IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 6, June 2016

Proxy Server for Custom Based Protocols in Cloud Computing

Aswini Retnan[1], Mr. M. Nakkeeran M.E[2]

Computer Science and Engineering, SVS College of Engineering[1]

Assistant Professor, Computer Science and Engineering, SVS College of Engineering[2]

Abstract: Cloud computing is an emerging data interactive paradigm to realize users' data remotely stored in an online cloud server. Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be illegally accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. In this paper, we propose a shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security); 2) attribute based access control is adopted to realize that the user can only access its own data fields; 3) proxy re- encryption is applied to provide data sharing among the multiple users. Meanwhile, universal composability (UC) model is established to prove that the SAPA theoretically has the design correctness. It indicates that the proposed protocol is attractive for multi-user collaborative cloud applications.

Keywords: Cloud computing, authentication protocol, privacy preservation, shared authority, universal composability.

INTRODUCTION

Cloud computing is emerging as a prevalent data interactive paradigm to realize user's data remotely stored in an online cloud server. Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. A cloud storage system, consisting of a collection of storage servers, provides long-term storage services over the Internet. Storing data in a third party's cloud system causes serious concern over data confidentiality. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. We propose a threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated.

LITERATURE REVIEW

1 A Secure Decentralized Erasure Code for Distributed Network Storage.

We consider the problem of constructing an erasure code for storage over a network when the data sources are distributed. Specifically, we assume that there are n storage nodes with limited memory and k < n sources generating the data. We want a data collector, who can appear anywhere in the network, to query any k storage nodes and be able to retrieve the data. We introduce Decentralized Erasure Codes, which are linear codes with a specific randomized structure inspired by network coding on random bipartite graphs. We show that decentralized erasure codes are optimally sparse, and lead to reduced communication, storage and computation cost over random linear coding. In this correspondence, we address the problem of distributed networked storage when there are multiple, distributed sources that generate data that must be stored efficiently in multiple storage nodes, each having limited memory. As a motivating application, one can think of sensor networks where the sensor measurements are inherently distributed and sensor motes have constrained communication, computation, and storage capabilities. In addition, distributed networked storage can be useful for peer-to-peer networks or redundant arrays of independent disks (RAID) systems. The distributed sources are k data nodes, each producing one data packet of interest. We also assume we have n storage nodes that will be used as a distributed network memory. H.-Y Lin and W.-G Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.

2 Plautus: Scalable Secure File Sharing on Untrusted Storage.

Plautus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plautus features highly scalable key management while allowing individual

users to retain direct control over who gets access to their files. We explain the mechanisms in Plautus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. We have built a prototype of Plautus on Open AFS. Measurements of this prototype show that Plautus achieves strong security with overhead comparable to systems that encrypt all network traffic. To protect stored data, it is not sufficient to use traditional network security techniques that are used for securing messages between pairs of users or between clients and servers. Thinking of a stored data item simply a message with very long network latency is a misleading analogy
M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plautus: Scalable Secure File Sharing on Untrusted Storage," Proc. Second USENIX Conf File and Storage Technologies (FAST),pp. 29-42, 2003.

3 Total Recall: System Support for Automated Availability Management.

Availability is a storage system property that is both highly desired and yet minimally engineered. While many systems provide mechanisms to improve availability – such as redundancy and failure recovery – how to best configure these mechanisms is typically left to the system manager. Unfortunately, few individuals have the skills to properly manage the trade-offs involved, let alone the time to adapt these decisions to changing conditions. Instead, most systems are configured statically and with only a cursory understanding of how the configuration will impact overall performance or availability. While this issue can be problematic even for individual storage arrays, it becomes increasingly important as systems are distributed – and absolutely critical for the wide area peer-to-peer storage infrastructures being explored. This paper describes the motivation, architecture and implementation for a new peer-to-peer storage system, called Total Recall that automates the task of availability management. R. Bhagwan, K. Tati, Y.-C. Cheng, S. Savage, and G.M. Voelker, "Total Recall: System Support for Automated Availability Management," Proc. First Symp. Networked Systems Design and Implementation (NSDI), pp. 337-350, 2010.

