International Journal of Advanced and Innovative Research (2278-7844) / Volume 7 Issue 6

Security by Using Encrypted Key Exchange between client and cloud storage: - A Review

Tanuj Sharma
M Tech Scholar
Department of Computer Science & Engineering
SAMCET Bhopal MP
Sharmatanuj048@gmail.com

Ankur Tanuja
Assistant Professor
Department of Computer Science & Engineering
SAMCET Bhopal MP
ankurtaneja5@gmail.com

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 important role in today's life, information security becomes more important. This paper is focused on the security by using encrypted key Exchange between client and cloud Storage and techniques to overcome the data privacy issue. The client only needs to download the encrypted secret key from the Authorized party 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 Authorized party. 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 also check the Authorized party is valid or not like proxy servers 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.

Keywords

Cloud Computing, Cloud Security, Security issues

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. C LOUD 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.

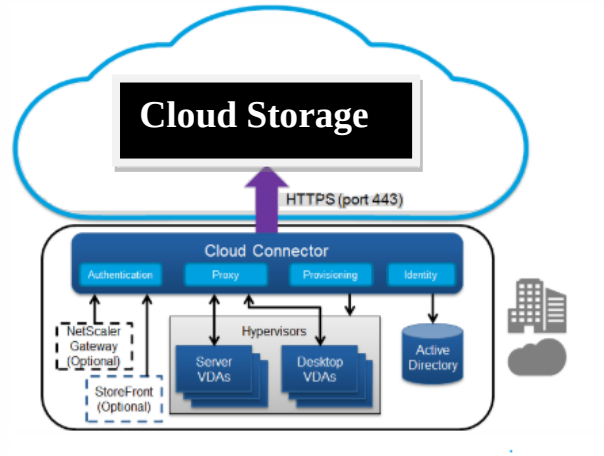

Figure 1: Cloud Client Distributed

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.

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

Chanying Huang et al**." 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 ciphertext 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.[1]

PROPOSED WORK

cloud storage auditing protocol with secure outsourcing of key updates is composed by seven algorithms (SSetup, EUpdate, VESK, DESK, AuthGen, Proof- Gen, ProofVerify and Check Proxy TPA), shown below:

- SSetup: the system setup algorithm is run by the client. It takes as input a security parameter k and the total number of time periods T, and generates an encrypted initial client's secret key ESK0, a decryption key DK and a public key PK. Finally, the client

holds DK, and sends ESK0 to the TPA.

- EUpdate: the encrypted key update algorithm is run by the TPA. It takes as input an encrypted client's secret key ESKj , the current period j and the public key PK, and generates a new encrypted secret key ESKj+1 for period j + 1.
- VESK: the encrypted key verifying algorithm is run by the client. It takes as input an encrypted client's secret key ESKj , the current period j and the public key PK, if ESKj is a well-formed encrypted client's secret key, returns 1; otherwise, returns 0.
- DESK: the secret key decryption algorithm is run by the client. It takes as input an encrypted client's secret key ESKj , a decryption key DK, the current period j and the public key PK, returns the real client's secret key SKj in this time period.
- AuthGen: the authenticator generation algorithm is run by the client. It takes as input a file F, a client's secret key SKj , the current period j and the public key PK, and generates the set of authenticators _ for F in time period j.
- ProofGen: the proof generation algorithm is run by the cloud. It takes as input a file F, a set of authenticators a challenge a time period j and the public key PK, and generates a proof P which proves the cloud stores F correctly.
- Checking algorithm for proxy server of TPA Proof Verify: the proof verifying algorithm is run by the TPA. It takes as input a proof P, a challenge a time period j, and the public key PK, and returns

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

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.