Secure Data Group Sharing and Distribution with Multi-Owner using Multi Cloud Storage Services

Ms. Judith Peters, Prof. M.E. Sanap

PG student, Computer Department, STES'S SAE, Kondhwa, Pune, India
Associate Professor, Computer Department, STES'S SAE, Kondhwa, Pune, India.

Abstract: A secure data cluster sharing and conditional dissemination theme with multi-owner in cloud computing, with in which data owner will share non-public data with a group of users via the cloud in an exceedingly secure manner, and data communicator will share the data to a brand new cluster of users if the attributes satisfy the access policies within the ciphertext. We have a tendency to additional gift a multiparty access management mechanism over the disseminated cipher text, within which the data co-owners will append new access policies to the cipher text thanks to their privacy preferences. Moreover, 3 policy aggregation ways, together with full permit, owner priority and majority permit, are provided to solve the privacy conflicts downside caused by completely different access policies. Many schemes are recently advanced for storing information on multiple clouds. Distributing data over completely different cloud storage suppliers (CSPs) mechanically provides users with a definite degree of data run management, for no single purpose of attack will leak all the data. However, unplanned distribution of data chunks will cause high information revealing even whereas exploitation multiple clouds. An efficient storage plan generation algorithmic rule supported cluster for distributing information chunks with least data escape across multiple clouds. So to provide more security to user's data we will divide our data into multiple blocks and upload those blocks onto multiple clouds. As each block is on different cloud, if there is attack on any cloud the remaining blocks which are stored on other clouds will be safe, this is how we are providing more security to user's data.

Keywords — Data Sharing, Conditional Proxy re-encryption, Attribute-based encryption, Privacy Conflict, System Attack ability, Remote Synchronization, Distribution and Optimization.

I. INTRODUCTION

The fame of distributed computing is acquired from the advantages of rich stockpiling assets and moment get to. It totals the assets of processing infrastructure and then gives on-request benefits over the Internet. Many famous companies are now providing public cloud services, such as Amazon, Google, and Alibaba. These services allow individual users and enterprise users to upload data (e.g. photos, videos and documents) to cloud service provider (CSP), for the purpose of accessing the data at any time anywhere and sharing the data with others. With the more and more fast uptake of devices like laptops, cell phones and tablets, users need associate degree present and massive network storage to handle their ever-growing digital lives. To fulfill these demands, several cloud-based storage and file sharing services like Dropbox, Google Drive and Amazon S3, have gained quality because of the easy-to-use interface and low storage price. However, these centralized cloud storage services are criticized for grabbing the management of users' knowledge that permits storage suppliers to run analytics for promoting and advertising [1]. One possible resolution to scale back the chance of data leak is to use multi cloud storage systems [2], [3], [4], [5] in which no single purpose of attack will leak all the data. A malicious entity, like the one disclosed in recent attacks on privacy [6], would be needed to oblige all the various CSPs on that a user would possibly place her knowledge, so as to induce a complete image of her knowledge. Put simply, as the saying goes, do not put all the eggs in one basket.

The re-encryption key is associated with a set of attributes, thus the proxy can re-encrypt the ciphertext only when the re-encryption key matches the access policy. In this way, data owner can customize fine-grained dissemination condition for the shared data. For example, data owner allows project managers in the organization to disseminate the progress report in OneDrive, while only permits executive directors in finance department to disseminate the project budget in OneDrive during a specific time period. Besides the need of conditional data dissemination, multiparty access control problem for data sharing in cloud computing like cloud collaboration and cloud-based social networks comes along [18, 19], which means the special authorization requirements from multiple associated users are often accommodated together to control the shared data. Consider an example where a co-authoring document or a co-photo in cloud computing with three users, Alice, Bob, and Carol. If Alice who is that the data owner uploads this co-authoring document or co-photo to the CSP and tags both Bob and Carol because the co-owners. Alice can restrict this data to be disseminated to a certain group of users, while the co-owners Bob and Carol may have different privacy concerns about this data. It is a massive and high privacy problem if applying the preference of just one party, which can cause such data to be shared with undesired receivers.

