Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 02, pp.65431-65434, February, 2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

REVIEW ARTICLE

A REVIEW ON QUERY ANSWER AUTHENTICATION IN CLOUD OVER ANONYMOUS DATA

*Mr. Shashikant S. Nagdive and Dr. Prashant N. Chatur

Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH) India

ARTICLE INFO

Article History:
Received 28th November, 2017
Received in revised form
17th December, 2017
Accepted 19th January, 2018
Published online 28th February, 2018

Key words:
Cooperation,
Query Answer Authentication,
Identity privacy,
Non-Repudiation Protocol.

ABSTRACT

Uploading anonymous data over untrustworthy cloud service providers (CSP), the privacy and security concerns emerge over the authenticity of the query answer and the leakage of the Data Owner (DO) identity. Providing signature of data owner is always a good solution but the signatures can reveal identity of data owner. In this paper we try to review some techniques and methods which can be used collaboratively to satisfy the aforementioned requirements. These techniques are ring signature scheme for anonymous data upload, Merkel Hash Tree (MHT) for data authentication and non-repudiable service protocol using online trusted authority (TA). To protect trading behavior between the user and the cloud service provider, non-repudiation protocol is used during the transmission of the query answer and the verification object (VO).

Citation: Mr. Shashikant S. Nagdive and Dr. Prashant N. Chatur. 2018. "A Review on Query Answer Authentication in Cloud over Anonymous Data.", *International Journal of Current Research*, 10,(02). 65431-65434.

INTRODUCTION

With the advances in wireless networks and Internet of Things (IoT), large amount of data is collected. As time goes, this fast growing data become hard to store due to weak storage and computing resources. It rise the question that how to store this large data efficiently as well as how to perform queries on it efficiently. Cloud storage resources can be used to solve these issues as it provides flexible, on demand and low cost services. Thus many enterprises, individuals i.e. Data Owner (DO) outsource their data on cloud storage and can get their information of interest by asking the Cloud Service Provider (CSP) to search the outsourced data.There are three main entities in such cloud system, which are Data Owner (DO), Cloud Service Provider (CSP) and User.Operations among data owner, cloud service provider, and user are collaborative due to which many security and privacy issues need to be consider. Three such issues are anonymous identity of data owner, verification of query result for user and non-repudiation of query transaction for cloud service provider. At present, some researches have been done related to the query answer authentication over the data that is outsourced. But none of the research satisfies the above mentioned issues simultaneously. Data owners' requirement of anonymity conflicts with the trustiness of data source authentication.

To solve the aforementioned security and privacy requirements simultaneously, a novel scheme has been proposed in (Wang, 2017), in which various methods are used. Like ring signature scheme is used to satisfy anonymity requirement of data owner, Merkel Hash Tree (MHT) is used to satisfy trustiness authentication of data source. And also non-repudiation service protocol with offline Trust Authority (TA) is used to satisfy non-repudiation of services between user and cloud service provider. The offline TA is used so that it should not intervenes the transaction until both user and CSP have correct behavior. This paper mainly focuses on non-repudiation of service provided by above mentioned scheme, in which offline TA let one of the party in transaction i.e. either user or CSP to break the protocol and deny to be served (in case of user) or charge for service which is not given to user (in case of CSP).In the proposed scheme offline TA is replaced with the online TA, so that now it actively takes part in the transaction. Due to online TA the proposed scheme tries to avoid the incorrect behavior of user or CSP, instead of letting it happen and then try to resolve.

BACKGROUND

The query answer authentication system consist of four entities CSP, DO, user and TA as shown in Figure 1.

***Corresponding author:** Mr. Shashikant S. Nagdive,
Department of Computer Science and Engineering, Government College of Engineering, Amravati (MH) India,

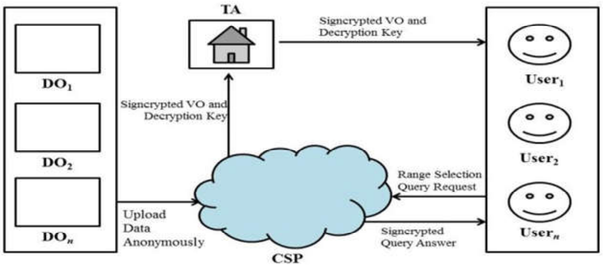
TA
Signcrypted VO and Decryption Key
DO$_1$
DO$_2$
DO$_n$
Signcrypted VO and Decryption Key
User$_1$
User$_2$
User$_n$
Range Selection Query Request
Upload Data Anonymously
Signcrypted Query Answer
CSP

