International Journal of Information Processing, 10(2), 51-61, 2016
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Secure Multi-Keyword Search and Multi-User Access Control over an Encrypted Cloud Data

Raghavendra S[a], Doddabasappa P A[a], Geeta C M[a], Rajkumar Buyya[b], Venugopal K R[a], S S Iyengar[c], L M Patnaik[d]

[a]Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore-560001, Contact: raghush86@gmail.com

[b]The University of Melbourne, Australia

[c]Florida International University, USA

[d]INSA, National Institute of Advanced Studies, Indian Institute of Science Campus, Bangalore, India

Cloud computing provides economical and effective solution for sharing data among cloud users with low maintenance cost. The security of data and identity confidentiality while sharing data in multi-owner way cannot be assured by the Cloud Service Providers (CSP's). The Cloud Service Providers are reliable but curious to know the recurrent membership changes in the cloud. In this paper, we propose a secure multi-owner data sharing for dynamic group in the cloud with RSA Chinese Remainder Theorem(RSA-CRT) encryption technique and substring index generation method. RSA-CRT efficiently manages revocation list, key management, with reduced storage and computational overhead. The substring Index generation algorithm reduces the storage space and Search algorithm is reduces the time to search files from the cloud compared to wild card fuzzy alogorithm [1].

1. INTRODUCTION

Cloud computing is the service which is provided over the Internet. It is used to share resource at low maintenance cost, as service is completely managed by the cloud service vendor. The service is provided on demand and charged as much as the user uses the service. This service is fully managed by the cloud service provider and thus reduce the maintenance complexity, data loss problem as well as reduces capital investment for purchasing hardware and software. This uses a large group of servers which is running at low cost PC technology and provides specialized data processing. Cloud computing is a customer-oriented application in financial portfolios which delivers personalized information to provide data storage and sharing among the members of an organization. It provides a scalable and reliable database which is maintained by the provider. They provide various services such as Communication-as-a-Service (CaaS), Infrastructure-as-a-Service S(IaaS), Platform-as-a-Sevice (PaaS), Monitoring-as-a-Service (MaaS) and Software-as-a-Service (SaaS).

In cloud computing, security is provided to the data in cloud by encrypting and uploading file. The data owner gives access to the users by disseminating the decryption key to the authorized users to decrypt the files [2,3]. The early encryption methods includes dynamic broadcast encryption [4] in which the users can be added dynamically and the communicator or broadcaster broadcast the decryption key to the authorized users who in turn can access the files. In this technique, storage overhead increases with the increase in the number of users as well as revoked users.

Due to this drawback many encryption techniques were developed [5–7]. Riedel *et al.,* pro-

There is no need to re-generate the key when the users join or leave thus providing easy and flexible way of access control without much key management, and in addition to maintain forward and backward secrecy.

7. CONCLUSIONS

In this paper, the concept of Master key generation is used to encrypt and store the contents in the cloud. An efficient index building algorithm is designed for fast and cost efficient file retrieval from the cloud. The Master key generation algorithm where only the master-key is updated with every revocation or membership change, keeping the existing group members private and public keys unaltered. This approach reduces the storage space of the index file and key size. Further this protocol can be enhanced to other form of text and multimedia files. The faster index building algorithm can be explored to retreival files efficiently.

REFERENCES

1. Neelam S Khan, C Rama Krishna, and Anu Khurana. Secure Ranked Fuzzy Multi-Keyword Search over Outsourced Encrypted Cloud Data, *In proceedings of the 2014 International Conference on Computer and Communication Technology (ICCCT)*, pages 241–249, 2014.
2. Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, and MMA Hashem. A Newer User Authentication, File Encryption and Distributed Server Based Cloud Computing Security Architecture, *arXiv preprint arXiv:1303.0598*, 2013.
3. Cong Wang, Kui Ren, and Jia Wang. Secure and Practical Outsourcing of Linear Programming in Cloud Computing. *In Proceedings of the IEEE INFOCOM*, pages 820–828, 2011.
4. Min-Ho Park, Young-Hoon Park, Han-You Jeong, and Seung-Woo Seo. Secure Multiple Multicast Services in Wireless Networks. *IEEE Transactions on Mobile Computing*, 2012.
5. Mahesh Kallahalla Erik Riedel, Ram Swaminathan Qian Wang, and Kevin Fu. Plutus: Scalable Secure File Sharing on Untrusted Storage.
6. Zhiguo Wan, June Liu, and Robert H Deng.HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. *In IEEE Transactions on Information Forensics and Security,* 7(2):743–754, 2012.
7. Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. *In ACM Transactions on Information and System Security (TISSEC)*, 9(1):1–30, 2006.
8. Li Zhou and Mostafa H Ammar. A File-centric Model for Peer-to-peer File Sharing Systems. *In Proceedings of the 11th IEEE International Conference on Network Protocols,* pages 28–37. IEEE, 2003.
9. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan. Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud. *In IEEE Transactions on Parallel and Distributed Systems,* 24(6):1182–1191, 2013.
10. Hung-Min Sun and Mu-En Wu. An Approach Towards Rebalanced RSA-CRT with Short Public Exponent. *IACR Cryptology ePrint Archive,* 2005:53, 2005.
11. B Wang, Baochun Li, and H Li. Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud. 2014.
12. Bernhard Amann and Thomas Fuhrmann. Cryptographically Enforced Permissions for Fully Decentralized File Systems. *In Proceedings of the 2010 IEEE Tenth International Conference on Peer-to-Peer Computing (P2P),* pages 1–10, IEEE, 2010.
13. S Raghavendra, C M Geeta, K Shaila, Rajkumar Buyya, K R Venugopal, S S Iyengar, and L M Patnaik. MSSS: Most Significant Single-keyword Search over Encrypted Cloud Data. *In Proceedings of the 6th Annual Intrernational Conference on ICT: BigData, Cloud and Security*, 2015.
14. S Raghavendra, C M Geeta, Rajkumar Buyya, K R Venugopal, S S Iyengar and L M Patnaik. DRSIG: Domain and Range Specific Index Generation for Encrypted Cloud Data", *In Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016.* IEEE, March 2016.
15. S Raghavendra, C M Geeta, Rajkumar Buyya, K R Venugopal, S S Iyengar and L M Patnaik. MSIGT: Most Significant Index Generation Technique for Cloud Environment. *In Proceedings of the 12th IEEE India International Con-*

