IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105129

A REVIEW ON SECURE DATA GROUP SHARING AND DISTRIBUTION WITH MULTI-OWNER USING MULTICLOUDSTORAGE SERVICES

Ms. Gayatri Patil[1], Prof. Mr. Rahul Gaikwad[2]

Computer Department, Godavari collage of Enginneering, India[1,2]

Abstract:A secure data cluster sharing and conditional dissemination theme with multi-owner in cloud computing, within that knowledge owner can share private data with a gaggle of users via the cloud in associate extremely secure manner, and data person can publicize the information to a different cluster of users if the attributes satisfy the access policies at intervals the ciphertext. we've got an inclination to further gift a multiparty access management mechanism over the disseminated cipher text, at intervals that the information co-owners can append new access policies to the ciphertext because of their privacy preferences. Moreover, three policy aggregation ways in which, in conjunction with full allow, owner priority and majority allow, are provided to unravel the privacy conflicts draw back caused by fully completely different access policies. several schemes area unit recently advanced for storing data on multiple clouds. Distributing knowledge over fully completely different cloud storage suppliers (CSPs) automatically provides users with a precise degree of information run management, for no single purpose of attack can leak all the data. However, unplanned distribution {of data |of knowledge |of data} chunks can cause high information revealing even whereas exploitation multiple clouds. associate economical storage arrange generation algorithmic program supported cluster for distributing information chunks with least knowledge escape across multiple clouds. thus to supply additional security to user's knowledge we'll divide our knowledge into blocks and transfer every block to completely different cloud suppliers.

Keywords: Data Sharing, Conditional Proxy re-encryption, Attribute-based encryptionn, Privacy Conflict, System Attackability, Remote Synchronization, Distribution and Optimization

I. INTRODUCTION

The popularity of cloud computing is obtained from the advantages of made storage resources and instant access. It aggregates the resources of computing infrastructure, and so provides on-demand services over the net. several famed firms square measure currently providing public cloud services, like Amazon, Google, and Alibaba. These services enable individual users and enterprise users to transfer knowledge (e.g. photos, videos and documents) to cloud service supplier (CSP), for the aim of accessing the info at any time anyplace and sharing the info with others. With the a lot of and a lot of quick uptake of devices like laptops, cellphones and tablets, users want associate gift and big network storage to handle their ever-growing digital lives. to satisfy these demands, many cloud-based storage and file sharing services like Dropbox, Google Drive and Amazon S3, have gained quality attributable to the easy-to-use interface and low storage worth. However, these centralized cloud storage services square measure criticized for grabbing the management of users' information that allows storage suppliers to run analytics for promoting and advertising [1]. One potential resolution to cut back the possibility of information leak is to use multicloud storage systems [2], [3], [4], [5] during which no single purpose of attack can leak all the info. A malicious entity, just like the one disclosed in recent attacks on privacy [6], would be required to oblige all the assorted CSPs on it a user may place her information, thus on induce a whole image of her information. Put simply, because the locution goes, don't place all the eggs in one basket.

CSPs like Dropbox, among several others, use rsync-like protocols [7] to synchronize the native file to remote get into their centralized clouds [8]. each native file is divided into tiny chunks and these chunks square measure hashed with procedure algorithms like SHA-1, MD5. Thus, a file's contents is unambiguously known by this list of hashes. for every update of native file, solely chunks with modified hashes are going to be uploaded to the cloud. so as to shield the privacy of users, most cloud services deliver the goods access management by maintaining access management list (ACL). during this manner, users will opt to either publish their knowledge to anyone or grant access rights just to their

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105129

approved folks. However, the protection risks have raised issues in folks, thanks to the info is keep in plaintext type by the CSP. Once the info is announce to the CSP, it's out of the info owner's management.

II. RELATED WORK

They created [1], a framework for Ciphertext-Policy Attribute primarily based cryptography. Our framework takes into thought another type of encoded get to manage wherever client's non-public keys square measure specific by a great deal of qualities and a gathering scrambling info will verify a method over these qualities indicating that purchasers will decrypt. Our framework permits ways to be communicated as associate degreey monotonic tree get to structure and is mothproof to intrigue assaults during which an aggressor might acquire varied non-public keys. At long last, we tend to gave a usage of our framework, that incorporated a number of sweetening ways.

Intermediary primarily based, [2] varied cloud capability framework that for all intents and functions tends to the unwavering quality of the current cloud reinforcement warehousing. NCCloud not simply offers adaptation to internal failure away, however additionally permits sensible fix once a cloud for all time falls flat. NCCloud executes a viable adaptation of the FMSR codes, that recovers new equality items throughout fix subject to the required level of knowledge excess. Our FMSR code usage dispenses with the coding necessity of capability hubs (or cloud) throughout fix, whereas guaranteeing that the new arrangement of place away lumps when every spherical of fix jam the required adaptation to non-critical failure. Our NCCloud model shows the viability of FMSR codes within the cloud reinforcement use, as way as cash connected expenses and reaction times.

