tend to square measure reaching to prepare the DO and cloud servers one by one ii) we tend to square measure reaching to apply a definite symmetrical proxy re-encryption theme with the projected protocol.

In this paper, they projected a proxy re-encryption technique that uses ABE in hybrid with Syalim et al.s Centro trigonal proxy re-encryption theme so as that data could also be re-encrypted by cloud servers, but disadvantage that it takes longer computation time than the trivial answer of AES and ABE.

In this paper, each user is assigned a set of attributes that characterize his identity among the system. The encrypted datasets to be shared among users ar hold on among the cloud, and additionally the access management is provided by science ways that. the premise of the system is multi-authority attribute-based secret writing theme. among the long run, they commit to expand the utility of our paradigm to substantiate the protection of users groups operational with shared resources hosted among the cloud.

In this paper, the knowledge owner is capable of amendment, downloading and proving access management to the data saved by the Cloud Service provider (CSP). {the data|the knowledge|the data} owner is to boot prepared of storing this information in encrypted kind on the remote cloud servers. Also, among the event of disagreement concerning data integrity, a trustworthy Third Party (TTP) is in an exceedingly position to create your mind au fait the users that unit dishonest.

In this paper atmosphere is developed to access data firmly between numbers of users. code algorithmic rule is utilized for secret writing. By victimization multiple key data is in re-encrypted sort and performed secure access between numbers of users. Future scope are going to be, to introduce compression among the cluster for rising speed of data sharing and it'll be used another secret writing algorithmic rule.

From this literature survey, we've known the analysis downside on that we've outlined our planned work. we've found that for security purpose utterly completely different cryptography techniques unit used. They works well but they're going to decrypted by attackers. thus we would decide to develop Multi Attribute based cryptography technique to make safer and reliable.

