The Efficiency of Data Sharing in a Cloud by Security Analysis Using Mona

[1]Gunde Priyanka, [2]Sayeed Yasin
[1]Dept. of CSE, NIMRA Institute of Science & Technology, Vijayawada, AP, India
[2]NIMRA Institute of Science & Technology, Vijayawada, AP, India

Abstract
The cloud serversmanaged by cloud providers are not completely trusted by userswhile the data files stored in the cloud may be responsive andconfidential such as business plans. To preserve data privacy a basic solution is to encrypt data files and thenupload the encrypted data into the cloud. Regrettablyconnivingacapable and secure data sharing scheme forgroups in the cloud is not an effortless task due to the followingchallenging issues. Sharing data in a multi owner manner while preserving data and characteristics privacy from anuntrusted cloud is often a challenging issue due to the frequent change of the membership. In this paper we propose a secure multiowner data sharing scheme named Mona for dynamic groups in the cloud.We look at the problem in the context of a network augmentedwith storage nodes and target at range query a very general andpowerful type of query.

Keywords
Cloud Computing, Data Sharing, Privacy-Preserving, Access Control, Dynamic Groups

I. Introdcution

To store data on the sensornodes is excessive due to the limited storage space on each sensor node and the obscurity in collecting all the data to acentral repository. Conveying all the data to the base station on the other hand has to address the limited transmissionrate that is mainly throttled by the funnel effect around thebase station and attenuated per node transmission bandwidth.The foreword of the storage nodes helps to assuage thetransmission bandwidth dilemma by distributing the local datatransmission to the storage node. As users no longer actually possess the storage oftheir data traditional cryptographic primitives for thereason of data security protection cannot be straightadopted. It is ofteninadequate to detect the data corruption only whenaccessing the data as it does not give users rightnessassurance for those unaccessed data and might be too late to recover the data loss or damage. Allowing forthe large size of the outsourced data and the user'sconstrained resource capability the tasks of auditingthe data correctness in a cloud environment can befrightening and high-priced for the cloud users.

II. Related Work

We can scrutinize that how tostrongly share data files in a multiple-owner manner fordynamic groups while preserving identity privacy from anuntrusted cloud remains to be a challenging issue. In thispaper we propose a novel Mona protocol for secure datasharing in cloud computing. Lu et al. proposed a secure provenance schemewhich is put together upon group signatures and ciphertext-policyattribute-based encryption techniques. Predominantly thesystem in their format is set with a single attribute. Eachuser attainedtwo keys after the registration a groupsignature key and an attribute key. Yu et al. presented a scalable and fine-grained dataaccess control scheme in cloud computing based on the KPABEtechnique. The data owner uses a random key toencrypt a file where the arbitrary key is additional encryptedwith a set of attributes using KP-ABE.

III. Literature Survey

The fact that users no longer have physical possession of the outsourced data makes the data honesty protection inCloud Computing a formidable taskparticularly for users with inhibited computing resources. Furthermore users ought to be ableto just use the cloud storage as if it is local without worrying about the need to confirm its integrity. Thus enabling public audit ability for cloud storage is of decisive importance so that users can resort to a third party auditor (TPA) to ensure the integrity of outsourceddata and be worry-free. To steadily introduce an effective TPA the auditing process should bring in no new vulnerabilities towardsuser data privacy and commence no additional online burden to user. In this paper we propose a secure cloud storage systemsupporting privacy-preserving public auditing. We further extend our result to enable the TPA to act upon audits for multiple usersconcurrently and capably.

We regard as a sensor network that is not fullytrusted and ask the question how we preserve privacy for thecollected data and how we authenticate the data reply from the network.We discover the problem in the context of a network enlargedwith storage nodes and target at range query a very general andpowerful type of query. We use bucketization to mix the data fora range, use message encryption for data integrity and occupyencoding numbers to prevent the storage nodes from droppingdata.