4 Ubiquitous Access to Distributed Data in Large-Scale Sensor Networks through Decentralized Erasure Codes

Consider a large-scale+ wireless sensor network of n nodes, where a fraction k out of n generate data packets of global interest. Assuming that the individual nodes have limited storage and computational capabilities, we address the problem of how to enable ubiquitous access to the distributed data packets. Specifically, we assume that each node can store at most one data packet, and study the problem of diffusing the data so that by querying any k nodes, it is possible to retrieve all the k data packets of interest (with high probability). We introduce a class of erasure codes and show how to solve this problem efficiently in a completely distributed and robust way. Specifically we show that we can efficiently diffuse the data by "pre-routing" only O(ln n) packets per data node to randomly selected storage nodes. By using the proposed scheme, the distributed data becomes available "at the fingertips" of a potential data collector located anywhere in the network.

PROPOSED RE-ENCRYPTION WORK

Cloud Formation

The public cloud environment is the IaaS/PaaS Infrastructure or Platform as a Service that we rent from Linux (IaaS) or Microsoft (PaaS). Both are enabled for web hosting. Then, your SaaS stack will run under your Internet environment most likely in a virtualized one on your own equipment which would make it private. In this project we specialize in private cloud technology. Here we execute in a cloud environment. If strict security requirements go public or hybrid and if not, try the public or community cloud environment.

Data Owner

This is the initial module of this project. Data ownership refers to both the possession of and responsibility for information. Ownership implies power as well as control. The control of information includes not just the ability to access, create, modify, package, derive benefit from, sell or remove data. Data ownership is the act of having legal rights and complete control over a single piece or set of data elements.

Construction of secure cloud storage

Here the construction of the cloud will be more secured. The encryption methods are follows in the next module. The two biggest concerns about cloud storage are reliability and security. Basically, a cloud storage system can be considered to be a network of distributed data centres which typically uses cloud computing technologies like virtualization, and offers some kind of interface for storing data.

Proxy Re-Encryption

We consider the problem of constructing an erasure code for storage over a network when the data sources are distributed in the cloud server. Specifically, we assume that there are n storagenodes with limited memory and k < n sources generating the data. We want a data collector, who can appear anywhere in the network for accessing the data, to query any k storage nodes and be able to retrieve the data.

Data forwarding over cloud

It is one of the advanced encryption model which works on both real system and virtual systems. This works more efficient on cloud systems. Proxy re- encryption schemes are cryptosystems which allow third- parties (proxies) to alter a cipher text which has been encrypted for one party, so that it may be decrypted by another. Proxy re-encryption schemes are traditional symmetric or asymmetric encryption schemes.

FUTURE WORK

In the proposed system, we propose a protocol based threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated. By using the threshold proxy re-encryption scheme, we present a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure. Storing data in a third party's cloud system causes serious concern on data confidentiality.

CONCLUSION

Thus we are concluding that all the result obtained according to the committed abstract. In this paper, we consider a cloud storage system consists of storage servers and key servers. We integrate a newly proposed threshold proxy re-encryption scheme and erasure codes over exponents. The threshold proxy re-encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way. To decrypt a message of k blocks that are encrypted and encoded ton code word symbols, each key server only has to partially decrypt two codeword symbols in our system.

REFERENCES

[1] R. Bhagwan, K. Tati, Y.-C. Cheng, S. Savage, and G.M. Voelker, "Total Recall: System Support for Automated Availability Management,"Proc. First Symp. Networked Systems Design and Implementation (NSDI),pp. 337-350, 2004.

[2] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Ubiqui-tous Access to Distributed Data in Large-Scale Sensor Net-works through Decentralized Erasure Codes,"Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN),pp. 111-117, 2005.

[3] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Decen-tralized Erasure Codes for Distributed Networked Storage," IEEE Trans. Information Theory, vol. 52, no. 6 pp. 2809-2816, June 2006.

[4] M. Mambo and E. Okamoto, "Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts," IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, vol. E80-A, no. 1, pp. 54-63, 1997.