Indian Journal of Science and Technology, Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/102544, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Secure and Efficient Authentication Protocol on Cloud: Survey

Sunghyuck Hong*

Division of Information and Communication, Baekseok University, Cheonan, Chungnam, 33065, Korea; sunghyuck.hong@gmail.com

Abstract

Objectives: The purpose of this study is to improve authentication protocol on Cloud. **Methods/Statistical Analysis**: The use of authentication and access control technology authorized users only and is limited to random replicates data by providing secure area, to initialize the data stored upon a certain number of password errors for the loss in data protection that recovery is impossible or location. **Findings**: Cloud computing service is popular and ongoing developing project for the future computer network, which data possessors can remotely saveits data on the cloud storage to use on demand high-resolution based on service and applications from the common pool of configuration and computational H/W and S/W resources. Therefore, security argument is only argued heuristically in the typical model. **Improvements/Applications:** The proposal is the first publicly making sure secure cloud storage protocol in the standard model whereas the previous work is not enough security.

Keywords: Access Control, Authentication, Cloud Storage, User Behavior

1. Introduction

Cloud computing service has been progressed as the next-generation architecture of the IT enterprise due to its long list of unprecedented advantages in IT: rapid resource elasticity, location-independent resource pooling, on-demandself-service, ubiquitous network access, usage-based pricing, and transference of jeopardizing[1,2]. One basic type is which data is being centralized and outsourced into the Cloud environment. However, the current shared storage solutions for team collaboration applications are very far from satisfaction. Some of the solutions rely on self-built storage infrastructure, which is becoming a big issue, especially for these small or medium companies. Cloud storage is not a concept of a specific device having a storage nature, a hierarchical structure in the environment provided by the cloud service provider. Next to the advent of Web 2.0 and user participation in the center with a fast growing network of web 3.0 is a core component of large amounts of data storage and processing in the cloud computing era[3,4]. Google, Youtube, and share photos, videos, documents, etc. from heterogeneous devices tablets and smart phones using the cloud storage in large vendors such as Facebook, and easy Fa correctly over the bulk network transfer of data stored It approached the data. It has been emerging as a business model, cloud storage data with the growth and development in the world[5,6]. Cloud storage has to offer cloud storage services at low cost, availability, scalability, and security services to the new concept of network storage. EX, Asana allows-cloud users to share their files with their team from Naver N-Drive, Google Drive, or Dropbox, but this method is not efficient for their team co-work, and not enough security[7]. Infrastructure cloud services (IaaS: Infrastructure as a Service):the user operation processing is receiving provision of storage, the net Manage basic computing resources such as work directly, Apple can be controlled from the application to the operating system. Nature Lamb cloud services are provided in a variety of forms, respectively. The different range of security should be taken into account for each service. It apart from use neck and cloud service model depending enemy, it can be divided in the

*Author for correspondence

following manner. International cloud providers such as IBM, Amazon, HP, NetApp, and EMC are a cloud storage service as well. Also, GFS, HDFS, EMC Atoms, Amazon S3, HP Up line, Data ONTAP, Cloud NAS, a trend that will increase a lot like FilebStore cloud storage platform. These various cloud storage platforms to standardize it for SNIA (Storage Network Industry Association) in 2009 cloud users, service providers, developers, etc. 140 more companies and with the cloud service standards CDMI (Cloud Data Management Interface)[8]. Cloud storage is the same as the structure and hierarchical structure of cloud services based on cloud computing environment. The configuration of this system is as shown in Figure 1. Software as a service (SaaS) cloud services cloud, users can access via the Internet to use the software required to use the application software layer.Also, Platform as a service (PaaS) is API interface and storage management and storage virtualization to the configured hierarchy. Infrastructure as a service(IaaS) is provided to the server, and allow users use for the hardware resources, and the server[9,10].Data Storage as a Service(DaaS) is a well-known cloud storage system architecture as data storage to configure storage service interface from data extraction, or transmission by existing cloud users with various service functions to provide. This service is an example of CIFS or NFS, sometimes using the existing standard protocols, such as WebDAV.A cloud storage based middleware system is consist of tons of storage hardware cluster furnace with a network connection to a distributed file system provides a cloud service to the users and, SLA (Service Level Agreement), distributed file system, resource resources, the network device a containing structure. To provide the user with a more compatible function and physical interaction, yet it must provide logical functions.

