SECURE CLOUD STORAGE FOR CONVENIENT DATA ARCHIVE OF SMART PHONES

Sue-Chen Hsueh[*1]*, Jing-Yan Lin*[1]*, and Ming-Yen Lin*[2]
[1]Dept. of Information Management, Chaoyang University of Technology, Taiwan (R.O.C.)
[2]Dept. of Information Engineering and Computer Science, Feng Chia University, Taiwan (R.O.C.)
{schsueh, s9914632} @cyut.edu.tw; linmy@fcu.edu.tw

ABSTRACT

The importance of the data stored in the smart phones is increased as more applications are deployed and executed. Once the smart phone is damaged or lost, the valuable information treasured in the device is lost altogether. If cloud storage can be integrated with cloud services for periodical data backup of a mobile client, the risk of data lost can be minimized. However, the important data might be uncovered by a malicious third party during retrieval or transmission of information using wireless cloud storage without proper authentication and protection. Therefore, in this paper, we design an archive mechanism that integrates cloud storage, hybrid cryptography, and digital signatures to provide security requirements for data storage of mobile phones. Our mechanism not only can avoid malicious attackers from illegal access but also can share desired information with targeted friends by distinct access rights.

1 INTRODUCTION

Clouds [1][3] are a very new and popular topic in the field of IT. Though this is not a new technology, it is a new concept: the main purpose of the original cloud is that "users can use the service anytime, anywhere through the Internet, directly through the browser." It is an extension of distributed computing through the Internet. A huge operation procedure is automatically split into several smaller operation procedures, processed by a number of extensive systems of the server, and the output finally goes through the search and operations to return to the user. This approach can handle thousands of processes like a "supercomputer." In fact, "cloud" refers to the "network," that is, the network of operational capability. The alternative is to install software or replace the data stored on the computer; because the cloud can use the desired browser for service, the data can be stored in virtual space. The user only needs to enter simple commands to use network services. In the future, smart phones and mobile devices would also be able to use cloud computing for more services.

As long as science and technology continue to advance, there will be information security issues. Clouds need security too, but they are a new concept, so no safety standard has actually been developed; each company is developing its own standards. Data security issues include data stored in a server; servers can be accessed through browsers to obtain internal information. If a hacker attacks many servers to steal information, data stored in the server's security is a concern. Management reliability refers to cloud security mechanisms to prevent security breaches. Protecting user privacy in clouds is the most important issue in the industry. If the cloud industry boasts of its own security mechanism as being safe and it is then broken, clouds will no longer be trusted by users. Clouds have the feature of enabling user access anywhere at any time. Before the development of many algorithms, distributed computing, and grid computing, we need to understand the underlying architecture and structure. We also require specific hardware and software facilities. Clouds do not need to understand the underlying structure; the user only needs browsers connected to the network with the required capabilities. Compared to before, traditional applications are expensive and complicated for both hardware and software. In addition, the number of processes that must be tested by experts, installed, and maintained is very large.

Mobile phones have become an integral part of life; mobile users store personal data on phones, such as contact lists, text messages, photos, and programs. Smart phones can perform many of the programs detailed above. Business owners keep schedules in the phone; although the information may not be important to other mobile users, it is important to the owner of the phone. If the phone is lost or damaged, or phone numbers are changed, the issue comes up of what to do with the data stored in the phone. In previous methods, mobile users would backup data inside a computer; in the event of data loss, they would retrieve the data from the computer and place it back into the phone memory. The same procedure would apply when phones are changed. Thus, the data are backed up despite actions, but this procedure is not very convenient: there is no means to update the data in real time. Remote backup is convenient to business owners; by referring to the phone number, they can plan their schedules and save important documents, which many people may find too complicated to back up on a computer. Moreover, if a phone is damaged or suddenly no longer working, there is no way to get data from other places. Clouds have to be accessible over the network. However, with the constant threats of attacks and tampering on the Internet, clouds do not have the best security protection, so users do not want to store data there owing to concerns

978-1-61284-842-6/11/$26.00 ©2011 IEEE

over tampering of transmissions of personal data. In addition to these issues, there have been information security incidents in the past as well as incidents of conspiracies to attack enterprises, which involve the loss of a lot more data than general attacks. In enterprise databases, there is a great deal of personal information; companies can easily extract member information and information about how other enterprises do business to get the maximum benefits.