II. RELATED WORK

They made [1], a framework for Ciphertext-Policy Attribute Based Encryption. Our framework takes into consideration another kind of encoded get to regulate where client's private keys are specified by tons of qualities and a gathering scrambling information can determine a technique over these qualities indicating which clients can decode. Our framework permits strategies to be communicated as any monotonic tree get to structure and is impervious to intrigue assaults during which an assailant may acquire numerous private keys. At long last, we gave a usage of our framework, which incorporated a couple of enhancement methods.

Intermediary based, [2] numerous cloud capacity framework that for all intents and purposes tends to the unwavering quality of the present cloud reinforcement stockpiling. NCCloud not just gives adaptation to internal failure away, yet in addition permits practical fix when a cloud for all time falls flat. NCCloud executes a viable adaptation of the FMSR codes, which recovers new equality pieces during fix subject to the necessary level of information excess. Our FMSR code usage dispenses with the encoding necessity of capacity hubs (or cloud) during fix, while guaranteeing that the new arrangement of put away lumps after each round of fix jam the necessary adaptation to non-critical failure. Our NCCloud model shows the viability of FMSR codes in the cloud reinforcement use, as far as money related expenses and reaction times.

The Internet of Things (IoT) [3], gadgets continually create information, and require the information examination to be fast, which can't be given by the conventional distributed computing design. With the objective of breaking down the IoT information near the gadgets that create and work on the information, edge figuring has been acquainted for the expansion with the edge of the system from distributed computing. Despite the fact that edge registering encourages distributed computing in tending to the inertness issue of information handling, it likewise brings greater security and protection issues to the current distributed computing system. Because of the reality that property based encryption (ABE) underpins fine-grained (or versatile) get to control for information things in scrambled structures, ABE has been generally accepted to be a perfect answer for ensure information security and protection for situations of distributed computing. To accomplish fine-grained get to control for the edge figuring condition, in this paper, we proposed an idea named intermediary supported ciphertext-approach characteristic based encryption (PA- CPABE). Subsequent to portraying a conventional development of PA-CPABE, we officially examined its security. What's more, we displayed and actualized a launch of PA-CPABE to assess its proficiency.

In this paper [4], we have a tendency to tend to propose a combined the cloud-side and knowledge owner-side access management in encrypted cloud storage, that is proof against DDoS/EDoS attacks and provides resource consumption accounting. Our system supports absolute CP-ABE constructions. The event is secure against malicious information users and a covert cloud provider. We have a tendency to tend to relax the protection demand of the cloud provider to covert adversaries, which can be an extra wise and relaxed notion than that with semi-honest adversaries.

We presented [5], the principal personality based communicate encryption (IBBE) conspire with steady size ciphertext and private keys. One intriguing open issue would be to build an IBBE framework with consistent size ciphertext and private keys that is secure under a progressively standard supposition, or which accomplishes a more grounded security idea, identical to full security in IBE plans.

To address the data protection [6], problem in cloud computing, we propose and implement a role-based self-contained data protection scheme called RBAC-CPABE. Based on the classic RBAC model, we first propose a data-centric access control model, DC-RBAC, which allows the data owner to specify individualized RBAC policies for each data object. Besides role-level constraints, DC-RBAC also contains user attribute constraints and environment constraints, which correspond to information about the authorized users and contextual information about the environment, respectively. Hence, DC-RBAC achieves more flexible and fine-grained access control. Next, to construct the self-contained data protection mechanism, we fuse the DC-RBAC into ECP-ABE by extending ECP-ABE and defining a policy mapping model. By using RBAC-CPABE, information contained in the data itself determines whether users are authorized to perform decryption instead of relying on other parties.