Fig. 1. The cloud system model with non-repudiation service

In this system DO is producer of data, CSP provide services to user, user request data to CSP and TA is used to provide non repudiation of service between CSP and user. This system assumes that the CSP is untrustworthy. When DO uploads data to cloud, it completely loses control over uploaded data. The uploaded data can be lost, altered or tampered by the CSP or may be by the attackers. Therefore user can suspect about the authentication, completeness and trustiness of the query answer provided by the CSP. DO want to upload his data over cloud, but CSP is untrustworthy. Therefore DO generate a merkel hash tree (MHT) using collision resistant hash function. The leaf nodes of the tree contains the hash value if the data. Then select some nodes of this hash tree as key nodes (KN), which signed using ring signature scheme. The ring signature scheme uses *n* DOs to generate digital signature so that the identity of the original DO is hidden. The merkel hash tree and signed key nodes are used calculate verification object (VO), which is used to verify the authenticity of the data by the user. When CSP receive a query from user, it calculates the Result (R) and Verification Object (VO) and sends them to the user in response to query. This VO is used to verify the result R by user. If there are no network errors and no incorrect behavior of CSP and user then Trusted Authority (TA) does not involve in the transaction. But if any network error occurs or if CSP and user any one has incorrect behavior then TA can solve the dispute between them by presenting appropriate evidences. TA can solve the dispute by following the abort or recovery protocol accordingly.

Different techniques used in query answer authentication

Different techniques are used to satisfy different requirements of the system such as Anonymous data upload, Query answer authentication and Non-repudiation of services.

Anonymous Data Upload

Anonymous data upload techniques mainly aims to hide the identity of the data uploader. The origin of anonymous data uploading is *k*-anonymity model, which was proposed by Samarati P. and Sweeney L. in 1998 (Samarati, 1998). Afterwards some new techniques discovered such as *l*-diversity model (Machanavajjhala, 2007), *t*-closeness model (Li, 2007) and some data models with anonymity (Aggarwal, 2008; Ren *et al*., 2012). All these techniques require that data publisher must be trusted which is not possible always as CSP is data publisher in query answer authentication system. So ring signature scheme is introduced, which cutoff the correlation between data and data signer which is DO. Also this scheme guarantees the trustiness of the data. The first ever effective construction of the ring signature scheme was proposed by Rivest, Shamir and Tauman in 2001 (Rivest, 2001).

Afterwards different variants and constructions have been appeared (Chow, 2005; Dodis *et al*., 2004; Zhang, 2002; Huang, 2015; Yang *et al*., 2015). Using ring signature scheme DO can sing the data anonymously and user can check the trustiness of the signature without revealing the signer of data (Tsang *et al*., 2010; Bresson *et al*., 2002; Melchor *et al*., 2011; Yuen, 2013). If ring signature scheme is used directly, DO will have to sign the entire data records one by one, which is not possible with large data in cloud environment.

Query Answer Authentication

The query answer authentication scheme is used to verify the data downloaded as a result of query by the query user. A very simple and straight forward approach to do that is to generate digital signature for each of the data record in the query result. MHT (Merkle, 1989) can be used as an improvement over the traditional scheme that can reduce the numbers of digital signature to be generate by great extent. The basic idea is to replace the signature with the hashvalues in MHT. Basically MHT is a binary tree in which each of the internal nodes contains the hash value of concatenation of its left and right child, and the leaf node contains hash value of the actual data value. The data value is considered to be correct because the hash value of the tree root is published authentically using digital signature. The DO sends the user actual data value and the hash value of the sibling nodes that lie in the path from root to that data value, to prove the authenticity of the data value. The user can recomputed the hash of the root by iteratively calculating and concatenating the appropriate hashes and verify its correctness by using digital signature of root. The collision resistant hash functions and the security of digital signature of the hash value of the root node guarantees the correctness of the value. MHT is mainly used in query authentication over outsourced data (Gan, 2014; Liu *et al*., 2015; Wu *et al*., 2015). MHT has several disadvantages when dealing with large data environment. In such cases, constructed MHT can be very high and when executing verification, it requires user to calculate hash values of complete internal nodes to get the hash value the root node. If the digital signature of the root node is tampered then all these hash calculation will be useless. Also multiple data owners are not well supported.