Simply by using clouds, users can store personal data and back up actions. The cloud can also be used simply for personal data management and real-time updates. It can be used anytime and anywhere by users with mobile phones as a carrier. The biggest issue with mobile users keeping personal data in the cloud is security of the personal data. In this study, a method was developed by which mobile users register and share in a stage through the certification center to verify the signature of legitimate sources. Mobile users generate a random number that is passed along to telecommunication. The telecommunication returns random values to verify the transmission of the user registration information. The transmission process uses the hash function to verify whether the transmission was tampered with. If any tampering is found, the transmission is not performed. Trust is important among mobile users, telecommunication, and clouds, so the method generates a secret value that is only known to the three parties. If any party receives a message with no secret value, then no action is performed. Not a great deal of mobile user information is saved to prevent collusion attacks. In the telecommunication database, storage of personal data is encrypted, which also prevents attacks and internal staff theft. In each phase, encryption is done asymmetrically. The use of encryption methods, digital signature, hash function, random number, and secret value is to let users have peace of mind in a cloud environment.

The rest of this paper is organized as follows. Section 2 introduces the cloud data storage security; Section 3 is devoted to the structure of the system and the five stages. Section 4 presents the safety analysis, and Section 5 presents the conclusion.

2 RELATED WORK

Google Storage [4] for Developers offers a rich set of features and capabilities. The basic operations are as follows: (1) store and access data from anywhere on the Internet; (2) Range determination for large objects; and (3) manage metadata. Security and sharing have the following features: (1) user authentication using secret keys or a Google account; (2) authenticated downloads from a Web browser for Google account holders; (3) secure access using SSL; (4) easy and powerful sharing and collaboration via ACLs for individuals and groups. Performance and scalability have the following features: (1) strong data consistency (read-after-write consistency for all uploads and deletes operations); (2) name space for the user domain (only the user can create bucket URIs containing the domain name); and (3) data replicated in multiple data centers across the USA and within the same data center. Finally, the tools include (1) a Web-based storage manager; (2) GSUtil, which is an open-source command line tool; and (3) compatibility with many existing cloud storage tools and libraries.

With respect to functionality, Amazon S3 is intentionally built with a minimal feature set. It has the following features. (1) Write, read, and delete objects containing 1 byte to 5 terabytes of data each; the number of objects that can be stored is unlimited. (2) Each object is stored in a bucket and retrieved via a unique developer-assigned key. (3) A bucket can be stored in one of several regions. The user chooses a region to optimize latency, minimize costs, or address regulatory requirements. Amazon S3 is currently available in the US Standard, EU (Ireland), US West (Northern California), Asia Pacific (Singapore), and Asia Pacific (Tokyo) regions. The US Standard region automatically routes requests to facilities in northern Virginia or the Pacific Northwest by using network maps. (4) Objects stored in a region never leave the region unless transferred out by the user. For example, objects stored in the EU (Ireland) region never leave the EU. (5) Authentication mechanisms are provided to ensure that data are kept secure from unauthorized access. Objects can be made private or public, and rights can be granted to specific users. (6) Standards-based REST and SOAP interfaces are designed to work with any Internet-development toolkit. (7) It has flexibility so that a protocol or functional layers can be added easily. The default download protocol is HTTP. A BitTorrent™ protocol interface is provided to lower costs for high-scale distribution. (8) Amazon S3 is reliable and is backed with the Amazon S3 Service Level Agreement.

With respect to data protection, Amazon S3 provides a highly durable storage infrastructure designed for mission-critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. To help ensure durability, Amazon S3 PUT and COPY operations synchronously store data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired by using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Amazon S3 [5] provides further protection via Versioning. Versioning can be used to preserve, retrieve, and restore every version of every object stored in an Amazon S3 bucket. This allows a user to easily recover from both unintended actions and application failures. By default, requests retrieve the most recently written version. Older versions of an object can be retrieved by specifying a version in the request. Storage rates apply for every version stored.

