International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

Proxy-Oriented Data Uploading & Monitoring Remote Data Integrity in Public Cloud

Tanmay Borkar[1], Mangesh Dudhal[2], Snehal Ghadage[3], Sumit Kawale[4]

[1, 2, 3 & 4]*Dept. of Computer Engineering, NBN Sinhgad School of Engineering, Maharashtra, India*

Abstract - *In today's modern era, each & every person is connected to Cloud Infrastructure for storing his huge data sets due to rapid development in Cloud Computing. Cloud Services are getting very prominent but introduction to new threats &security issues restricts users from uploading data to cloud. When a user is restricted to upload a data, he/she will alter his proxy & to upload his data to Cloud Environment. Uploading data with proxy alteration, also introduces new treats like Data stealing & uploading malware on Cloud Infrastructure. Furthermore, remote integrity checking of data is also an major security issue in public cloud storage. It makes client monitor his/her data set's integrity without actually downloading it. To counter such issues, we present a Cryptographic Proxy Oriented Data Uploading to avoid data from fake sources & algorithms to protect user data from external or internal threats.*

Key Words: Cloud Computing, ID-PUIC, Proxy Orientation, Malware Detection, Data Integrity, Key Generation, Encryption & Decryption.

1. INTRODUCTION

Due to rapid progress in cloud computing, many users prefer to save their data to public cloud servers. Newly developed security problems have to be solved to help as many clients as possible to compute their data in public cloud. When the client is restricted to access Public Cloud Server, he/she will alter its proxy to process his data & upload them.

In addition to this, checking of remote data integrity is the most trivial security issue in public cloud storage. It ensures that the client data are kept undamaged without downloading the whole data.

Based on security problems, we propose a system called proxy-oriented data uploading and remote data integrity checking system using identity-based public key cryptography: remote data integrity checking in public cloud and identity-based proxy-oriented data uploading (ID-PUIC).

We design a system & security model that is robust ID-PUIC protocol which is efficient to counter visible problems. The proposed ID-PUIC protocol is securely based on the stiffness of computational Diffie–Hellman problem. This proposed ID-PUIC protocol is not only efficient but also flexible. Depending on the client's authorization, the proposed ID-PUIC protocol can perform checking of private remote integrity of data to avoid any anonymous data from false sources and maintain protection of data integrity.

2. EXISTING SYSTEM

Now a day's most of the users over internet use public cloud to upload and store their data. In fact, users prefers to store huge amount of data on PCS (public cloud system), it may be normal photographs or files to a large amount of a secret data of a company or corporates. Once it is uploaded by client on PCS, then its data integrity is checked over the internet and this causes the problem for most of the times. For example, let say in case of small organization where individual manager uploads secret and commercial data on PCS and later on the same manager found in commercial fraud of the organization then obviously he/she may not be able to access the public cloud network against safe guarding the business. But even if he/she can't be able to process the huge data over a time period then the company will be in serious issues so he/she has to appoint some loyal person so that they can process the data. But in this case also the manager will not be sure on his/her delegates whether they can process the data integrity correctly and efficiently. Publicly checking the data integrity may lead to privacy issue of data leaking over PCS. The data stored on PCS may lead to malicious activities. As the data uploaded on PCS is very confidential and has to be kept secured. So there has to be a provision of private data integrity which can be only done by a Manager or his/her level person of an organization. So he/she has to appoint someone as a proxy to check the data integrity part. So we will be having a remote data integrity checking, through a protocol, which will be done by certain certificate management. When the person like Manager delegate the data integrity part over PCS, then the delegate has to check the data integrity through the certificates checking and validity each time.

3. DISADVANTAGES OF EXISTING SYSTEM

1. In case of Public Key Infrastructure, we need to take care of lot of things like certificate generation, its verification, revocation of certificate and its renewal which increases the time complexity and overhead on PCS.

2. In PCS, the other devices like IPADS, Tablets and mobile phone may result into low computational capacity.

4. LITERATURE REVIEW

In today's digital era, cloud computing plays a significant role in storage of data. The substantial development in cloud, solves many issues of storing enormous static or runtime datasets. Along with advantages, it contains much vulnerability. It is more prone to maliciously uploading of data & data theft attacks. It also contains vulnerability of monitoring the erectness of uploaded data.

Customers tend to upload, store and retrieve all their essential data and information through the cloud service providers that is CPSs using distributed computing. New security issues come across that whether the data is safe, is it from a trusted user, etc. Data honesty is also another issue which needs to be overlooked. Issues of checking whether the data is kept in a safe location or not is also needed to be checked. To overcome such issues Remote Integrity information system is used. In the paper the use of Identity based Proxy oriented data uploading and remote data integrity checking (ID-PUIC) protocol is proposed. This is effective and adaptable and can understand the private remote information honesty checking, and open remote information honour checking. Customers store their large data/information in the remote open cloud servers while using the cloud computing concept. It does not guarantee whether the data is stored in right place. Thus, remote information integrity checking enables the customers to understand the storage of information and location of information. Due to its limitations, owner's information is known to limited people. Using the real client's permission or authorization this protocol ensures the private checking and public checking respectively.