III. PROPOSED METHODOLOGY

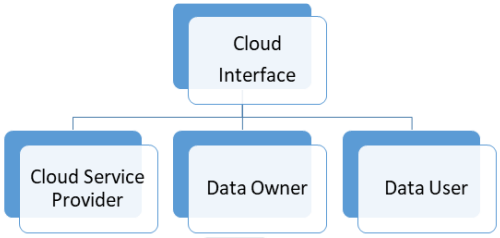


Figure 1. Main Components of Our Cloud

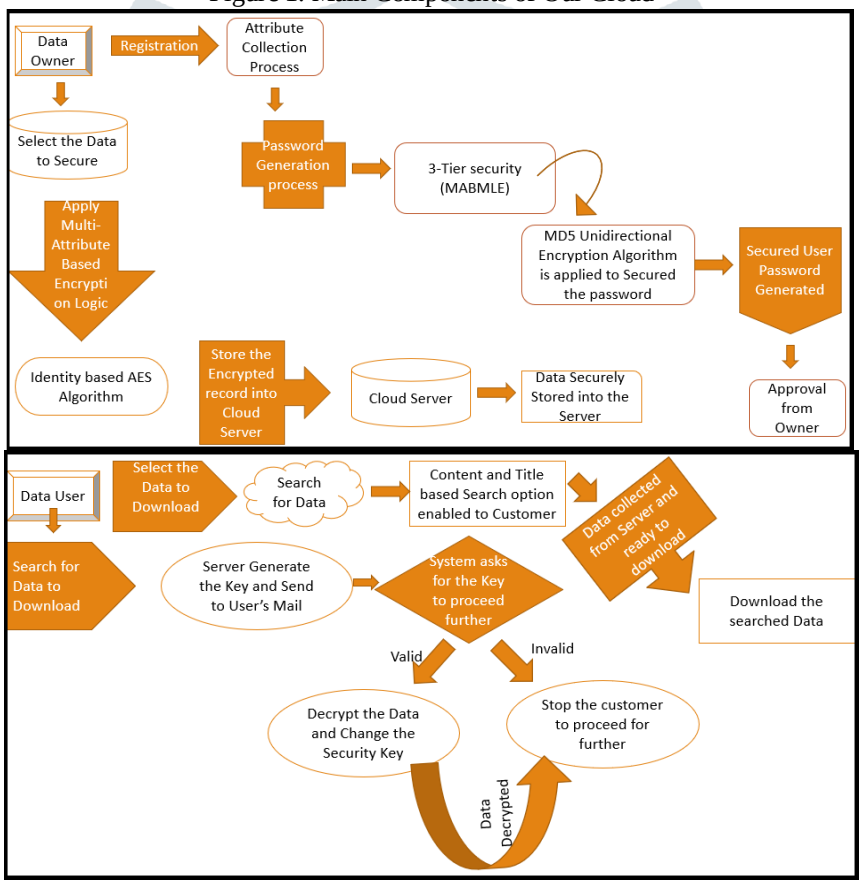


Figure 2 Working of cloud owner and user

Algorithm-1: Multi-attribute Based Multi Level Encryption Algorithm (MABMLE)

If Fake Intruder will enter in our cloud as owner or user then difficult to keep cloud safe So important to keep multi-level security.

Step-1: Registration Required for Owner & User

Step-2 : Registration Module

Step-3: Insertion of details

- Name
- E-mail Id
- Mobile Number
- City
- State
- Country
- Type of User (Owner / User)

Note : Not Asked Password

Step-4 : All necessary validations – alert generation
Step-5 :Security Level-1

- Get 3 attributes from name (NM) , Get 3 attributes from Mobile Number (MB)
- Key Generation (RN) -> Random number generation for 6 digits
- Multi-attribute based secure code -> NM + MB+ RN

Step-6 : Security Level-2

- MD5 Encryption of multi attribute password
- Used md5cryptoserviceprovider
- Compute hash from the bytes of text
- Get hash result after compute it
- Change it into 2 hexadecimal digits for each byte

Step-7 : Security Level -3

- Credential Details are pushed in server but "**Active=0** "& when we are giving same email id and password still " **Invalid authentication**"
- Without **permission to push/ Retrieve data** by Cloud Service Provider, Owner can not enter into the cloud.
- For that, Cloud Service Provider will enter into the cloud.

Step:-8: Approval

- Cloud service provider can view all data users and data owners
- Any time they can activate or deactivate users.
- For that one parameter "Active" if active 0 then owner or user can not enter in cloud.
- If active=1 by the CSP then only they can enter.

Step:-9: Data Insertion

Modified Rijindeal algorithm

Input: 128 bytes of information for encryption
Output: Same sized ciphertext block

1. KeyExpansion—

Round keys are derived using Rijndael's key schedule from the from the cipher key.
2. InitialRound
i. AddRoundKey—The round key is XORed with each byte of the state.
3. Internal Rounds
i. SubBytes—a non-linear substitution step where each byte is replaced
with another according to a lookup table.
ii. ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
iii. MixColumns—a mixing operation which operates on the columns of
the state, combining the four bytes in each column.
iv. AddRoundKey
v. Evaluate rotate key code using parity bits on round keys as explained.
vi. RotateMatrix—rotates the entire matrix by an angle specified by
rotate key code.
4. Final Round (no MixColumns)
i. SubBytes
ii. ShiftRows
iii. AddRoundKey
iv. RotateMatrix

Identity based dynamic re-encryption algorithm

Step-1: Use Modified Rijndael Algorithm
Step-2: Dynamic Encryption key
(In every algorithm public key or private is static but we have different keys for different user so It can not decrypt)

- Unique -> RegID, Name= Nm, Mail Id = MI , Mobile - Mb
- Encryption Key = RegID + Nm + Ml + Mb;

Step-3: Re-Encryption of previous output
Step-4: Store encrypted file in cloud
Step-5: any one can view that uploaded file.
Step-6: Data user inserts credentials
Step-7: search data
Step-8: Retrieval of data
Step-9: Last level security