In this paper [7], we propose a protected customer side deduplication plot KeyD to successfully oversee focalized keys. Information deduplication in our structure is accomplished by co-operations between information proprietors and the Cloud Service Provider (CSP), without support of other confided in outsiders or Key. The board Cloud Service Providers. The security examination shows that our KeyD guarantees the secrecy of information furthermore, security of joined keys, and well ensures the client possession protection simultaneously. Exploratory outcomes exhibit that the security of our plan isn't at the cost of the exhibition. For our future work, we will attempt to look for approaches to ensure the personality security of information proprietors, which isn't considered in our plan.

From an occupant perspective [8] , the cloud security model doesn't yet hold against risk models produced for the ustomary model where the hosts are worked and utilized by a similar association. Nonetheless, there is a consistent advancement towards fortifying the IaaS security model. In this work we displayed a system for confided in foundation cloud arrangement, with two center focuses: VM organization on trusted register hosts and space based insurance of put away information. We depicted in detail the structure, usage furthermore; security assessment of conventions for trusted VM dispatch and space based stockpiling assurance. The arrangements depend on necessities evoked by an open human services authority, have been actualized in a famous open-source IaaS stage and tried on a model sending of a circulated EHR framework. In the security investigation, we presented a progression of assaults and demonstrated that the conventions hold in the predefined risk model. To acquire further certainty in the semantic security properties of the conventions, we have demonstrated and checked them with ProVerif [32]. At long last, our execution tests have indicated that the conventions present an inconsequential presentation overhead.

III. PROPOSED ALGORITHM

a. *Description of the Proposed Algorithm:*

1) Register & Login

- In this module, data owner, data co-owner, data disseminator and data user register with system based on his username, password, name, mobile no, and so on.
- Followed by, both are login and access file upload & download process in multi cloud.

2) Encrypt & Upload:

- In this module, a data owner wants to upload his files to Multi-cloud.
- So to do it data owner will require keys, so it sends request to third party auditor.
- Third party auditor generates public key and private key for each request and sends it to the respective data owner.
- After this data owner chooses the policy aggregation strategy amongst full permit, owner priority and majority permit.
- Then the data owner splits a file into blocks and encrypts each block. At the same time, it generates HMACSHA1 signature for each encrypted block.
- Then upload all encrypted blocks with signatures to multi-cloud.
- After this we have data co-owner in our system that re-encrypts the data which is already encrypted by data owner.
- Like owner, data co-owner also sends request for keys to the third party auditor.
- After this the data co-owner append the policy aggregation strategy amongst full permit, owner priority and majority permit
- The third party auditor sends generated public, private and symmetric key to respective data co-owner.
- Now with keys, data co-owner re-encrypts the data and uploads it to the different cloud.

3) Download & Decrypt:

- In this module we have data disseminator and data user.
- The data disseminator disseminates its data i.e. it holds the record of data owner and co-owners uploaded files.
- Data disseminator broadcast these records to all the data users in the system.
- Now, the registered data user will come to know that which blocks are available to download.
- So the data users request for keys, once they have keys they can download the encrypted blocks of files and also can decrypt the text to get the original one.

IV. PSEUDO CODE

Data Owner:
Steps:

1. Register
2. Login
3. Symmetric Key (AES), Secret Key, Public and Private Key Generation
4. Chooses the policy aggregation strategy amongst the full permit, owner priority and majority permit.
5. Data Owner sends the tagged notification to registered data co-owners.
6. Calculate size of the file.
7. Split or Divide the file into 3 different blocks.
8. Each part of the file is encrypted and uploaded to the multicloud environment.