5. PROPOSED SYSTEM

The area remote data integrity checking and identity based proxy oriented data uploading is focused in this project. As the certificate management is eliminated, with the use of identity based public key cryptology our proposed ID-PUIC protocol is efficient.

ID-PUIC is remote data integrity checking model in public cloud as well as a novel proxy oriented data uploading. We give the formal system model and security model for ID-PUIC protocol.

The first ID-PUIC protocol was designed on the basis of bilinear pairing. Our ID-PUIC model is proven to be secure in the random oracle model. Our protocol can realized delegated checking, private checking and public checking based on the original client authorization.

6. ADVANTAGES OF PROPOSED SYSTEM

1. The efficiency of our system is improved coz we are implementing data integrity on PCS through a proxy oriented data upload.
2. The main advantage of our system is that security is improved as we are implementing identity based proxy oriented scheme for data uploading through a concrete ID-PUIC protocol which is secure and efficient.

7. SYSTEM ARCHITECTURE

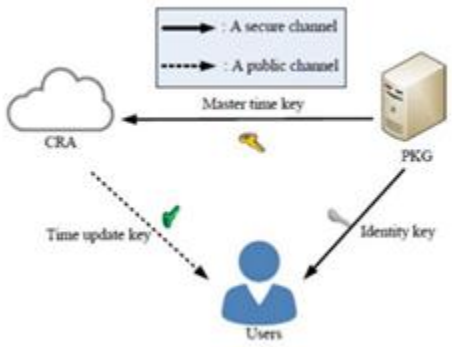

Fig. 1. System Architecture

The concrete ID-PUIC protocol comprises four procedures:

Setup, Extract, Proxy-key generation, TagGen, and Proof. In order to show the intuition of our construction, the concrete protocol's architecture is depicted in Figure 1. First, Setup is performed and the system parameters are generated. Based on the generated system parameters, the other procedures are performed as Figure 1. It is described below:

(1) In the phase Extract, when the entity's identity is input, KGC generates the entity's private key. Especially, it can generate the private keys for the client and the proxy.

(2) In the phase Proxy-key generation, the original client creates the warrant and helps the proxy generate the proxy key.

(3) In the phase TagGen, when the data block is input, the proxy generates the block's tag and uploads block-tag pairs to PCS.

(4) In the phase Proof, the original client O interacts with PCS. Through the interaction, O checks its remote data integrity

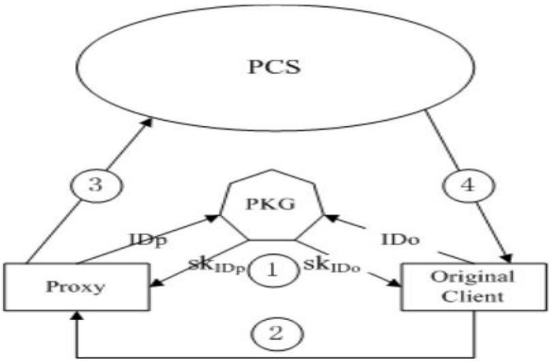

Fig. 2. Working

8. CONCLUSION

In this paper, we introduce proxy based data uploading concept and have successfully implemented in public cloud. Furthermore, we have also introduced malware detection while uploading the data to cloud and have successfully implemented the feature that can correct the malware on its detection. In addition to this, our system has even successfully ingrained the ability to check the robustness of data placed in public cloud with downloading the whole contents for robust test.

In general, the system proposed in this paper is designed to be responsive and adaptive to run time data variety and protection from malicious file without explicitly programmed.

9. REFERENCES

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, Achieving efficient cloud search services: multi-keyword ranked search over encrypted cloud data sup-porting parallel computing, IEICE Transactions on Communications, vol. E98-B, no. 1, pp.190-200, 2015.

[2] Y. Ren, J. Shen, J. Wang, J. Han, S. Lee, Mutual verifiable provable data auditing in public cloud storage, Journal of Internet Technology, vol. 16, no. 2, pp. 317-323, 2015.

[3] A. Marnerides, C. James, A. Schaeffer, S. Sait, A. Mauthe, and H. Murthy, Multi-level network resilience: Traffic analysis, anomaly detection and simulation, ICTACT Journal on Communication Technology, Special Issue on Next Generation Wireless Networks and Applications, vol. 2, pp. 345356, June 2011.

[4] M.Mambo, K. Usuda, E. Okamoto, Proxy signature for delegating signing operation, CCS 1996, pp. 48C57, 1996.

[5] E. Zhou and Z. Li, An improved remote data possession checking protocol in cloud storage, in Algorithms and Architectures for Parallel Processing.

[6] H. Wang, Proxy provable data possession in public clouds, IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551-559, 2013.