- Send OTP
- Verify the authenticity

Then user can download the decrypted data

IV. Result Analysis

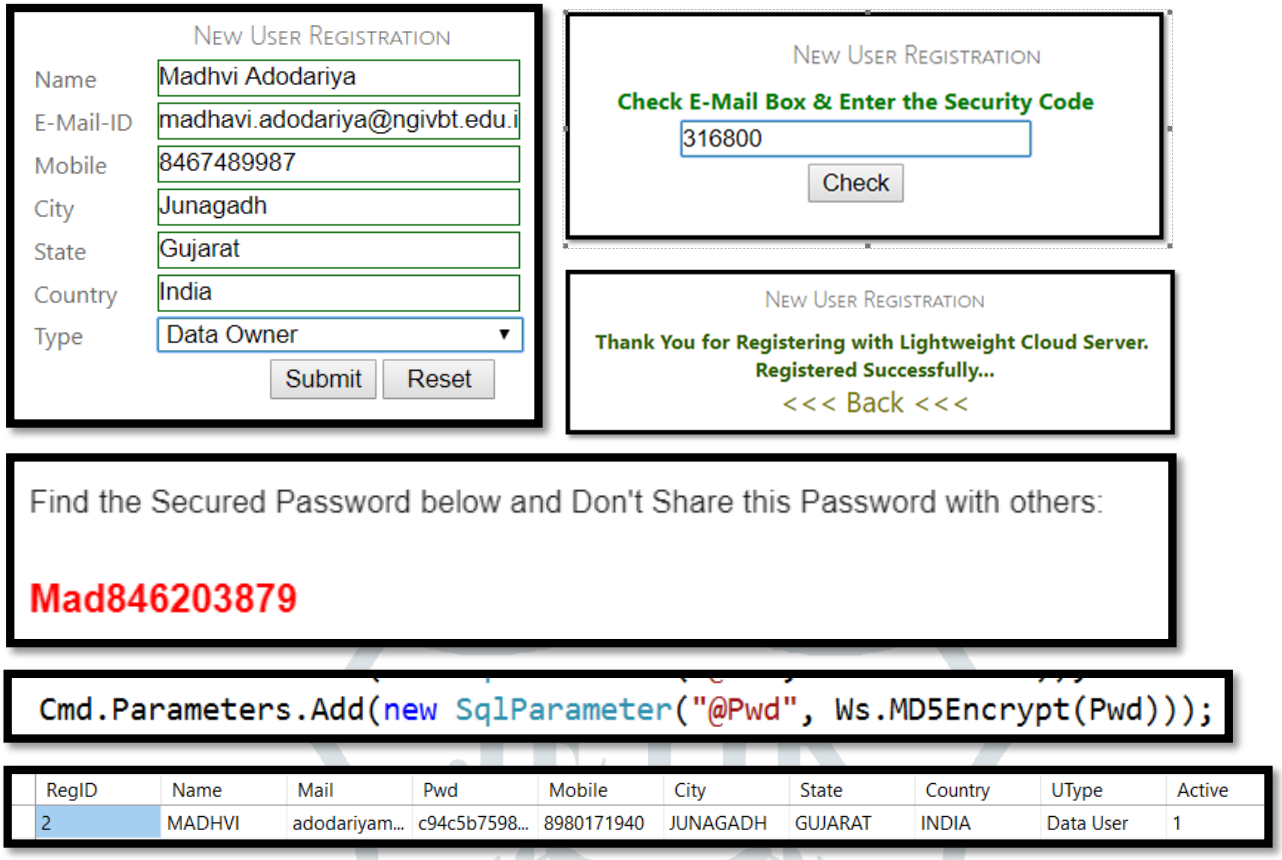
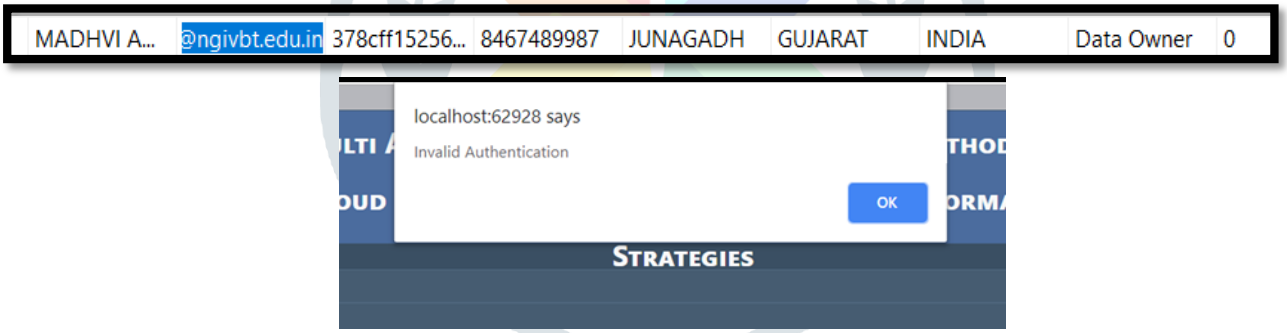