Data Co-Owner:

Steps:

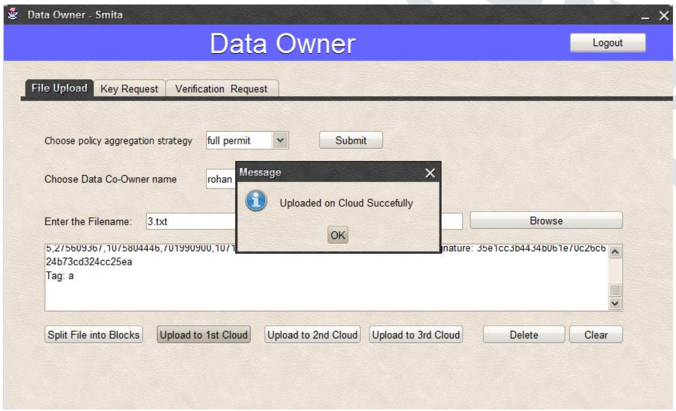
1. Register
2. Login
3. Symmetric Key (AES), Secret Key, Public and Private Key Generation
4. Appends the policy aggregation strategy to the data owner's blocks.
5. Selects the file amongst the available files and re-encrypt the file data.
6. After this, calculates the file size, and splits the file into 3 different blocks.
7. Each part of the file is encrypted and uploaded to the multi cloud environment.

Data User:

1. Register
2. Login
3. After successful login the data user have two options to download file.
4. First one is it can download data which is uploaded by data owner and second one is it can download data which is re-encrypted by data co-owner.
5. When it choses data owner he will get original data , but with data co-owner due to double encryption data is in encrypted form only.
6. As we have uploaded data to multiple clouds so to access it, we need to make a request for each block.
7. First form first clouds, data user selects the block of the file then it downloads the file.
8. Request for keys and decrypts the text to its original form.
9. Like first block, same procedure is followed for second and third block of the file
10. To download data form data co-owners, blocks are decrypted but they are in encrypted form only as we have applied re-encryption on them so rest of the procedure is same as data owner.

V. SIMULATION RESULTS

In proposed system there are six different users like data owner, data co-owner, data disseminator, data user, third party auditor and cloud service provider. Registered users in the system sends request for keys to the third party auditor, once users have keys they can perform respective tasks of them. Such as data owner will first choose the policy aggregation strategy from full permit, owner priority and majority permit strategies. After this splits file into blocks and encrypts each block along with signature generated uploads each block to different cloud so that if any block is attacked the remaining blocks will be safe from attacker. And in this project we are implementing multi cloud concept. Now data co-owner gets the tagged notification by data owner it selects policy aggregation strategy to append it to file and re-encrypts the file data and again splits that file into different blocks and upload them to different clouds. Data user with keys can download and decrypt the file data.


Data Owner - Smita

Data Owner

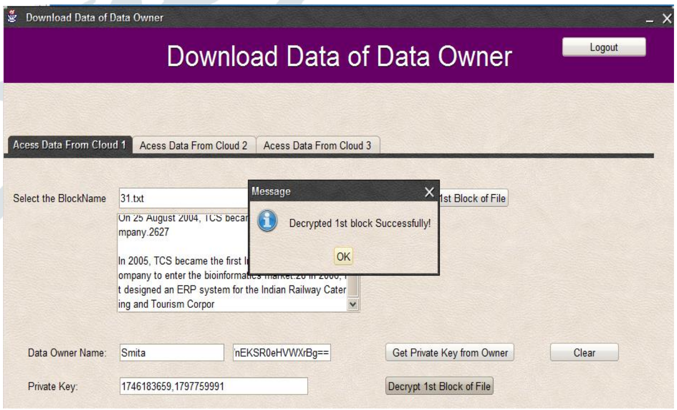
Choose policy aggregation strategy: full permit

Choose Data Co-Owner name: rohan

Enter the Filename: 3.txt

5,2756093б7,1075804446,701990900,107 … nature: 35e1cc3b4434b061e70c26c6
24b73cd324cc25ea
Tag: a