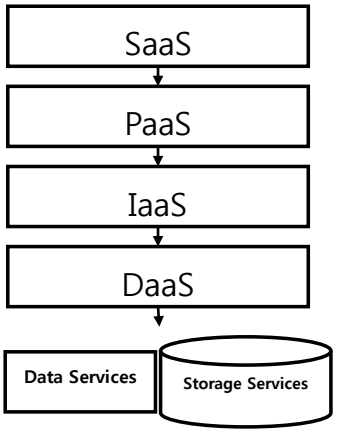

Figure 1. Cloud storage system structure.

1.1 Cloud Storage System

Cloud storage is a large-scale expansion of storage resources to the beginning of the storage technology, Network Attached Storage (NAS) or a Storage Area Network (SAN) using such storage-based virtualization technology according to the user's request is a function, and without regard to a specific geographic location. It should have flexible features to the application. In particular, to be capable of expansion in a large scale, it can be mentioned NAS cluster (Clustered NAS) using multiple servers at the same time a wide distributed file system that runs on a conventional NAS structure typical example. NAS cluster will disperse data and metadata (Metadata) to the cluster nodes or storage; the core technology is a distributed file system that is used at this time. When it comes to the core conclusion of the current cloud storage technology, it can be seen as a distributed file system. Cloud storage-related technologies can be categorized as commercial software. Open source software and technology are Hadoop (Hadoop), Article cluster FS, Swift (Swift, Open Stack Object Storage), etc., and commercial software from IBM SoFA (Scale-out File Services) such as SoFS for including EMC, Microsoft, Hitachi Data System(HDS), etc. There is a linear extend support to Scale-out approach and unified storage (Unified storage) approach to cloud storage market targeting[11]. Hadoop is an open-type software-based framework that services distributed software running on the clustercapacity computer that can handle a large volume of material[12–14]. Hadoop was initiated based on the MapReduce (MapReduce) and GFS (Google File System), Google (Google). Hadoop is currently being operated as a sub-project of Apache (Apache), consists of a large Hadoop kernel (Kernel), MapReduce, HDFS 3 different areas: Hadoop is being established in Java, and it has a connection with the other projects, including the Apache-based Hive, Hbase, Zookeeper. Hadoop is for public cloud has the largest number of sub-projects during storage technologies, the most widely used high scalability, providing a variety of functions including, and being used as a base technology for commercial companies. When organized a project associated with the Hadoop as follows in Table 1[14–16].

1.2 Cloud Authentication System

Founded as a nonprofit organization for Cloud Security in December 2008, CSA is committed to a cloud service security the most active in the world. As part of this effort,

Table1. Hadoop sub-project

Project name	Contents
Hbase	As a distributed column-oriented (Column-Oriented) database uses the HDFS storage. It supports both the batch method and the calculation method of the random read is possible query point using the MapReduce.
Zookeeper	Provides a distributed lock (Distributed Lock) such primitives (Primitive) that can be used as a high availability Adjustments (Highly available coordination) services to multiple computers distributed processing to build distributed applications.
Hive	First proposed in the Facebook open source data warehousing solutions based on Hadoop. As well as a web interface that provides a simple query configuration capability and provides a query language similar to SQL. Hive is available to provide ad hoc (ad-hoc, informal) The biggest problem with easy-to-use features that provide a query interface, if not professional developers what if some familiarity with SQL.
Chukwa	Performing a collector (Collector) for storing data to HDFS a distributed data acquisition and analysis system, and using the MapReduce to generate a report.
HDFS	A distributed file system is carried out in a large cluster of general purpose computers.
Pig	Developed by Yahoo, Hadoop is underway as part of the current project. Pigs project provides advanced language Pig Latin (Pig Latin) for the operation of Hadoop and Map Reduce. This has become an easy means of access than developers are accustomed to manipulating data using SQL. Also, as well as the Java API, it provides an interactor tee bracket (Interactive) interface. Pigs can be used even in Hbase and Cassandra databases.
MapReduce	An execution environment and a distributed data processing model are carried out in a large cluster of general purpose computers.
Avro	Cross-Language (Cross-Language) is a data serialization system for RPC and permanent data storage.
Core	It provides devices and interfaces for the distributed file based systems and common Input / Output.