Non-Repudiation of Services

Non-repudiation of services mainly aims to collect, maintain and validate non refutable evidences about the transaction. Also make these evidences available whenever there is need to solve the dispute between two parties involved in the transaction. Dispute occurs when any one party involved in transaction is denying that a certain action or event took place. In such situations some irrefutable evidences are collected during the transaction and presented to resolve any of such disagreement. Two types of evidences are generated and collected during the stransactions that are evidence of non-repudiation of origin and evidence of non-repudiation of receipt. They work in four separate phases: generation of evidence, transferring and storing the evidence, verification of evidence and dispute resolution. The first ever fair non-repudiation protocol was proposed by Zhou J. and Gollmann D. in 1996 (Zhou, 1997; Zhou, 1996). Later on, many variants of the protocol have appeared which make use of different encryption techniques (Yildiz *et al*., 2016; Li *et al*., 2015; Wu *et al*., 2013; Feng *et al*., 2011; Feng *et al*., 2010; Luo *et al*., 2009; Kremer *et al*., 2002) such as encryption based on hash function, block encryption based on Chinese Remainder Theorem, encryption with secret sharing technique, multiple block encryption technique, etc.Non-repudiation protocol model can be divided into two types based on inclusion of Trusted Authority (TA): non-repudiation with TA and non-repudiation without TA. In non-repudiation without TA, two parties exchange the information step by step (Tedrick, 1984; Tedrick, 1984). This method cannot be used in cloud services because it requires high computing power of communicating parties. Non-repudiation protocol model with TA can well support the security of the non-repudiation services. In non-repudiation protocol with TA, there can be three types of TA online TA, inline TA and offline TA (Kremer, 2002).

Conclusion

In this paper we have made survey on query answer authentication and various techniques that have been used in the system. We also identify the some issues and drawbacks of these techniques when used in cloud environment. From the above discussion we can conclude that if some little changes are made in MHT, ring signature and non-repudiation with TA techniques they can be used in cloud storage system.

REFERENCES

Aggarwal, C.C.2008. “On unifying privacy and uncertain data models,” in *Proc. IEEE 24th Int. Conf. Data Eng.*, Apr., pp. 386–395.

Bresson, E., Stern, J. and Szydlo, M. 2002. “Threshold ring signatures and applications to ad-hoc groups,” in *Proc. Annu. Int. Cryptol. Conf.*, pp. 465–480.

Chow, S.S., Yiu, S.M. and Hui, L. C. 2005. “Efficient identity based ring signature,” in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, pp. 499–512.

Dodis, Y., Kiayias, A., Nicolosi, A. and Shoup, V. 2004. “Anonymous identification in ad hoc groups,” in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn.*, pp. 609–626.

Feng, J., Chen, Y., Ku, W.S. and Liu, P. 2010.‘‘Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms,’’ in Proc. 39th Int. Conf. Parallel Process. Workshops, Sep. pp. 251–258.

Feng, J., Chen, Y., Summerville, D., Ku, W.S. and Su, Z. 2011. ‘‘Enhancing cloud storage security against roll-back attacks with a new fair multiparty non-repudiation protocol,’’ in Proc. IEEE Consum. Commun. Netw. Conf. (CCNC), Jan. pp. 521–522.

Gan, H. and Chen, L. 2014. “An efficient data integrity verification and fault-tolerant scheme,” in *Proc. 4th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Apr. pp. 1157–1160.

Han, Z.G. and Luo, J.Z. 2009. ‘‘Analysis and improvement of timeliness of a multi-party non-repudiation protocol,’’ Acta Electron. Sinica, vol. 37, no. 2, pp. 377–381.

Huang X. *et al.* 2015. “Cost-effective authentic and anonymous data sharing with forward security,” *IEEE Trans. Comput.*, vol. 64, no. 4, pp. 971–983, Apr.

Kremer, S., Markowitch, O. and Zhou, J. 2002.‘‘An intensive survey of fair nonrepudiation protocols,’’ Comput. Commun., vol. 25, no. 17, pp. 1606–1621, Nov.

Li, J., Lu, H. and Guizani, M. 2015.‘‘ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs,’’ IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 4, pp. 938–948, Apr.

Li, N., Li, T. and Venkatasubramanian, S. 2007. “T-closeness: Privacy beyond k-anonymity and l-diversity,” in *Proc. IEEE 23rd Int. Conf. Data Eng.*, Apr. pp. 106–115.