Message: Uploaded on Cloud Succefully


Download Data of Data Owner

Download Data of Data Owner

Select the BlockName: 31.txt

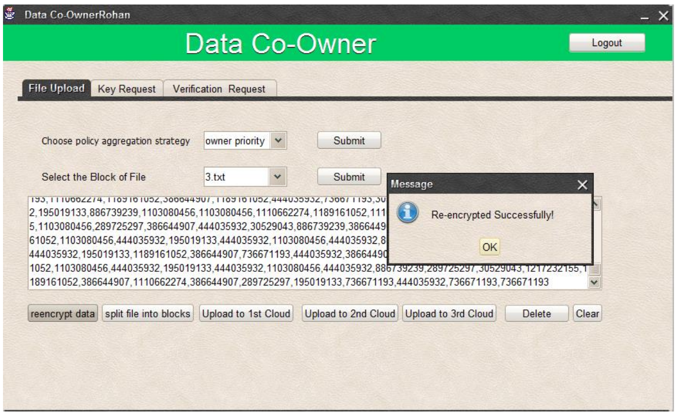
On 25 August 2004, TCS becar
mpany.2627

In 2005, TCS became the first I
ompany to enter the bioinforma
t designed an ERP system for the Indian Railway Cater
ing and Tourism Corpor

Message: Decrypted 1st block Successfully!

Data Owner Name: Smita 'nEKSR0eHVWXrBg==

Private Key: 1746183659,1797759991


Data Co-OwnerRohan

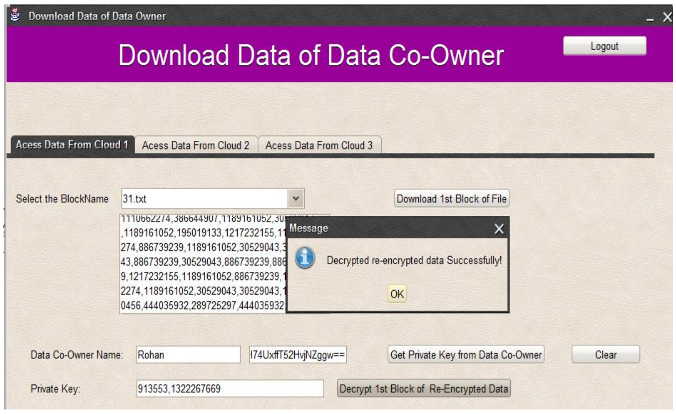
Data Co-Owner

Choose policy aggregation strategy: owner priority

Select the Block of File: 3.txt

2,195019133,886739239,1103080456,1103080456,1110662274,1189161052,111
5,1103080456,289725297,386644907,444035932,30529043,886739239,3866449
61052,1103080456,444035932,195019133,444035932,1103080456,444035932,8
444035932,195019133,1189161052,386644907,736671193,444035932,3866449
1052,1103080456,444035932,195019133,444035932,1103080456,444035932,886739239,289725297,30529043,1217232155,1
189161052,386644907,1110662274,386644907,289725297,195019133,736671193,444035932,736671193,736671193

Message: Re-encrypted Successfully!


Download Data of Data Owner

Download Data of Data Co-Owner

Select the BlockName: 31.txt

1110662274,386644907,1189161052,30
,1189161052,195019133,1217232155,11
274,886739239,1189161052,30529043,3
43,886739239,30529043,886739239,886
9,1217232155,1189161052,886739239,1
2274,1189161052,30529043,30529043,1
0456,444035932,289725297,444035932

Message: Decrypted re-encrypted data Successfully!

Data Co-Owner Name: Rohan I74UxffT52HvjNZggw==

Private Key: 913553,1322267669
Logout
Acess Data From Cloud 1
Acess Data From Cloud 2
Acess Data From Cloud 3
Download 1st Block of File
OK
Get Private Key from Data Co-Owner
Clear
Decrypt 1st Block of Re-Encrypted Data

VI. CONCLUSION AND FUTURE WORK

Distributing knowledge on multiple clouds provides users with a certain degree of data run management there in no single cloud supplier are aware of the entire user's knowledge. However, unplanned distribution of information chunks will cause avoidable information run. The data security and privacy is a concern for users in cloud computing. In particular, how to enforce privacy concerns of multiple owners and protect the data confidentiality becomes a challenge. Here, we are providing information leakage aware storage system and confidentiality of the data in an multi cloud environment.

