IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 1, January 2020

A Survey on Secure Data Group Sharing and Distribution with Multi-Owner using Multicloud Storage Services

Ms. Judith Peters[1], Prof. M.E. Sanap[2]

Computer Department, STES'S SAE, Kondhwa, Pune, India[1]

Assistant Professor, Computer Department, STES'S SAE, Kondhwa, Pune, India[2]

Abstract: A secure knowledge cluster sharing and conditional dissemination theme with multi-owner in cloud computing, within which data owner will share non-public information with a group of users via the cloud in an exceedingly secure manner, and knowledge communicator will publicize the info 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 ciphertext, within which the info co-owners will append new access policies to the ciphertext 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 knowledge. 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 blocks and upload each block to different cloud providers.

Keywords: Data Sharing, Conditional Proxy Re-Encryption, Attribute-Based Encryption, Privacy Conflict, System Attackability, Remote Synchronization, Distribution and Optimization

I. INTRODUCTION

The popularity of cloud computing is obtained from the benefits of rich storage resources and instant access. It aggregates the resources of computing infrastructure, and then provides on-demand services 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, cellphones 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 multicloud 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.

CSPs such as Dropbox, among many others, employ rsync-like protocols [7] to synchronize the local file to remote file in their centralized clouds [8]. Every local file is partitioned into small chunks and these chunks are hashed with fingerprinting algorithms such as SHA-1, MD5. Thus, a file's contents can be uniquely identified by this list of hashes. For each update of local file, only chunks with changed hashes will be uploaded to the cloud. In order to protect the privacy of users, most cloud services achieve access control by maintaining Access Control List (ACL). In this way, users can choose to either publish their data to anyone or grant access rights merely to their approved people. However, the security risks have raised concerns in people, due to the data is stored in plaintext form by the CSP. Once the data is posted to the CSP, it is out of the data owner's control.

II. RELATED WORK

They made [1], a framework for Ciphertext-Policy Attribute Based Encryption. Our framework takes into consideration another sort of encoded get to control where client's private keys are specified by a lot of qualities and a gathering scrambling information can determine a strategy 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 in which an assailant may acquire numerous private keys. At long last, we gave a usage of our framework, which incorporated a few 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 ciphertexts and private keys. One intriguing open issue would be to build an IBBE framework with consistent size ciphertexts 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 us to mary 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. DATA SHARING

Data sharing in the cloud is a technique that permits users to handily access knowledge over the cloud. The information owner outsources their data in the cloud due to price reduction and the nice conveniences provided by cloud services.

IV. CONDITIONAL PROXY RE-ENCRYPTION

In a Proxy Re-Encryption (PRE) system [4], a proxy, licensed by Alice, will convert a ciphertext for Alice into a ciphertext for Bob while not seeing the underlying plaintext. Conditional proxy re-encryption (C-PRE), whereby solely ciphertext satisfying a selected condition set by Alice is reworked by the proxy and so decrypted by Bob.

V. INFORMATION LEAKAGE

Information leakage could be a class of package vulnerabilities within which info is accidentally disclosed to end-users, probably aiding attackers in their efforts to breach application security. The key criteria for info escape are that the exposure is unintentional and helpful to attackers.

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.

ACKNOWLEDGEMENT

I profoundly grateful to **Prof. M.E. Sanap** for his/her expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. I would like to express my deepest appreciation towards Principal **Dr K.P. Patil**, HOD, **Prof. M.E. Sanap** department of computer engineering and PG coordinator, **Prof.S Shelke**. I must express my sincere heartfelt gratitude to all staff members of computer engineering department who helped me directly or indirectly during this course of work. Finally, I would like to thank my family and friends, for their precious support.

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
[26]. P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: a provably secure scheme under keyword guessing attack," IEEE Transactions on Computers, vol. 62, no. 11, pp. 2266-2277, 2013