Reduced redundancy storage (RRS) is a new storage option within Amazon S3 that enables customers to reduce their costs by storing noncritical, reproducible data at lower levels of redundancy than Amazon S3's standard

storage. It provides a cost-effective, highly available solution for distributing or sharing content that is durably stored elsewhere or for storing thumbnails, transcoded media, or other processed data that can be easily reproduced. The RRS option stores objects on multiple devices across multiple facilities, providing 400 times the durability of a typical disk drive, but it does not replicate objects as many times as standard Amazon S3 storage and thus is even more cost effective.

3 THE PROPOSED METHOD

3.1 Overall Framework

Data storage in the cloud is designed so that users can use mobile phones as a platform to upload, download, share, and synchronize information through cloud computing anywhere at any time. Security uses a combination of TPM chips in the mobile phones to protect the identity of mobile users as well as security technology to protect data transmissions from malicious attacks and tampering for data integrity.

For registration, synchronization, and sharing, the identity of mobile users is also protected through third-party certification. A certification center confirms the source of a signature; the user must confirm the legality of the source operation. After legal user authentication, the center allows data transmission to the destination.

The system architecture consists of mobile users, an authentication center, telecommunication, and cloud form. The tasks are divided into registration, upload, download, sharing, and synchronization processes. The roles of the components for the main tasks are presented in Table 1.

Table 1. Roles

Role	Mission
Mobile User	Upload, download, sharing, and synchronization
Certificate Authority	Authentication source
Telecommunication	Generated cloud password, store user information action
Cloud	Storage mobile user personal data

As shown in Fig. 1, mobile users use mobile phones to access the Internet and then send registration information to the authentication center, which is subsequently passed on to the signature telecommunication. The telecommunication sends a cloud password back to the mobile user to complete the registration operation. Mobile users can use the password to upload and download the cloud. Cloud data storage can also be synchronized with other mobile phones and shared with friends.

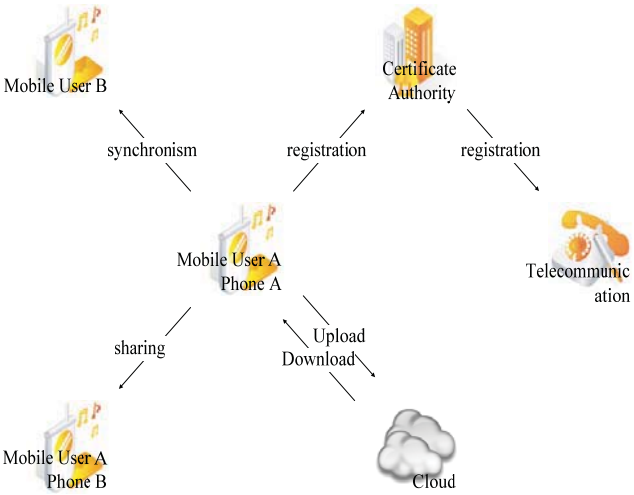

Figure 1. The Framework

3.2 Five Stages of the Method

For mobile users to use the cloud, the process can be divided into five steps: registration, upload, download, sync, and sharing. Next, the procedure for each of these steps is detailed. Table 2 lists the notations used in the paper.

Table 2. Notations used in the paper

Symbol	Description
MU*x*	Mobile User
NO*x*	Phone Number
TE	Telecommunication
CA	Certificate Authority
Un	Random Number
CPW	Cloud Service Password
SV	Secret Value
TK	NO&CPW Random
h(k)	Hash Function
S*x*(k)	*x* 's Signature
PK*x*	*x* 's Public Key
SK*x*	*x* 's Secret Key
SEK	Session Key

Registration stage (Fig. 2)

Step 1: Mobile users send information to the authentication center.

MU➔CA: E_{PKTE} (MU, NO, TK), Un, S_{SKMU}(h(MU, NO)), h(MU, NO), Apply

Transmission of information containing the mobile user's name, number, and password makes use of the private signature, which contains the hash function. The user authentication center uses the signature to determine the legitimacy of the action, transmits registration messages after Apply, and uses a random number for proof of the identity of the mobile user.

Step 2: Certification center receives information that is passed to telecommunication.

CA➔TE: E_{PKTE} (MU, NO, TK), Un, S_{SKCA}(h(MU, NO)), Apply

The certification action user receives the information. Authentication information is first considered for whether to turn the data over. The hash function is used for validation; if it is correct, the certification center's private signature is then validated to

recognize that the information is legal. The data are then transmitted from five telecommunications to a trusted third party.