Liu, C., Ranjan, R., Yang, C., Zhang, X., Wang, L. and Chen, J. 2015. ‘‘MuRDPA: Top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud,’’ IEEE Trans. Comput., vol. 64, no. 9, pp. 2609–2622, Sep.

Luo, J.Z., Han, Z.G. and Wang, L.M. 2009. ‘‘Trustworthy and controllable network architecture and protocol framework,’’ Chin. J. Comput., vol. 32, no. 3, pp. 391–404.

Machanavajjhala, A., Kifer, D., Gehrke, J. and Venkitasubramaniam, M. 2007. “L-diversity: Privacy beyond k-anonymity,” *ACM Trans. Knowl. Discovery Data*, vol. 1, no. 1, Mar, Art. no. 3.

Melchor, C. A., Cayrel, P.L., Gaborit, P. and Laguillaumie, F. 2011. “A new efficient threshold ring signature scheme based on coding theory,”*IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4833–4842, Jul.

Merkle, R.C. 1989. “A certified digital signature,” in *Proc. Conf. Theory Appl. Cryptol.*, pp. 218–238.

Ren, X. M., Yang, J., Zhang, J. P. and Jia, Z. F. 2012. “Uncertain data privacy protection based on k-anonymity via anatomy,”*Adv. Eng. Forum*, vols. 6_7, pp. 64–69, Sep.

Rivest, R. L., Shamir, A. and Tauman, Y. 2001. “How to leak a secret,” in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, pp. 552–565.

Samarati, P. and Sweeney, L. 1998. “Protecting privacy when disclosing information: K-anonymity and its enforcement through generalization and suppression,” Comput. Sci. Lab., SRI Int., Menlo Park, CA, USA, Tech. Rep. SRICSL-98-04.

Tedrick, T. 1984.‘‘Fair exchange of secrets,’’ in Proc. Workshop Theory Appl. Cryptogr. Techn., , pp. 43

Tedrick, T. 1984.‘‘How to exchange half a bit,’’ in Advances in Cryptology. New York, NY, USA: Plenum Press, pp. 147–151.

Tsang, P. P., Au, M. H., Liu, J. K., Susilo, W. and Wong, D. S. 2010. “A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity,” in *Proc. Int. Conf. Provable Secur.*, pp. 166–183.

Wang, L. and Xie, Q. 2017. “Cooperative Query Answer Authentication Scheme Over Anonymous Sensing Data,” *IEEE Access*, vol. 5, pp. 3216-3227.

Wu, C.Y., Xiong, Y., Huang, W.C., Lu, Q.W., and Gong, X.D. 2013. ‘‘A trusted fair non-repudiation protocol based on dynamic third party in mobile ad hoc networks,’’ Acta Electron. Sinica, vol. 41, no. 2, pp. 227–232.

Wu, D., Choi, B., Xu, J. and Jensen, C. S. 2015. ‘‘Authentication of moving top-k spatial keyword queries,’’ IEEE Trans. Knowl. Data Eng., vol. 27, no. 4, pp. 922–935, Apr.

Yang, X., Wu, W., K. J. Liu, and Chen, X. 2015. “Lightweight anonymous authentication for ad hoc group: A ring signature approach,” in *Proc. Int. Conf. Provable Secur.*, pp. 215–226.

Yildiz, H. U., Bicakci, K., Tavli, B., Gultekin, H. and Incebacak, D. 2016. ‘‘Maximizing wireless sensor network lifetime by communication/computation energy optimization of non-repudiation security service: Node level versus network level strategies,’’ Ad Hoc Netw., vol. 37, pp. 301–323, Feb.

Yuen, T.H., Liu, J. K., Au, M. H., Susilo, W. and Zhou, J. 2013. "Efficient linkable and/or threshold ring signature without random oracles,"*Comput. J.*, vol. 56, no. 4, pp. 407–421.

Zhang, F. and Kim, K. 2002."ID-based blind signature and ring signature from pairings," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, pp. 533–547.

Zhou J. and Gollmann, D. 1996. ''A fair non-repudiation protocol,'' in Proc. IEEE Symp. Secur. Privacy, May, pp. 55–61.

Zhou J. and Gollmann, D. 1997. ''An efficient non-repudiation protocol,'' in Proc. 10th Comput. Secur. Found. Workshop, Jun., pp. 126–132.

****