it has been presented to the authentication framework of the three steps is as shown in Figure 2. Step 1 is to release on September 1, 2011 by Consensus Assessment Initiative Questionnaire (CAIQ) v1.1[17]. September 26, 2013 release by Cloud Control Matrix (CCM) v3.0[17].It is to enable a self-assessment, Two steps that cloud services are satisfied with the CCM, ISO27001, AICPA SOC2 third party and authenticating three steps cloud services are in compliance with compliance, security, privacy, integrity, and operational security.If you check to see whether the evidence provides the Cloud Trust Protocol (CTP) and to guarantee that it is well-run[18–20]. In the first stage, which utilizes CAIQ, CCM is both April 2009 and published in 2011 by the release of v3.0 SGCAFCC (Security Guidance for Critical Areas of Focus Cloud Computing) (one people "Security Guidance")21. It was madeby the basis. Security Guidance includes the contents composed of 14 domains (domain) as shown in Table 1 in detail for each domain. In other words, the contents of CAIQ and CCM can be said to be similar standing, there as most of the Security Guidance details the scale and detail. It called framework that can guarantee reliability in the sense that soon covers the contents in detail, as well as all aspects of security can do. To receive the two-factor authentication, it complies with the CCM and the ISO27001 or SOC2 which is reflected because the British Standards Institute (British Standardization Institute, BSI) and authentication with cooperation. Confirm the details on the overall security can be seen given that assurance. It is an addition to meet the SOC2 that cloud services can provide very strong security authentication service because it also means that must be satisfied in IT and information security audit by the SOX Act[22–24]. The European Union (EU) in the security in respect of each State of the gateway and while overall[25].It became the European Union began to apply it based on the cloud service. ENISA published by the Cloud Computing Information Assurance Framework at the same time the Directive was presentedon the basis of a framework of governance for the private sector. And private companies are service level agreements (Service Level Agreement) to be able to make 41 questions consisting survey and analysis of security variables in cloud. Among the sources of Cloud Computing Risk Assessment is a risk (threat) policy and organizational risks (policy and organizational risks) 7 dogs, technical risks (technical risks) 13 dogs, legal risk (legal risks) 4 Dog, Cloud specialization,

but it is not a general security risk classification 11 total, including 35 dogs and vulnerabilities are also classified and presented 53 pieces total. East Guide is published to help cloud service providers to be used as a means for obtaining authentication. It can be said that in the data published by the ENISA as described above by presenting a list of risk and vulnerability to security and reflects the content enough to consider fully when assessing the risks of the asset.

2. Proposed Model

By applying security to USB and studies, it has been conducted for data loss prevention and evaluate the technology trends for the market to market. By default, the USB security for technology is divided to the authentication and access control techniques and data encryption and decryption techniques. The fingerprint authentication is allowed access to the USB only when authenticated by the user's fingerprint. Image drive method using a virtual image drive and provides a secure area drive only when the user authentication. The reserved area utilization method provides access to the secure area after the user authentication in the same manner and utilizing the reserved area in the file system. However, this system is difficult to realize the cost is excessive. Are classified as data encryption and decryption technique in hardware manner and a software manner, the hardware manner, and using a separate dedicated chip decryption module, using the PUF was introduced additionally to protect the secret key system as well. My way software takes advantage of the USB software programs and real-time encryption method has the On-The-Fly Encryption (OTFE) with optional file encryption methods[26]. OTFE is performed by creating virtual encrypted disk encrypted disk partitions or the entire region. Selective file encryption method is a method for performing an encryption multiple

Figure 2. CSA open certification framework.

