Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

A Review on Security by using Encrypted Key Exchange Between Client and Cloud Storage

Sonam Maheshwari[1]
Research Scholar,
Department of Computer Science,
RITS Bhopal (MP)

Shivank Kumar Soni[2]
Asst .Professor,
Department of Computer Science,
RITS Bhopal (MP)

Chetan Agrawal[3]
Head,
Department of Computer Science,
RITS Bhopal (MP)

***Abstract*- Cloud Computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. As information exchange plays an vital role in today's life, information security becomes more important. This paper mainly focuses on providing the security by using encrypted key Exchange between client and cloud Storage and techniques to overcome the issues of data privacy. The client only needs to download the encrypted secret key from the Authorized party when uploading new files to cloud. Our design also equips the client with capability to further verify the validity of the encrypted secret keys provided by Authorized party. All these features are carefully designed to make the whole auditing procedure with key exposure resistance as transparent as possible for the client. We also check the Authorized party is valid or not like proxy servers the definition and the security model of this paradigm.**

Keywords- Cloud Computing, Cloud Security, Security issues,TPA

I. INTRODUCTION

Cloud computing paradigm has witnessed an enormous shift towards its adoption and it has become a trend in the information technology space as it promises significant cost reductions and new business potential to its uses and providers. CLOUD computing, as a new technology paradigm with promising further, is becoming more and more popular nowadays. It can provide users with unlimited computing resource. Enterprises and people can outsource time-consuming computation workloads to cloud without spending the extra capital on deploying and maintaining hardware and software. In recent years, outsourcing computation has attracted much attention and been researched widely. It has been considered in many applications including scientific computations.

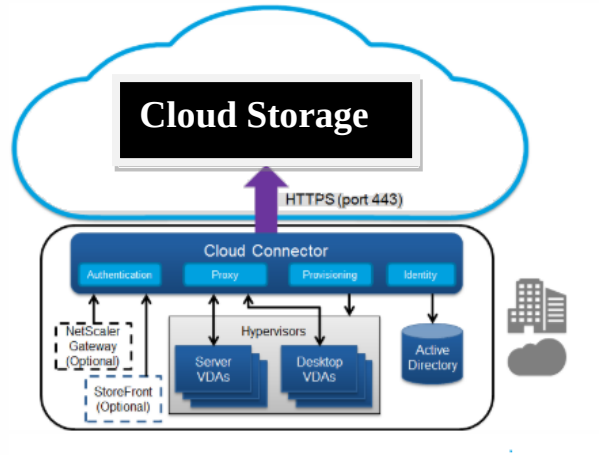

Figure 1: Cloud Client Distributed

However, it needs to satisfy several new requirements to achieve this goal. Firstly, the real client's secret keys for cloud storage auditing should not be known by the authorized party who performs outsourcing computation for key updates. Otherwise, it will bring the new security threat. So the authorized party should only hold an encrypted version of the user's secret key for cloud storage auditing. Secondly, because the authorized party performing outsourcing computation only knows the encrypted secret keys, key updates should be completed under the encrypted state.

II. RELATED WORK

Jia Yu et al. "Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates" In this paradigm, key updates can be safely outsourced to some authorized party, and thus the key-update burden on the client will be kept minimal. Specifically, we leverage the third party auditor (TPA) in many existing public auditing designs, let it play the role of authorized party in our case, and make it in charge of both the storage auditing and the secure key updates for key-exposure resistance. In our design, TPA only needs to hold an encrypted version of the client's secret key, while doing all these burdensome tasks on behalf of the client. The client only needs to download the encrypted secret key from the TPA when uploading new files to cloud. Besides, our design also equips the client

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

with capability to further verify the validity of the encrypted secret keys provided by TPA.

In 2017, Chanying Huang et al. has been proposed an Efficient anonymous attribute-based encryption with access policy hidden for cloud computing.