ference on E3 -C3 (INDICON 2015). IEEE, December 2015.
16. S Raghavendra, S Girish, C M Geeta, Rajkumar Buyya, K R Venugopal, S S Iyengar and L M Patnaik. IGSK: Index Generation on Split Keyword for Search over Cloud Data. *In Proceedings of the 2015 International Conference on Computing and Network Communications (CoCoNet15)*, pages 380–386, December 2015.
17. He Tuo and Ma Wenping. An Effective Fuzzy Keyword Search Scheme in Cloud Computing. *In proceedings of the 2013 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, pages 786–789, IEEE, 2013.
18. National Science Foundation Research Awards Abstracts 1990-2003. *http://kdd.ics.uci.edu/databases/nsfabs/nsfawards.html*, 2013.

Raghavendra S is a research scholar in the department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. He received his Bachelor degree in Computer Science and Engineering from BMS Institute of Technology, Visvesvaraya Technological University, Bangalore, India and Master degree from R V College of Engineering, Visvesvaraya Technological University, Bangalore, India. His research interests include Cloud Computing, applied cryptography and network security. He is a student member of the IEEE

Doddabasappa P A is a student of Computer Science and Engineering department, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. he has received B.E.degree in Computer Science and Engineering, from Visvesvaraya Technological University, Belgaum, Karnataka, India. His areas of interest are cloud computing and Big Data.

Geeta C M is a research scholar in the department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. she has received B.E.degree in Electronics and Communication and M.E degree in Information Technology, from Bangalore University, Bangalore, Karnataka, India. Her areas of interest are cloud computing and wireless sensor networks.

Rajkumar Buyya is Professor of Computer Science and Software Engineering, Future Fellow of the Australian Research Council, and Director of the Cloud Computing and Distributed Systems (CLOUDS) Laboratory at the University of Melbourne, Australia. He has authored over 500 publications and four text books including Mastering Cloud Computing published by McGraw Hill and Elsevier/Morgan Kaufmann, 2013 for Indian and international markets respectively. He is one of the highly cited authors in computer science and software engineering worldwide (h-index=100, g-index =192, 47412+ citations). Microsoft Academic Search Index ranked Dr. Buyya as the worlds top author in distributed and parallel computing between 2007 and 2012. He is serving as foundation Chair of the IEEE Technical Committee on Scalable Computing and five IEEE/ACM conferences. He has received award of 2009 IEEE Medal for Excellence in Scalable Computing from the IEEE Computer Society, USA. Manjrasofts Aneka Cloud technology developed under his leadership has received 2010 Asia Pacific Frost and Sullivan New Product Innovation Award and 2011 Telstra Innovation Challenge, Peoples Choice Award. He is a Fellow of IEEE.

Venugopal K R is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D in Economics from Bangalore University and Ph.D in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 57 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems *etc.*, He has filed 101 patents. During his three decades of service at UVCE he has over 550 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining. He is a Fellow of IEEE.

S S Iyenger is currently Ryder Professor, Florida International University, USA. He was Roy Paul Daniels Professor and chairman of the Computer Science Department of Louisiana state University. He heads the Wireless Sensor Networks Laboratory and the Robotics Research Laboratory at USA. He has been involved with research in High Performance Algorithms, Data Structures, Sensor Fusion and Intelligent Systems, since receiving hid Ph.D degree in 1974 from MSU, USA. He is Fellow of IEEE and ACM. He has directed over 40 Ph.D students and 100 post graduate students, many of whom are faculty of Major Universities worldwide or Scientists or Engineers at National Labls/Industries around the world. He has published more than 500 research papers and has authored/co-authored 6 books and edited 7 books. His books are published by John Wiley and Sons, CRC Press, Prentice Hall, Springer Verlang, IEEE Computer Society Press etc.. One of his books titled Introduction to Parallel Algorithms has been transalted to chinese.

L M Patnaik is currently Honorary Professor, Indian Institute of Science, Bangalore, India. He was a Vice Chancellor, Defense Institute of Advanced Technology, Pune, India and was a Professor since 1986 with the Department of CSA, Indian Institute of Science, Bangalore. During the past 35 years of his service at the Institute he has over 700 research publications in refereed International Journals and refereed International Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to High Performance Computing and Soft Computing. His areas of research interest have been Parallel and Distributed Computing, Mobile Computing, CAD, Soft Computing and Computational Neuroscience.