files or specific file according to a user's selection[26]. Security USB provides additional functions using an authentication and access control techniques and data encryption and decryption techniques. The use of authentication and access control technology for authorized users only is limited to random replicates data by providing secure area to initialize the data stored upon a certain number of password errors. For the loss in data protection, recovery is impossible, and location (IP address, etc.) also provides the ability to delete the data when it is connected in the other position through the track.In addition, USB security management system provides a systematic management via the management server to the built-in USB memory Agent program[27]. But also it appeared to circumvent the security mechanism of USB. For the physical method password has been exposed in plain text in the resulting access control program and the communication process by sniffing the contents to communicate with the USB drive, removing the flash memory portion.In recent years, it reverses the image file encryption when encrypting and decrypting a software-based through engineering analysis to extract the master key to decrypt the header of the image file has been found that this vulnerability can restore data. Such vulnerabilityare analyzed the access control program for the secure USB drive to combat and developed in Next, consider the vulnerabilities password exposure on existing as a system to manage the research, the secure USB register with the management server has been progressing on security USB management system to manage systematically the security features of the secure USB using secure encryption algorithms was applied to compensate. Recently, to work with data in a separate virtual space by applying the desktop virtualization technology, the data is impossible is another area in the virtual space. This research proposed two channel authentication with something you have a method. Username and password is something you know the method, and this is still popular. Table 2 shows the definition of notations and the configuration of proposed model is as shown in Figure 3. When user logins to Cloud server, then he/she enters his/her username and password with USB unique identification which is already registered in authentication server database. Once their credentials and PUF (Physical Unclonable Function) USB ID pass match with the registered one in the database, authentication server will notify and start a secure communication with User Pub and User Pri. Therefore, two-channel authentication can reduce the risk of single point of failure, and it can improve security on Cloud storage system.

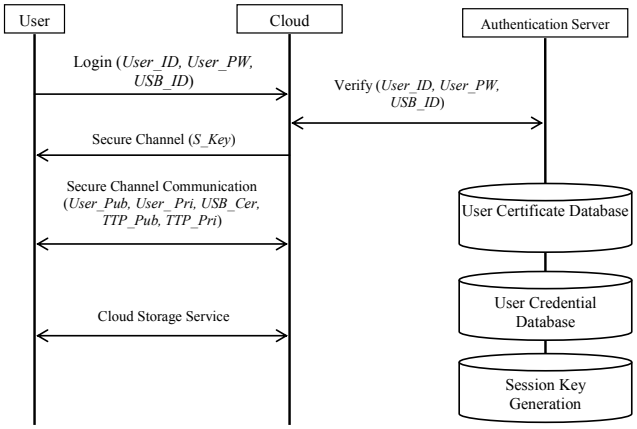

Figure 3. Proposed model system configuration.

Table 2. Definitions

User_ID	User's identification
User_PW	User's password
USB_ID	USB's identification with unique
User_Pub	User's public key
User_ Pri	User's private key
USB_Cer	Certificate in USB with Trust Third Party (TTP) Authorized
TTP_Pub	TTP's public key
TTP_Pri	TTP's private key
S_Key	Session key

3. Conclusion

Cloud computing, development, and Amazon of computing technology, theengaged strategic investment strategy of global companies such as Google and rapidly spread, has been attracting attention in the next generation of thecomputing environment.Types also vary from the storage service of a simple file to the remote desktop type of service, utilization of cloud computing is expected to increase further. As a result, the correspondence is urgently needed to the security vulnerabilities that cloud computing is inherent. In this paper, we tried to analyze against the threat of the possibility of security that occurs in the cloud computing environment, the integrity of the data that has been loaded into the cloud, confidentiality, technology and the cloud to ensure such availability. We discussed the research trends to ensure the reliability of the system itself. Cloud services have already reached the commercialization stage, prepared for the security is still unsatisfactory state.Prepared countermeasures against security threats are problems of cloud computing, if it is possible to construct a system reliability, high computing services reliable user in a simple low cost it is expected to position as a true next generation computing techniques that can be utilized.

4. Acknowledgement

This research is supported by 2016 Baekseok Research fund.

