



Efficient Verification of Trustiness and Authentication of Query Answers in Cloud

¹Ch. Mamatha Devi ²V. Aditya Ramalingeswar Rao

¹ Final Master of Science in Computer Science, Ideal college of Arts and Sciences, Vidyut Nagar, Kakinada, East Godavari, AP, India

² Assistant Professor, Department of Computer Science, Ideal college of Arts and Sciences, Vidyut Nagar, Kakinada, East Godavari, AP, India

ABSTRACT:

This recommends a cooperative query answer authentication system, based on the ring signature, the Merkle hash tree (MHT) and the non-repudiable service protocol. Through the cooperation among the entities in cloud service system, the proposed scheme could not only verify the query answer but also protect the DO's identity. First, it picks up the internal nodes of MHT to sign, as well as the root node. Thus, the verification computation complexity could be significantly reduced from $O(\log 2N)$ to $O(\log 2N^{0.5})$ in the best case. Then it improves an existing ring signature to sign the selected nodes. Furthermore, the proposed scheme employs the non-repudiation protocol during the transmission of query answer and verification object (VO) to protect trading behavior between the CSP and users. The security and performance analysis prove the security and feasibility of the proposed scheme.

KEYWORDS: Cloud service provider, encryption, signature scheme

1 INTRODUCTION:

With the advances of remote sensor systems and Internet of things, swarm detecting huge information is gathered by scrambling sensors over a huge field. As time passes by, the quickly developing information volumes make it difficult for the sensors to store because of their feeble stockpiling and registering assets. It turns into an issue that how to store these group detecting information financially, and additionally perform questions on it efficiently. Considering the flexible, on-request and minimal effort utilization of distributed storage assets [1], [2], [3], the undertakings and people, i.e., information proprietors (DO), outsource their information to the cloud server. Along these lines, the clients can get the data of enthusiasm by asking the cloud specialist co-op (CSP) for looking through the outsourced information [3], [4], [5], [6]. Watching

the administration display there are three substances in the framework: DO, client, and CSP. The group detecting information is given by numerous information proprietors. More clients and CSP would participate in the framework for using these information. Because of the cooperative task among DO, client and CSP, different security and protection issues must be mulled over.

2 LITERATURE SURVEY:

2.1 we additionally improve the security of ID-based ring mark by giving forward security: If a mystery key of any client has been traded off, all past created marks that incorporate this client still stay substantial. This property is particularly vital to any expansive scale information sharing framework, as it is difficult to ask all information proprietors to reauthenticate their information regardless of whether a mystery key of one single client has been traded off. We give a solid and proficient instantiation of our plan, demonstrate its security and give an execution to demonstrate its common sense.

2.2 we proposed a differential assault on one-to-numerous OPE by abusing the distinctions of the requested ciphertexts. The exploratory outcomes demonstrate that the cloud server can get a decent gauge of the dissemination of significance scores by a differential assault. Moreover, while having some foundation data on the outsourced archives, the cloud server can precisely induce the encoded catchphrases utilizing the evaluated conveyances.

3 PROBLEM DEFINITION:

The Existing framework contains Cloud Service Providers are conniving however they are the person who shares gives the information to client who acquire the information on request. In Existing System, information contains the information proprietor signature. This may prompt uncover Data Owners personality with the goal that they it might release the data about information proprietor. The security on information amongst client and CSP are exceedingly troublesome. Since CSP are conniving there might be shot of happening

effectively, yet additionally fulfil DO's prerequisite for secrecy and assurance non-disavowal benefit amongst CSP and client. Right off the bat, the proposed conspire picks and signs the KN in the MHT in light of the ring mark plot, which can both confirm the right of question result when keeping DO unknown, and backings numerous DOs. Also, we present a non-disavowal convention in light of VO to unravel the repudiable practices of CSP and client.

10 REFERENCES:

- [1] D. Kwak, R. Liu, D. Kim, B. Nath, and L. Iftode, "Seeing is believing: Sharing real-time visual traffic information via vehicular clouds," *IEEE Access*, vol. 4, pp. 3617–3631, 2016.
- [2] Q. Yang, B. Zhu, and S. Wu, "An architecture of cloud-assisted information dissemination in vehicular networks," *IEEE Access*, vol. 4, pp. 2764–2770, 2016.
- [3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on parallel and distributed systems*, vol. 25, no. 1, pp. 222–233, 2014.
- [4] W. Zhang, Y. Lin, S. Xiao, J. Wu, and S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1566–1577, 2016.
- [5] S. Tian, Y. Cai, and Z. Hu, "A parity-based data outsourcing model for query authentication and correction," in *IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2016, pp. 395–404.
- [6] J. Li, A. Squicciarini, D. Lin, S. Sundareswaran, and C. Jia, "Mmbcloud-tree: Authenticated index for verifiable cloud service selection," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–14, 2015.
- [7] H. Pang and K.-L. Tan, "Query answer authentication," *Synthesis Lectures on Data Management*, vol. 4, no. 2, pp. 1–103, 2012.
- [8] F. Li, K. Yi, M. Hadjieleftheriou, and G. Kollios, "Proof-infused streams: Enabling authentication of sliding window queries on streams," in *Proceedings of the 33rd international conference on Very large data bases. VLDB Endowment*, 2007, pp. 147–158.
- [9] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Linkable ring signature with unconditional anonymity," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 1, pp. 157–165, 2014.
- [10] R. C. Merkle, "A certified digital signature," in *Conference on the Theory and Application of Cryptology*. Springer, 1989, pp. 218–238.
- [11] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*. ACM, 2006, pp. 121–132.
- [12] —, "Authenticated index structures for aggregation queries," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 4, p. 32, 2010.
- [13] F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera, "Range query integrity in cloud data streams with efficient insertion," in *International Conference on Cryptology and Network Security*. Springer, 2016, pp. 719–724.
- [14] Q. Chen, H. Hu, and J. Xu, "Authenticated online data integration services," in *Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data*. ACM, 2015, pp. 167–181.
- [15] Vyas, A. Singh, J. Singh, G. Soni, and B. Purushothama, "Design of an efficient verification scheme for correctness of outsourced computations in cloud computing," in *International Symposium on Security in Computing and Communication*. Springer, 2015, pp. 66–77.



Ch. Mamatha Devi is a student of Ideal College of Arts and Sciences Kakinada. Presently she is in Final Master of Science in Computer Science this college and affiliated to Adikavi Nannaya University, Rajamahendravaram, Andhra Pradesh. Her area of interest includes Web Designing and Computer Networks, all current trends and techniques in Computer Science.



Mr. V. ADITYA RAMALINGESWAR RAO Presently working as an Assistant Professor in P.G. Department of Computer Sciences in Ideal college of Arts and Sciences (P.G. Courses) Kakinada. He obtained M.Sc. (Computer Science) from Andhra University Visakhapatnam. And he did M.Tech (Computer Science and Engineering) from Acharya Nagarjuna University Guntur. He has lecturer ship in Computer Science and Applications and have an Experience of 15 years of teaching.