REFERENCES

[1]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," Proc. IEEE Symposium on Security and Privacy (SP '07), pp. 321-334, 2007.

[2]. H. Chen, Y. Hu, P. Lee, and Y. Tang, "Nccloud: A network-coding-based storage system in a cloud-of-clouds," 2013.

[3]. H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," IEEE Access, vol. 6, pp. 30049–30059, 2018.

[4]. K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.

[5]. C. Delerabl´ee, "Identity-based broadcast encryption with constant size ciphertexts and private keys," Proc. International Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT '2007), pp. 200-215, 2007.

[6]. B. Lang, J. Wang, and Y. Liu, "Achieving flexible and self-contained data protection in cloud computing," IEEE Access, vol. 5, pp. 1510- 1523, 2017.

[7]. L. Liu, Y. Zhang, and X. Li, "KeyD: secure key-deduplication with identity-based broadcast encryption," IEEE Transactions on Cloud Computing, 2018,
https://ieeexplore.ieee.org/document/8458136.

[8]. N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 2017.

[9].T. G. Papaioannou, N. Bonvin, and K. Aberer, "Scalia: an adaptive scheme for efficient multi-cloud storage," in Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis. IEEE Computer Society Press, 2012, p. 20.

[10]. Z. Yan, X. Li, M.Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 485-498, 2017.

[11]. H. He, R. Li, X. Dong, and Z. Zhang, "Secure, efficient and fine-grained data access control mechanism for P2P storage cloud," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 471-484, 2014.

[12]. Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy reencryption for secure data sharing in cloud computing," IEEE Transactions on Services Computing, 2018, https://ieeexplore.ieee.org/docu ment/7448446.

[13]. J. Son, D. Kim, R. Hussain, and H. Oh, "Conditional proxy reencryption for secure big data group sharing in cloud environment," Proc. of 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 541–546, 2014

[14]. S. Choy, B. Wong, G. Simon, and C. Rosenberg, "A hybrid edge-cloud architecture for reducing on-demand gaming latency," Multimedia Systems, pp. 1–17, 2014.

[15]. L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," IEEE Access, vol. 5, pp. 13336 – 13345, 2017.

[16]. K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," Future Generation Computer Systems, vol. 52, pp. 95-108, 2015.

[17.] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing
and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584–36594, 2018.

[18]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” Proc. 13th ACM Conf. on Computer and Communications Security (CCS ‘06), pp.89- 98, 2006.

[19]. S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, “Attribute based data sharing scheme revisited in cloud computing,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1661–1673, 2016.

[20]. L. Guo, C. Zhang, H. Yue, and Y. Fang, “A privacy-preserving social assisted mobile content dissemination scheme in DTNs,” Proc. 32nd IEEE International Conf. on Computer Communications (INFOCOM ‘2013), pp. 2301-2309, 2013.

[21]. W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, “Attribute based access control with constant-size ciphertext in cloud computing,” IEEE Transactions on Cloud Computing, vol. 5, no. 4, pp. 617-627, 2017.

[22]. K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik, “Privacy-preserving attribute- based access control model for XML-based electronic health record system,” IEEE Access, vol. 6, pp. 9114-9128, 2018.

[23]. J. Weng, R. H. Deng, X. Ding, C. K. Chu, and J. Lai, “Conditional proxy reencryption secure against chosen-ciphertext attack,” in Proc. of 4th International Symposium on Information, Computer, and Communications Security (ASIACCS ‘09), pp. 322-332, 2009.

[24]. P. Xu, T. Jiao, Q.Wu,W.Wang, and H. Jin, “Conditional identity based broadcast proxy re-encryption and its application to cloud email,” IEEE Trans. on Computers, vol. 65, no. 1, pp. 66-79, 2016.

[25]. S. Jiang, T. Jiang, and L. Wang, “Secure and efficient cloud data deduplication with ownership management,”, IEEE Transactions on Services Computing, https://ieeexplore.ieee.org

JETIR