Using the idea of Boolean equivalent transformation, the proposed scheme can achieve fast encryption and protect the privacy for both data owner and legitimate access user. In addition, the proposed scheme can satisfy constant secret key length and reasonable size of cipher text requirements. We conduct theoretical security analysis, and carry out experiments to prove that the proposed scheme has good performance in terms of computational, communication and storage overheads. Akhilesh Yadav et al. "Securing Cloud Computing Environment using Quantum Key Distribution" Nowadays, Information Technology group is undergone significant shift in computing and protecting business value by using well-built, workable and authentic replacement of Cloud Computing. Cloud Computing is a contemporary computational architecture that provides another type of model. This paper proposes as a service of Advanced Quantum Cryptography in Cloud Computing. This paper discusses the security issues of cloud computing and the role of cryptography technique in Cloud computing to enrich the Information Security.

Rongzhi Wang "Research on Data Security Technology Based on Cloud Storage"
Encryption storage, integrity verification, access control and verification and so on.
Through the data segmentation and refinement rules algorithm to optimize the access control strategy, using the data label verification cloud data integrity, using replica strategy to ensure the data availability, the height of authentication to strengthen security, attribute encryption method using signcryption technology to improve the algorithm efficiency, the use of time encryption and DHT network to ensure that the cipher text and key to delete the data, so as to establish a security scheme for cloud storage has the characteristics of privacy protection.

Audit-Free Cloud Storage via Deniable Attribute-Based Encryption propose in year 2017.

Contribution:- Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected.

Journal and year :-IEEE Transactions on Cloud Computing June 2018.
Research on data security technology based on cloud storage

Contribution:- In this paper we develop two evaluation techniques, namely QPT and QHP, for conducting the quantitative assessment and analysis of the secSLA based security level
provided by CSPs with respect to a set of Cloud Customer security requirements. These
proposed techniques help improve the security requirements specifications by introducing a flexible and simple methodology that allows Customers to identify and represent their specific security needs. Apart from detailing guidance on the standalone and collective use of QPT and QHP, these techniques are validated using two use case scenarios and a prototype, leveraging actual real-world CSP sec SLA data derived from the Cloud Security Alliance's Security, Trust and Assurance Registry.

Journal and year :-ELSEVIER 2017 Procedia Engineering 174 (2 017) 1340 – n1355
Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates

Contribution:- In Authors design, TPA only needs to hold an encrypted version of the client's secret key, while doing all these burdensome tasks on behalf of the client. The client only needs to download the encrypted secret key from the TPA when uploading new files to cloud. Besides, our design also equips the client with capability to further verify the validity of the encrypted secret keys provided by TPA. All these salient features are carefully designed to make the whole auditing procedure with key exposure resistance as transparent as possible for the client. We formalize the definition and the security
model of this paradigm. The security proof and the performance simulation show that our detailed design instantiations are secure and efficient.

Journal and year :- IEEE Transactions on Information Forensics and Security (Volume:11 , Issue:6),11 February 2016
Securing Cloud Computing Environment using a New Trend of Cryptography Sign In or Purchase

Contribution:- Nowadays, Information Technology group is undergone significant shift in computing and protecting business value by using well-built, workable and authentic replacement of Cloud Computing. Cloud Computing is a contemporary computational architecture that provides another type of model. This paper proposes as a service of Advanced Quantum Cryptography in Cloud Computing. This paper discusses the security issues of cloud computing

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

and the role of cryptography technique in Cloud computing to enrich the Information Security.

Journal and year 2015 International Conference on Cloud Computing (ICCC) Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage

Contribution - In this paper, we first design an auditing framework for cloud storage and proposed an algebraic signature based remote data possession checking protocol, which allows a third-party to auditing the integrity of the outsourced data on behalf of the users and supports unlimited number of verifications. Then we extends our auditing protocol to support data dynamic operations, including data update, data insertion and data deletion. The analysis and experiment results demonstrate that our proposed schemes are secure and efficient.