The Internet of Things (IoT) [3], gadgets frequently produce info, and need the knowledge examination to be quick, that cannot be given by the standard distributed computing style. With the target of breaking down the IoT info close to the gadgets that make and work on the knowledge, edge reckoning has been acquainted with for the growth with the sting of the system from distributed computing. Despite the actual fact that edge registering encourages distributed computing in tending to the immobility issue of knowledge handling, it likewise brings larger security and protection problems to this distributed system. as a result of the fact that property primarily based cryptography (ABE) underpins fine-grained (or versatile) get to manage for info things in disorganised structures, ABE has been usually accepted to be an ideal account guarantee info security and protection for things of distributed computing. To accomplish fine-grained get to manage for the sting reckoning condition, during this paper, we tend to planned an inspiration named mediator supported ciphertext-approach characteristic primarily based cryptography (PA- CPABE). behind depicting a standard development of PA-CPABE, we tend to formally examined its security. what is additional, we tend to displayed and actualised a launch of PA-CPABE to assess its proficiency.

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

We conferred [5], the principal temperament primarily based communicate cryptography (IBBE) conspire with steady size ciphertexts and personal keys. One intriguing open issue would be to make associate degree IBBE framework with consistent size ciphertexts and personal keys that's secure beneath a increasingly customary supposition, or that accomplishes a additional grounded security plan, the image of full security in IBE plans.

To address the info protection [6], drawback in cloud computing, we tend to propose and implement a role-based self-contained information protection theme referred to as RBAC-CPABE. supported the classic RBAC model, we tend to initial propose a data-centric access management model, DC-RBAC, that permits {the information|theinfo|the information} owner to specify personalized RBAC policies for every data object. Besides role-level constraints, DC-RBAC additionally contains user attribute constraints and surroundings constraints, that correspond to info regarding the approved users and discourse info regarding the surroundings, severally. Hence, DC-RBAC achieves additional versatile and fine-grained access management. Next, to construct the self-contained information protection mechanism,

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105129

we tend to fuse the DC-RBAC into ECP-ABE by extending ECP-ABE and process a policy mapping model. By victimisation RBAC-CPABE, info contained within the information itself determines whether or not users square measure approved to perform coding rather than wishing on different parties.

In this paper [7], we tend to propose a protected client facet deduplication plot KeyD to with success administer focalized keys. data deduplication in our structure is accomplished by co-operations between data proprietors and also the Cloud Service supplier (CSP), while not support of alternative confided in outsiders or Key. The board Cloud Service suppliers. the safety examination shows that our KeyD guarantees the secrecy of knowledge what is more, security of joined keys, and well ensures the shopper possession protection at the same time. alpha outcomes exhibit that the safety of our arrange is not at the price of the exhibition. For our future work, we'll conceive to explore for approaches to confirm the temperament security of knowledge proprietors, that is not thought-about in our arrange.

From Associate in Nursing denizen perspective [8] , the cloud security model does not nonetheless hold against risk models made for the North American country to Madonna model wherever the hosts square measure worked and utilised by an identical association. however, there's a standardized advancement towards invigorating the IaaS security model. during this work we tend to displayed a system for confided in foundation cloud arrangement, with 2 center focuses: VM organization on trustworthy register hosts and house primarily based insurance of put away data. we tend to portrayed well the structure, usage furthermore; security assessment of conventions for trustworthy VM dispatch and house primarily based reposition assurance. The arrangements depend upon requirements elicited by Associate in Nursing open human services authority, are actualised during a far-famed ASCII text file IaaS stage and tried on a model causation of a circulated EHR framework. within the security investigation, we tend to given a progression of assaults and incontestible that the conventions hold within the predefined risk model. to amass more certainty within the linguistics security properties of the conventions, we've incontestible and checked them with ProVerif [32]. At long last, our execution tests have indicated that the conventions gift Associate in Nursing inconsequential presentation overhead.

III. DATA SHARING

Data sharing within the cloud may be a technique that allows users to handily access data over the cloud. Information owner outsources their data within the cloud thanks to step-down and therefore the nice conveniences provided by cloud services.

IV. CONDITIONAL PROXY RE-ENCRYPTION

In a proxy re-encryption (PRE) system [4], a proxy, licenced by Alice, can convert a ciphertext for Alice into a ciphertext for Bob whereas not seeing the underlying plaintext. Conditional proxy re-encryption (C-PRE), whereby exclusively ciphertext satisfying a particular condition set by Alice is reworked by the proxy then decrypted by Bob.

V. INFORMATION LEAKAGE

Information outpouring can be a category of package vulnerabilities inside that data is accidentally disclosed to end-users, most likely aiding attackers in their efforts to breach application security. The key criteria for information escape is that the exposure is unintentional and useful to attackers.

VI. CONCLUSION AND FUTURE WORK

Distributing information on multiple clouds provides users with an exact degree {of data |of information | of knowledge } run management there in no single cloud provider area unit tuned in to the whole user's knowledge. However, unplanned distribution {of information | of data | of knowledge} chunks can cause avertable information run. the information security and privacy may be a concern for users in cloud computing. above all, the way to enforce privacy issues of multiple house owners and defend the information confidentiality becomes a challenge. Here, we have a tendency to area unit providing data leak aware storage system Associate in Nursingd confidentiality of the information in an multi cloud surroundings.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105129

ACKNOWLEDGEMENT

I profoundly grateful to Prof. Mr. Rahul Gaikwad for his 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 Dr. Vijay H. Patil (Principal), Mr. Promod B. Gosavi (HOD), Prof. Rahul Gaikwad department of computer engineering and PG coordinator. 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.