5. References

1. Wang C, Ren K, Lou W, Li J. Toward publicly auditable secure cloud data storage services.IEEE Network. 2010 Jul–Aug;24(4):19–24.
2. Ning K, Zhou Z,Zhang LJ. Leverage personal cloud storage services to provide shared storage for team collaboration. IEEE International Conference on Services Computing; 2014. p. 613–20.
3. Above the clouds: A Berkeley view of cloud computing[Internet]. [cited 2009 Feb 10]. Available from:https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.
4. Burton J, Kaliski S. PORs: Proofs Of Retrievability for large files. *CCS '07 Proceedings of the 14th ACM conference on Computer and communications security;*2007 Oct. p. 584–97.
5. Secure cloud computing architecture on mobile internet [Internet]. [cited 2011 Aug 08]. Available from:http://ieeexplore.ieee.org/document/6010435/.
6. Robison S. A bright future in the cloud. Financial Times; 2008 Mar.
7. Ateniese G. Provable data possession at untrusted stores. *CCS '07 Proceedings of the 14th ACM conference on Computer and Communications Security;*2007. p. 598–609.
8. Rivest RL, Shamir A, Tauman Y. How to leak a secret?*Springer Berlin Heidelberg; 2001 Dec. p.552–65.*
9. Lindell Y. Anonymous authentication. Journal of Privacy and Confidentiality. 2010; 2(2):35–63.
10. Slamanig D. Anonymous authentication from public-key encryption revisited. *Springer Berlin Heidelberg*; 2011 Oct. p. 247–9.
11. Shuai Z, Shufen Z, Xuebin C. Cloud computing research and development trend. ICFN '10 Proceedings of the 2010 Second International Conference on Future Networks; 2010. p. 93–7.
12. Liping H, Lei S. Research on trust model of pki. International Conference onIntelligent Computation Technology and Automation (ICICTA), Shenzhen:Guangdong; 2011. p. 232–5.

13. Li W, Ping L. Trust model to enhance security and interoperability of cloud environment. *Springer Berlin Heidelberg*;2009 Dec. p. 69–79.
14. OpezMill GL, Perez MG, Perez MG, Skarmeta AFG. Pki-based trust management in inter-domain scenarios. Computers and Security. 2010 Mar; 29(2):278–90.
15. Afzal M, Hussain M, Ahmad M, Anwar Z. Trusted framework for health information exchange. Frontiers of Information Technology (FIT), Islamabad; 2011. p. 308–13.
16. Zhang N, Shi Q, Merabti M. Anonymous public-key certificates for anonymous and fair document exchange.IEE Proceedings-Communications. 2000 Dec;147(6):345–50.
17. Cloud Security Alliance[Internet]. [cited 2016 Jun 02]. Available from: https://en.wikipedia.org/wiki/Cloud_Security_Alliance.
18. ENISA.Cloud Computing Benefits, risks and recommendations for information security[Internet]. [cited 2012 Dec 08]. Available from:https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security.
19. Lee SH, Lee IY.A study on security solution for USB flashes drive. Journal of Korea Multimedia Society, (KMMS). 2010 Jan; 13(1):93–101.
20. Study on the security solutions of USB memory[Internet]. [cited 2009 Dec 20]. Available from:http://ieeexplore.ieee.org/document/5405671/.
21. Research on storage virtualization structure in cloud storage environment[Internet]. [cited 2010 Oct 29]. Available from:http://ieeexplore.ieee.org/document/5630956/.
22. Han M. Trends for security techniques of USB and products (Translated). IITA Weekly Technology Trends. 2009 Jan;1380(1380):14–20.
23. LEE H, *Park C, Lee G, Kim K, Lee S*. An analysis on secure USB at the point of forensic view (Translated). Proceeding of Korean Society Broadcast Engineering (KSOBE) Conference; 2008 Feb. p. 63–5.
24. Christensen CM. The innovator's dilemma: The revolutionary book that will change the way you do business. *HarperBusiness, Reprint (edn)*;2011 Oct.
25. Park JS, Bae YM, Jung SJ. Technical analysis of cloud storage for cloud computing.The Korea Institute of Information and Communication Engineering. 2013 May;17(5):1129–37.
26. Hong S.Multi-factor user authentication on group communication. Indian Journal of Science and Technology. 2015 Jul; 8(15):1–6.
27. Hong S.Hybrid routing algorithm on mesh network based on traffic records. Indian Journal of Science and Technology. 2015 Apr; 8(7):327–31.