By leveraging group signature and dynamic broadcastencryption techniques any cloud user can namelessly share data with others. Meanwhile the storage overhead and encryptioncomputation cost of our scheme are self-determining with the number of revoked users. In addition we analyze the security of our schemewith exact proofs and make obvious the efficiency of our scheme in experiments. With the character of low down maintenance cloud computing provides an economical and competent solution for sharing groupresource among cloud users.

IV. Existing System

Data owners stock up the encrypted data files in untrusted storage and deal out the corresponding decryption keys only to authorized users. Thus unauthorized users as well as storage servers cannot learn the content of the data files since they have no knowledge of the decryption keys. However the difficulties of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users respectively. By setting a group with a single attribute. Unfortunately the single owner manner hinders the acceptance of their scheme into the case where any user is granted to store and share data.

V. Disadvantages

Without the security of identity privacy users may be unwilling to join in cloud computing systems because their real identities could be with no trouble disclosed to cloud providers and attackers. Unconditionalindividuality privacy may acquire the abuse of privacy. The modifications of membership make secure data sharing particularly difficult.

VI. Proposed System

Wesuggest a secure multiowner data sharing scheme named Mona for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques any cloud user can namelessly share data with others. Meanwhile the storage overhead and encryption computation cost of our format are autonomous with the number of revoked users. In addition we analyze the security of our scheme with rigorous proofs and exhibit the efficiency of our scheme in experiments.

VII. Advantages

It is a secure multi-owner data sharing scheme. It involves that any user in the group can firmly share data with others by the untrusted cloud.Also able to support dynamic groups professionally. It declares any member in a group to anonymously utilize the cloud resource and achieveall-embracing simulations to make obvious the efficiency of our scheme in terms of storage and computation overhead.

VIII. System Architecture

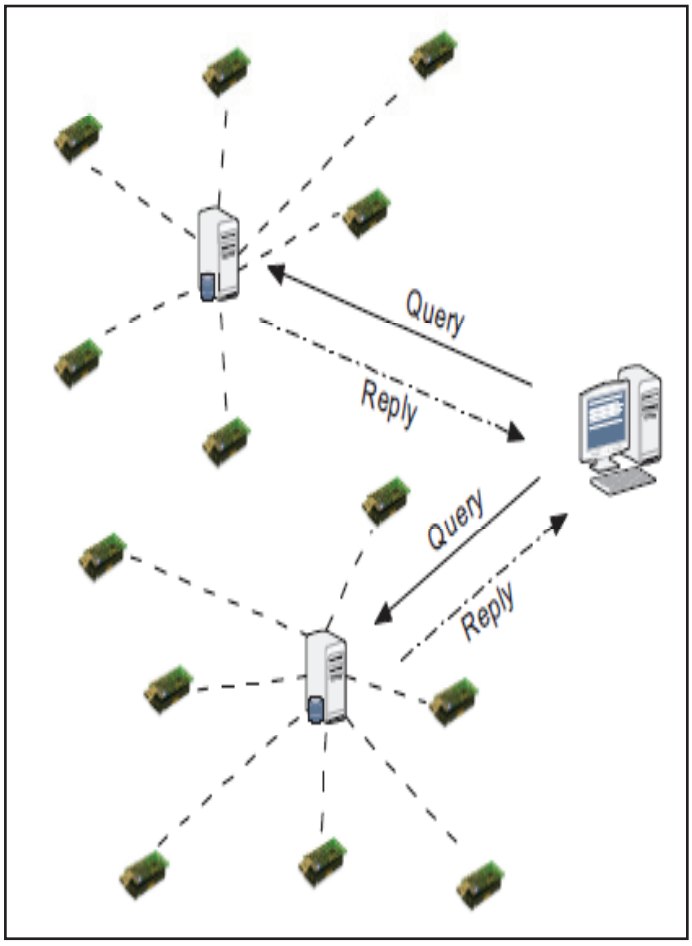

Fig. 1:

Data query froma user is absorbed to the storage nodes through the sink. Thispaper believes range query and users are endorsed to queryhistoric data. Thus in a query users identify the data valuerange [a, b] and the time slot they are interested in. We definean epoch as the smallest time period that a user is able toquery. Presuppose all sensors are harmonized so that they haveconformity on the beginning and end of an epoch. After everyepoch the composed data is sent to the nearby storage nodesby sensors and archived there for future queries.