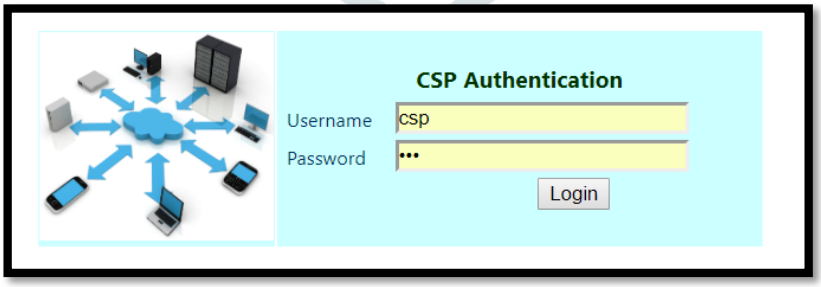
Figure 3. Two level security

Security level-3

Credential Details are pushed in server but "Active=0 "& when we are giving same email id and password still " Invalid authentication"



Need Cloud service provider for for Approval



If Red line -> Not Active , Green line -> Active

Activate / Deactivate Data Owners

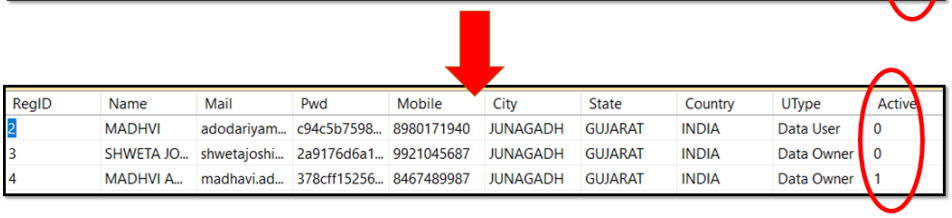
NAME	E-MAIL-ID	MOBILE	CITY	STATE	COUNTRY		
SHWETA JOSHI	shwetajoshi228@gmail.com	9921045687	JUNAGADH	GUJARAT	INDIA	Activate	Deactivate
MADHVI ADODARIYA	madhavi.adodariya@ngivbt.edu.in	8467489987	JUNAGADH	GUJARAT	INDIA	Activate	Deactivate

Suppose CSP wants to deactivate after some time then

Activate / Deactivate Data Users

NAME	E-MAIL-ID	MOBILE	CITY	STATE	COUNTRY		
MADHVI	adodariyamadhavi96@gmail.com	8980171940	JUNAGADH	GUJARAT	INDIA	Activate	Deactivate

RegID	Name	Mail	Pwd	Mobile	City	State	Country	UType	Active
2	MADHVI	adodariyam...	c94c5b7598...	8980171940	JUNAGADH	GUJARAT	INDIA	Data User	1
3	SHWETA JO...	shwetajoshi...	2a9176d6a1...	9921045687	JUNAGADH	GUJARAT	INDIA	Data Owner	0
4	MADHVI A...	madhavi.ad...	378cff15256...	8467489987	JUNAGADH	GUJARAT	INDIA	Data Owner	1



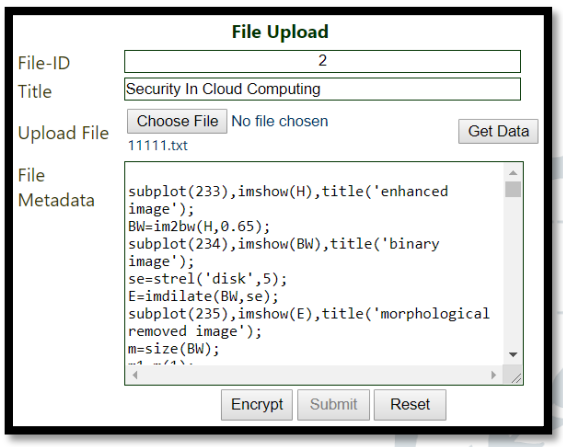
RegID	Name	Mail	Pwd	Mobile	City	State	Country	UType	Active
2	MADHVI	adodariyam...	c94c5b7598...	8980171940	JUNAGADH	GUJARAT	INDIA	Data User	0
3	SHWETA JO...	shwetajoshi...	2a9176d6a1...	9921045687	JUNAGADH	GUJARAT	INDIA	Data Owner	0
4	MADHVI A...	madhavi.ad...	378cff15256...	8467489987	JUNAGADH	GUJARAT	INDIA	Data Owner	1