Step 3: Telecommunication receives registration information to generate a CPW.

TE: E_{PKMU} (MU, NO, Un, E_{TK}(CPW))

The telecommunication receives registration information to generate a CPW. The registration information in the TK is then used to encrypt the CPW, which is stored in the telecommunication database. In addition to the CPW, the database also stores the user action name for later authentication. After execution, the telecommunication returns to pass information to the mobile users after receiving proof of the registration messages. It also passes on the mobile user's public key encryption, including the name and number of the mobile user. The mobile user has random numbers; the information is proved to be that of the mobile user with the use of TK encryption for the CPW.

Step 4: Authentication center switches to pass on to the mobile user:

CA➔ MU: E_{PKMU} (MU, NO, Un, E_{TK}(CPW)).

Step 5: Action to complete the registration the user receives the message including MU, NO and CPW.

Telecommunication receives the information returned to the mobile user. The SIM card stores the name, number, and CPW. The CPW provides the user with the TPM's [2] public key encryption, which is passed on to the mobile phone in the TPM chip.

Step 6: Stored in phone memory.

The information is stored in the phone memory CPW, since mobile users use the cloud. The password is simply extracted from memory and then decrypted through the TPM chip for use.

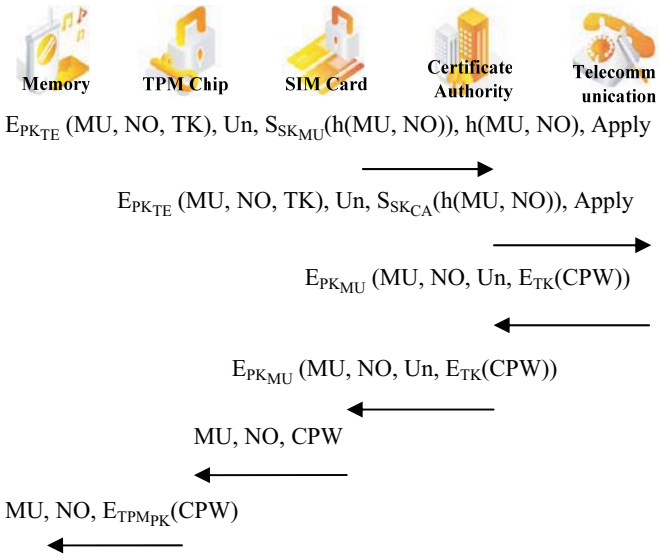

Figure 2. Registration

Upload stage (Fig. 3)

Step 1: Mobile user uploads data.

MU➔Cloud: CPW, MU, E_{SEK}(Data), S_{MU}(h(MU||SV|| E_{SEK}(Data))

A message including the CPW, name, and upload data is sent to upload the data encrypted with the session key. Mobile users use their own private key signature to get information from the cloud. This verifies the correctness of information sources and validates the data stored in the cloud.

Figure 3. Upload

Download stage (Fig. 4)

Step 1: Mobile users send download information including CPW, MU and h(MU||SV).

Information contains the CPW and mobile user name. This also includes the hash function. In this way, the cloud can verify that the source of the mobile user is correct and whether the transmission process was tampered with.

Step 2: Return the user's personal data (E_{SEK}(Data), h(E_{SEK}(Data||SV))to the cloud.

If the information source is not validated as correct and tampering is found, the cloud returns the mobile user's personal data.

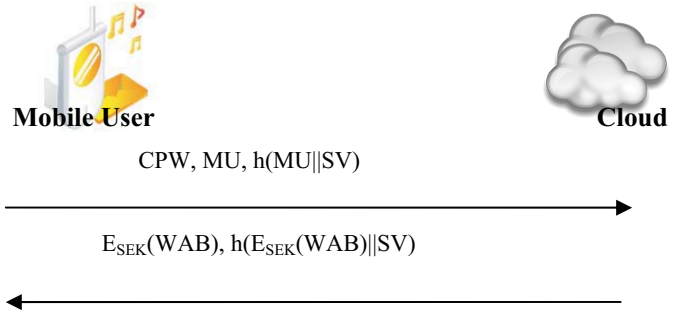

Figure 4. Download

Synchronism stage (Fig. 5)

Step 1: Mobile user uses phone A to upload data.