III. Comparative Analysis of different Encryption Techniques :-

Table 1: Comparison of memory used

Algorithm	Memory used (KB)
DES	18.2
3DES	20.7
AES	14.7
Blowfish	9.38
RSA	31.5

Table 2: Average entropy values

Algorithm	Average entropy per byte of encryption
DES	2.9477
3DES	2.9477
AES	3.84024
Blowfish	3.93891
RSA	3.0958

Table 3: Optimal encoding length

Algorithm	Average number of bits demanded to optimally encode a byte of encrypted data
DES	27
3DES	40
AES	256
Blowfish	128
RSA	44

IV. CONCLUSION

Cloud computing by itself is in evolving stag security implications in it are not complete. It is evident that even the leading cloud providers such as Amazon, Google etc are facing many security challenges and are yet to stabilize. Achieving complete solution for are facing many security challenge With this level of issues in cloud computing decisions to adopt cloud computing in an organization could be made only based on the benefits to risk ratio. By checking a proxy server we will find out the fault in encryption. Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the client end and the cloud server end. Main goal of cloud computing is securely store and transmit the data in cloud

V. REFERENCES

[1] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. ESpafford, “Secure outsourcing of scientific computations,” Trends in Software Engineering, vol. 54, pp. 215-272
[2] Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie, "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing", IEEE International Conference on Cloud Computing Technology and Science, 2010.
[3] Younis A. Younis, Kashif Kifayat, Madjid Merabti, "An access control model for cloud computing", Elsevier journal of information security and applications, 2014.
[4] C. Wang, Q. Wang, K. Ren, N. Cao, W. LouToward secure and dependable storage services in cloud computing IEEE Trans. Services Comput., 5 (2) (2012), pp. 220-232
[5] Duncan, Adrian, Sadie Creese, and Michael Goldsmith . “Insider attacks in cloud computing.” Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE,2012.
[6] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. E.Spafford, “Secure outsourcing of scientific computations,”Trends in Software Engineering, vol. 54, pp. 215-272 2002.
[7] D. Benjamin and M. J. Atallah, “Private and cheatingfree outsourcing of algebraic computations,” Proc. Sixth Annual Conference on Privacy, Security and Trust, pp. 240-245, 2008.
[8] C.Wang, K. Ren, and J.Wang, “Secure and practical outsourcing of linear programming in cloud computing,” IEEE INFOCOM 2011, pp. 820-828, 2011.
[9] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, “New Algorithms for Secure Outsourcing of Modular Exponentiations,” Proc. 17th European Symposium on Research in Computer Security, pp. 541-556, 2012.
[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 06, June-2019

[11] A. Juels, J. Burton, and S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 584-597, 2007.
[12] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Advances in Cryptology-Asiacrypt'08, pp. 90-107, 2008.
[13] G. Ateniese, R.D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. 4th International Conference on Security and Privacy in Communication Networks, 2008
[14] F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1-6, 2008.
[15] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PPDP: Multiple-Replica Provable Data Possession,"Proc. 28th IEEE International Conference on Distributed Computing Systems, pp. 411-420, 2008.
[16] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conference on Computer and Communications Security, pp. 756-758, 2010.
[17] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[18] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.
[19] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.
[20] Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Trans. on Services Computing, vol. 6, no. 2, pp. 409-428, 2013.
[21] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.
[22] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing, Vol. 6, no. 4, pp. 551-559, 2013.
[23] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, Vol. 62, No. 2, pp. 362-375, 2013.
[24] B. Wang, B. Li and H. Li. Oruta, "Privacy-Preserving Public Auditing for Shared Data in the Cloud," IEEETransactions on Cloud Computing, Vol.2, pp. 43-56, 2014.
[25] C. Erway, A. Kpc, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," Proc. of the 16th ACM conference on Computer and communications security, pp.213-222,2009.