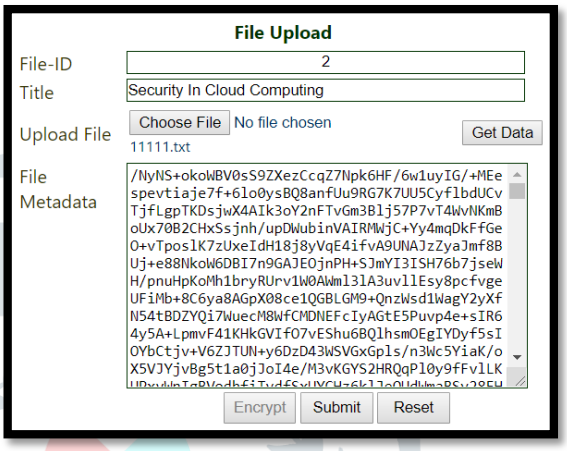
Grant from CSP to enter in system

So now data owner can push data on cloud after identity checking

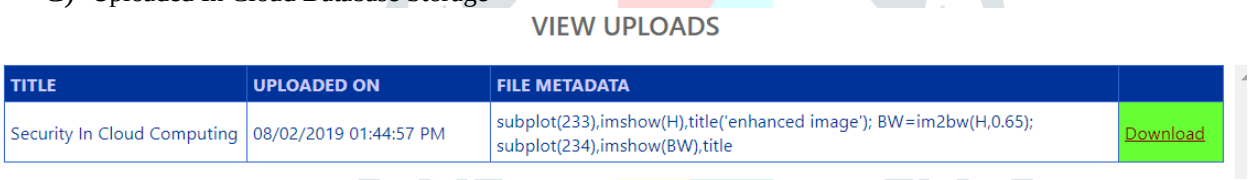
A) Push File in cloud and Select File

B) Re-encryption of file





C) Uploaded In Cloud Database Storage



Retrieval phase

User give credential then Search Data & retrieve data and does Authentication verification & download

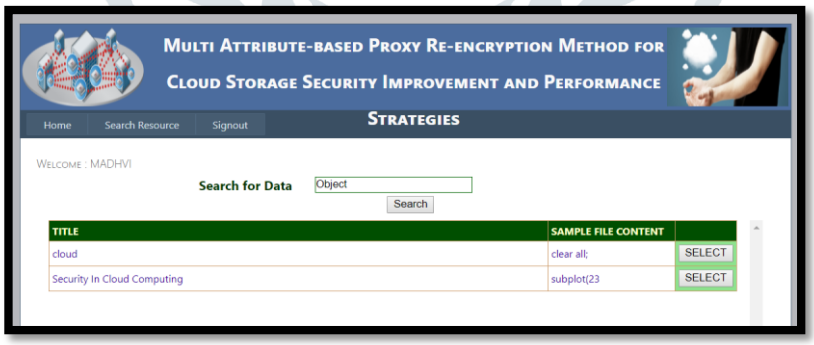


Table 1 . Parameters for evaluation

Aspects	Base	Proposed
Security	User Authentication security -> AES +ABE File Security -> No such method applied	User Authentication security -> RMABMLE+AES File Security -> Identity based re encryption
Availability	Implemented and tested in local machine	Live Cloud
Responsive	Faster Response in local machine	Faster Response in live cloud
Reliability	Less reliable because of level -1 security	3 tier security
Attack possibility	Possibility of attack is more	Not possible and if it happens then -> no useful data for attacker -> can not decrypt

V. CONCLUSION

In this paper, We have studied various encryption methods for cloud computing They works well but they can decrypted by attackers. So we have concluded from literature that we can extended attribute encryption method and that method is also extended with the help of Dynamic multi-attribute based encryption. We can extend it using multi attribute based key generation method. It has one way decryption so that it can not be decrypted. We have implemented in single live public cloud of MyASP.NET. To improve the retrieval we have added functionality of content base retrieval. In future we can increase file level security and give more focus on storage in cloud.