VIII. Cloud Module

Weform a local Cloud and afford priced abundant storage services. The users can upload their data in the cloud. We develop this module where the cloud storage can be made secure. Nevertheless the cloud is not entirely trusted by users since the CSPs are very probable to be outside of the cloud users' trusted domain. Comparablewe assume that the cloud server is truthful but curious. That is the cloud server will not unkindly delete or modify user data due to the protection of data auditing schemes but will try to find out the content of the stored data and the identities of cloud users.

IX. Group Manager Module

Group manager takes charge of System parameters generation,User registration, User revocation and revealing the real identity of a dispute data owner. For that reason we presuppose that the group manager is completely trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is accountable for user registration and also user revocation too.

X. Group Member Module

Group members are a set of registered users that willhoard their private data into the cloud server and share them with others in the group.make a note of the group membership is dynamically changed due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can vision the files which are uploaded in their group and also change.

XI. File Security Module

File stored in the cloud can be obliterated by either the group manager or the data owner i.e., the member who uploaded the file into the server.

X. Group Signature Module

A group signature methodconsents to any member of the group to sign messages while keeping the identity secret from verifiers. Besides the designated group manager can divulge the identity of the signature's originator when a dispute occurs which is denoted as traceability.

XI. User Revocation Module

User revocation is executed by the group manager via a public available revocation list (RL) based on which group members can encrypt their data files and make sure the secrecy against the revoked users.

Algorithm Used:

for $i = v_{min}$ to v_{max} **do**
  for $j = i$ to v_{max} **do**
    $\bar{E}[i,j] = \bar{E}[i,j-1] + F(j) \cdot j$
    $PT[i,j] = PT[i,j-1] + F(j)$
    variance $= \sum_{x=i}^{j} F(x)(x - \bar{E}[i,j])^2$
    entropy $= -\sum_{x=i}^{j} \frac{F(x)}{PT[i,j]} \log \frac{F(x)}{PT[i,j]}$
    if variance $> VAR_p$ and entropy $> EN_p$ **then**
      $valid[i,j] = true$
      $CF[i,j] = (\sum_{p=i}^{j-1}(p - v_{min} + 1)\sum_{x=p+1}^{j} F(x) + \sum_{p=i+1}^{j}(v_{max} - p + 1)\sum_{x=i}^{p-1} F(x)) \cdot n \cdot s \cdot d_{ss}$
      $CE[i,j] =$ EncodingLength$(PT[i,j]) \cdot c \cdot n(1 - PT[i,j])^s \cdot d_{avg}$
      $COST[i,j] = CE[i,j] + CF[i,j]$
for $w = 1$ to $v_{max} - v_{min} + 1$ **do**
  for $i = 1$ to $v_{max} - w$ **do**
    if $valid[i, i+w]$ **then**
      $M[i, i+w] = COST[i,j]$
    else
      continue
    for $j = 1$ to $w - 1$ **do**
      if $valid[i, i+j]$ **then**
        $cost = COST[i, i+j] + M[i+j+1, i+w]$
        if $cost < M[i, i+w]$ **then**
          $M[i, i+w] = cost$
          $H[i, i+w] = j$
return $M[v_{min}, v_{max}]$

XII. Experimental Results

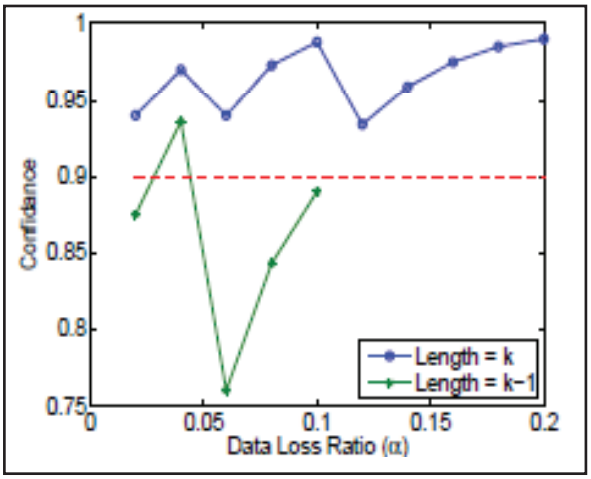

Fig. 2:

We evaluate conf (k) withconf (k−1) and the dashed line is the confidence requirement. As we can observeconf (k) is always greater and in mostcases.k− 1 is not aappropriate length for security protection.We conclude a good instruction ofselecting appropriate encoding lengths. Simulation has shownthat the suggested length value is enough for security andalso efficient in communication.

XIII. Conclusion

Monasupports proficient user revocation and new user joining.More particularlyprofessional user revocation can be accomplishedthrough a public revocation list devoid ofrevising theprivate keys of the remaining users and new users candirectly decrypt files stored in the cloud before theirparticipation.Moreover the storage overhead and theencryption calculation cost are steady. Extensive analysisshows that our proposed proposalconvinces the desiredsecurity requirements and guarantees competence as well. The collected data ina range is encrypted without being recognized by the storagenode but the data is connected with a tag that tells the storagenode which variety it belongs to. In this way storage node mayrespond to the range query without knowing the correct value of thedata. The query answer from the storage nodes will be establishedby examining the attached certificate so that the storage nodeis incapable to forge data for reply. To avoid storage nodefrom dropping data an encoding number is produced on eachsensor if no data in a range is collected on that sensor.

References

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, M.Zaharia,"A View of Cloud Computing", Comm. ACM, Vol. 53, No. 4, pp. 50-58, Apr. 2010.

[2] S. Kamara, K. Lauter,"Cryptographic Cloud Storage", Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, W. Lou,"Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage", Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, D. Boneh, "Sirius: Securing Remote Untrusted Storage", Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green, S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to SecureDistributed Storage", Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.

[7] R. Lu, X. Lin, X. Liang, X. Shen,"Secure Provenance: TheEssential of Bread and Butter of Data Forensics in CloudComputing", Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.

[8] B. Waters,"Ciphertext-Policy Attribute-Based Encryption: AnExpressive, Efficient, and Provably Secure Realization", Proc. Int'lConf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, [Online] Available: http://www.eprint.iacr.org/2008/290.pdf, 2008.

[9] V. Goyal, O. Pandey, A. Sahai, B. Waters,"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[10] D. Naor, M. Naor, J.B. Lotspiech,"Revocation and Tracing Schemes for Stateless Receivers", Proc. Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[11] D. Boneh, M. Franklin,"Identity-Based Encryption from theWeil Pairing", Proc. Int'l Cryptology Conf. Advances in Cryptology(CRYPTO), pp. 213-229, 2001.

[12] D. Boneh, X. Boyen, H. Shacham,"Short Group Signature", Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[13] D. Boneh, X. Boyen, E. Goh,"Hierarchical Identity BasedEncryption with Constant Size Ciphertext", Proc. Ann. Int'l Conf.Theory and Applications of Cryptographic

Techniques (EUROCRYPT), pp. 440-456, 2005.
[14] C. Delerablee, P. Paillier, D. Pointcheval,"Fully CollusionSecure Dynamic Broadcast Encryption with Constant-Size Ciphertextsor Decryption Keys", Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.
[15] D. Chaum, E. van Heyst,"Group Signatures", Proc. Int'l Conf.Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

Gunde Priyanka M.TECH student of Nimra Institute of Science & Technology an affiliated college of JNTU ,Kakinada,India.she has done her B.TECH in lakireddy balireddy college of engineering,mylavaram, vijayawada an affiliated college of JNTU Kakinada, INDIA.

SAYEED YASIN received his MTECH in Computer Science &Engg from JNTU Hyderabad.He is pursuing Ph.D in RayalaseemaUniversity ,Kurnool.He is currently working as Assoc. Professor & HOD in Nimra Institute of Science & Technology the Department of Computers Science and Engineering,Vijayawada.He has more than Eight years of experience in teaching.His area of interests are wireless networks & programming.