CPW, MU, E_{SEK}(WAB), S_{SKMU}(h(E_{SEK}(WAB)||MU||SV))

Step 2: Mobile user uses phone B to access the cloud. S_{SKMU}(MU, TK), h(MU||SV)

The mobile user uses phone B to access the cloud. The mobile phone user's name and TK are used as the user's signature, and the SV hash function is used to verify the identity of the mobile user.

Step 3: Cloud passes a message to telecommunication.

Cloud➔TE: MU, TK, h(MU||TK||SV)

The cloud receives the message from the mobile user using phone B and verifies the mobile user's hash function. If correct, the cloud follows the action coming from the user name. The name and TK are passed to telecommunication; telecommunication then follows the name and TK to pass the CPW to the mobile user.

Step 4: Telecommunication passes CPW to mobile user.
TE➔MU: E_{PKMU}(CPW)

Telecommunication uses the TK from the cloud to unlock mobile users existing before the CPW database password. The mobile user's public key is then passed to mobile users to allow them easy access to the cloud.

Step 5: Mobile user receives the CPW and stores the CPW, MU and h(MU||SV) in the phone B memory, and accesses the cloud again.

Step 6: Allow access to cloud and the cloud checks the CPW.

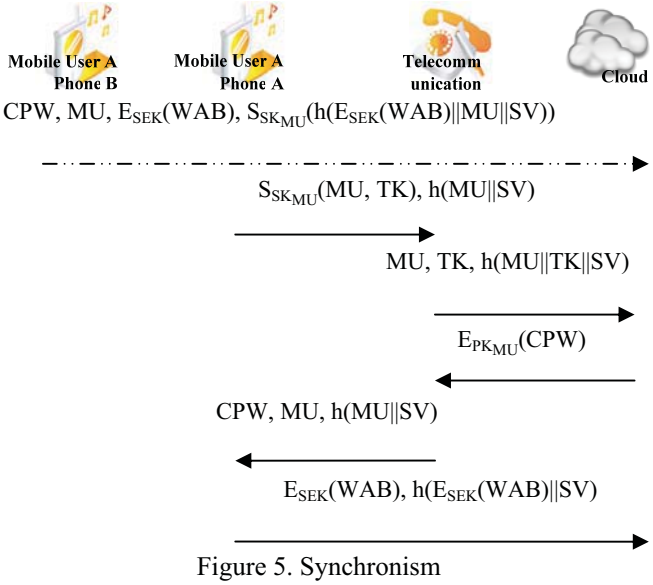

Figure 5. Synchronism

Sharing stage (Fig. 6)

Step 1: Requirements of mobile user B to share data
E_{PKMU} (MU_B, NO_B), Un, S_{SKMU}(h(MU_B, NO_B)), h(MU_B, NO_B), Share

If mobile user B wants mobile user A's personal data, B sends a message to A. The message must contain the name and number of the mobile user B so that mobile user A knows who it is. The random number and pass certification center's private signature allow two mobile users of a trusted third party to transmit this record for a combined sharing action.

Step 2: CA verifies the signature.
E_{PKMU}(MU_B, NO_B), Un, S_{SKCA}(h(MU_B, NO_B)), h(MU_B, NO_B), Share

CA verifies mobile user B and whether data were tampered with during transit. If not, the certification center uses the certification center's private signature key to pass on information to mobile user A.

Step 3: Mobile user A authenticates mobile user B
E_{PKMUB}(MU, NO, Un, SEK, CPW)

Mobile user A passed the message to the authentication center. If mobile user B is known, mobile user A's name, number, session key, and CPW are passed to mobile user B together with a random number. B confirms the action has been sent to A.

Step 4: Transmission of intact certification center.
E_{PKMUB}(MU, NO, Un, SEK, CPW)

Step 5: Mobile user B to access cloud.
S_{SKMUB}(CPW, MU, NO)

Mobile user B receives the message of mobile user A and uses the signature, private key of the CPW, and mobile user A's name and number to visit the cloud. However, at this stage, mobile user B cannot download the individual action data for mobile user A.