REFERENCES

[1] Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In Kaisa Nyberg, editor, EUROCRYPT'98, volume 1403 of LNCS, pages 127–144, Espoo, Finland, May 31 – June 4, 1998. Springer, Berlin, Germany.
[2] Anca Ivan and Yevgeniy Dodis. Proxy cryptography revisited. In NDSS 2003, San Diego, California, USA, February 5–7, 2003. The Internet Society.
[3] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In NDSS 2005, San Diego, California, USA, February 3–4, 2005. The Internet Society.
[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Transactions on Information and System Security, vol. 9, no. 1, pages 1–30. 2006.
[5] Yun-Peng Chiu, Chin-Laung Lei, and Chun-Ying Huang. Secure multicast using proxy encryption. In Sihan Qing, Wenbo Mao, Javier Lopez, and Guilin Wang, editors, ICICS 05, volume 3783 of LNCS, pages 280–290, Beijing, China, December 10–13, 2005. Springer, Berlin, Germany.
[6] J. Shao, P. Liu, G. Wei, and Y. Ling. Anonymous proxy reencryption. Security and Communication Networks, vol. 5, no. 5, pp. 439-449, 2012.
[7] K. Liang, M. H. Au, J. K. Liu, X. Qi, W. Susilo, X. P. Tran, D. S.Wong, and G. Yang. A dfa-based functional proxy reencryption scheme for secure public cloud data sharing. IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667-1680, 2014.
[8] Kaitai Liang, Joseph K. Liu, Duncan S. Wong, and Willy Susilo. An efficient cloud-based revocable identity-based proxy reencryption scheme for public clouds data sharing. In Miroslaw Kutylowski and Jaideep Vaidya, editors, ESORICS 2014, Part I, volume 8712 of LNCS, pages 257–272, Wroclaw, Poland, September 7–11, 2014. Springer, Berlin, Germany.
[9] Ying Wang, Jiali Du, Xiaochun Cheng, Zheli Liu, and Kai Lin. Degradation and encryption for outsourced png images in cloud storage. International Journal of Grid and Utility Computing, vol. 7, no. 1, pp. 22-28, 2016.
[10] Shuaishuai Zhu and Xiaoyuan Yang. Protecting data in cloud environment with attribute-based encryption. International Journal of Grid and Utility Computing, Vol. 6, No. 2, pp. 91-97, 2015.
[11] Shu Guo and Haixia Xu. A secure delegation scheme of large polynomial computation in multi-party cloud. International Journal of Grid and Utility Computing, Vol. 6, No. 2, pp. 1-7, 2015.
[12] Cristina Dutu, Elena Apostol, Catalin Leordeanu, and Valentin Cristea. A solution for the management of multimedia sessions in hybrid clouds. International Journal of Space-Based and Situated Computing, Vol. 4, No. 2, pp. 77-87, 2014.
[13] Meriem Thabet, Mahmoud Boufaida, and Fabrice Kordon. An approach for developing an interoperability mechanism between cloud providers. International Journal of Space-Based and Situated Computing, Vol. 4, No. 2, pp. 88-99, 2014.
[14] Lihua Wang, Licheng Wang, Masahiro Mambo, and Eiji Okamoto. Identity-based proxy cryptosystems with revocability and hierarchical confidentialities. In Miguel Soriano, Sihan Qing, and Javier Lopez, editors, ICICS 10, volume 6476 of LNCS, pages 383–400, Barcelona, Spain, December 15–17, 2010. Springer, Berlin, Germany.
[15] Xu An Wang, Yunlong Ge, and Xiaoyuan Yang. PRE+: Dual of proxy re-encryption and its application. Cryptology ePrint Archive, Report 2013/872, 2013. http://eprint.iacr. org/2013/872.