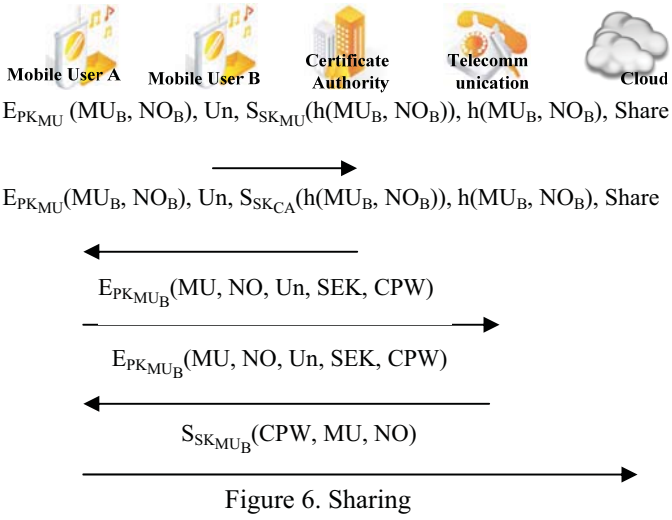

Figure 6. Sharing

4 SECURITY ANALYSIS

In this section, three aspects to the narrative are discussed: conspiracy, not credible, and attacks.

Conspiracy: A conspiracy between enterprises in order to earn more interest would violate the moral conscience. A member of the database may sell information to other companies to earn fees. Collusion between two companies may occur: the members leak information and jointly deceive users, who are unaware of what is happening. To prevent this, in the proposed method, the authentication center, telecommunication, and cloud do not store too much personal information. Instead, the information is stored in the enterprise and encryption technology is used for ciphertext, which lets businesses transmit information only to real members, as all ciphertext is protected.

Not credible: Irrespective of the circumstances, when a message or mail is received, the credibility of the source will be doubted with a security breach. In the method, a certified center is used to confirm the identity of the source in addition to multi-layer protection as well as achieve non-repudiation. Digital signature technology can confirm the identity. This way, only digital signatures from the sender using the receiver's public key can be used to open a message. Without the sender's private key, the message cannot be opened.

Attack: In the Internet, users can be attacked everywhere. As long as the Internet is accessed to send a message, the message transmission is subject to attack. In the method, the existence of personal data in the cloud must be through the Internet. An attacker may be present, but in this method, the transmission is encrypted asymmetrically. The transfer also includes one-way hash functions that are

encrypted and cannot be decrypted by only an action without verification.

5 CONCLUSION

In the study, we used some very simple security technology. During transmission, each character is recognized by using the hash function to determine whether the transfer was deliberately tampered with during the process. Communication between mobile users uses a random number, so that parties can be recognized. A message for mobile users is verified by a trusted third-party certificate authority. Messages can be transmitted with more layers of protection. If a user does not admit to sending or receiving messages, the recovery of information can be checked at the certification center. The digital signature can also be used to recognize legal status. In each role, data are not stored to the database, as internal staff may take it for illegal purposes. Not storing the data also reduces the opportunities for internal attackers. To handle external attackers, the encryption method is asymmetric. Personal data are stored into the clouds so that the text is stored in secret with the hash function used for validation. A disposable lost session key is encrypted into the cloud. This is different for every upload, so it is difficult for an attacker to break.

6 ACKNOWLEDGEMENTS

This work was supported partially by the National Science Council, Taiwan under grant NSC 99-2410-H-324-010.

7 REFERENCES

[1] Rimal, B.P., Eunmi Choi and Lumb, I. “A Taxonomy and Survey of Cloud Computing Systems”. *International Joint Conference on INC, IMS and IDC*, Seoul, pages 44-51. Aug, 2009.

[2] Nuno Santos, Krishna P. Gummadi, Rodrigo Rodrigues, “Towards Trusted Cloud Computing”, International Conference on *Hot topics in cloud computing,* pages 3-3, 2009.

[3] Grossman, R.L., “The Case for Cloud Computing”, *International Conference on IT Professional*, page 23-27, March-April, 2009.

[4] Google Storage for Developers: http://code.google.com/intl/zh-TW/apis/storage/docs/overview.html

[5] Amazon Simple Storage Service: http://aws.amazon.com/s3/