Design of StraaS (Streaming as a Service) based on Cloud Computing

Byung-Rae Cha[1], Soo-Bong Park[2] and Yoo-Kang Ji[3]

[1]SCENT Center GIST
[2]Dept. of Information & Communication Eng. DognShin Univ.
[3][Corresponding Author] Dept. of Information & Communication Eng. DongShin Univ.

[1]brcha@nm.gist.ac.kr, [2]sbpark@dsu.ac.kr, [3]neobacje@gmail.com

Abstract

In this paper, we define and design the Streaming service based on cloud computing. And we describe the various function and security function to StraaS service. Specially, we introduce KS-MMA and SIES as security function for streaming service and cloud computing.

Keywords: *Streaming, StraaS, Cloud Computing*

1. Introduction

The recent IT issues include Cloud Computing and Big Data, and the Industry-University-Institute collaborations are actively going on. Cloud Computing has risen as new paradigm in computing environment area, and Big Data has become a new issue by active social networking. The services over these two areas are just the streaming service. Many problems related to Big Data are newly emerging by the streaming service and for solving these problems we would design the streaming service based on Cloud Computing.

This research sets the goal on the StraaS design supporting the streaming service based on the Cloud Computing. The searchable code system is the technique which can make search data without decoding of encoded data. The searchable code systems have researched as the solution of problems appearing when personal information stored in exterior spaces

Recently reported personal information leaks like customer information disclosure of the company database and personal photos in individual homepages, the security about the data stored in exterior spaces becomes an issue. The security concern in exterior spaces differs from the past when people managed their own data using personal separated storage space. It’s because basically the data owner and the storage manager are separated. The access control and the key management systems mainly used for data protection in the database are good for blocking foreign invaders. Though they fundamentally can’t protect stored data from reading by the owner of the storage.

Chapter 2 describes relative studies about Big Data, Cloud Computing and Scale out. Chapter 3 designs StraaS service based on Cloud Computing, Chapter 4 describes the security of StraaS service, and Chapter 5 applications and business models of StraaS, and the brief conclusion.

2. Related Work

2.1. Big Data

There are many forms and requirements of Big Data in each company, and the computing environments diversified accordingly. Especially in the aspect of storage, not only saving data but also systematic interworking between various computing environments are the key factor deciding entire computing environments. Figure 1 shows 3 components of Big Data, Volume, Velocity, and Various. "Big Data: The next frontier for innovation, competition, and productivity” of McKinsey [1] describes monthly 30 billion contents are shared through Facebook, and IT expenses have increased 5%. It also includes that Big Data can give 330 billion dollars value production possibility in the area of USA medicine (more than twice of medical expenses of Spain yearly), and 250 billion euro reduction in European public service area (the amount of GDP for Greece), and in USA until 2018 140~190 thousand analysis specialists and 1.5 million data administers can be needed.

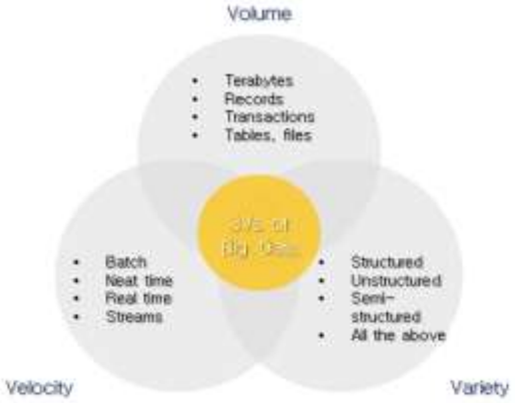


Figure 1. 3 Components of Big Data

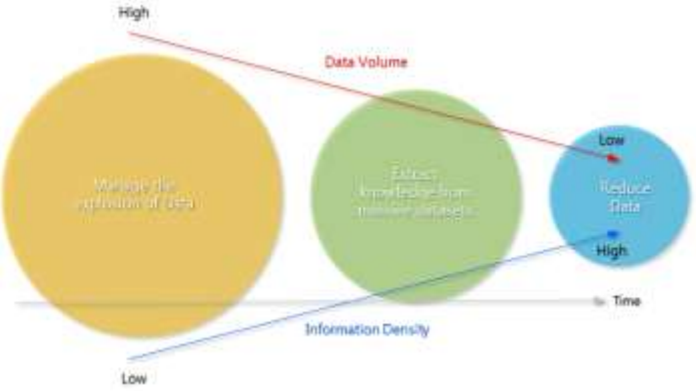
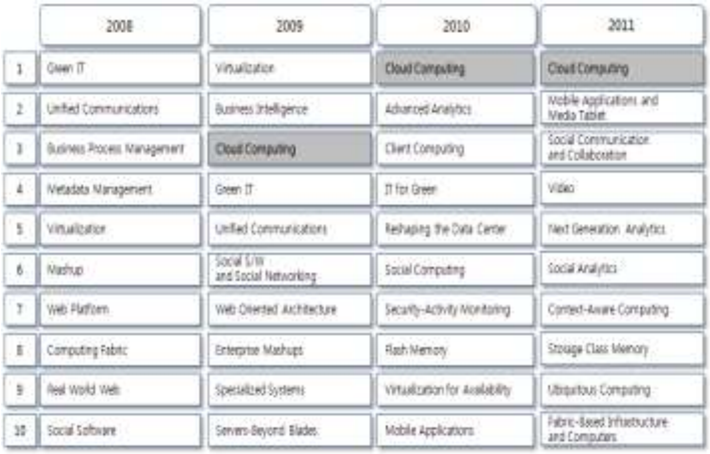


Figure 2. Value Creation of Big Data

Every field related to Big Data can give effective conjugation of Big Data and value creation. Especially the solutions like Hadoop, MapReduce can solve complexity problems of Big Data. As shown in Figure 2 abundant computing resources of Cloud Computing system and scaling of network can make real time analysis of Big Data and develop the infrastructure for the new value creation. Existing wire and wireless network and frequency management also need diverse techniques for handling complicated and various Big Data.

2.2. Cloud Computing Paradigm

Every year Gartner [2] group announces 10 strategy techniques of next year, and the most potential strategy technique for next 3 years. The recent trend is shown in Figure 3.



	2008	2009	2010	2011
1	Green IT	Virtualization	Cloud Computing	Cloud Computing
2	Unified Communications	Business Intelligence	Advanced Analytics	Mobile Applications and Media Tablet
3	Business Process Management	Cloud Computing	Client Computing	Social Communication and Collaboration
4	Metadata Management	Green IT	IT for Green	Video
5	Virtualization	Unified Communications	Reshaping the Data Center	Next Generation Analytics
6	Mashup	Social S/W and Social Networking	Social Computing	Social Analytics
7	Web Platform	Web Oriented Architecture	Security-Activity Monitoring	Context-Aware Computing
8	Computing Fabric	Enterprise Mashups	Flash Memory	Storage Class Memory
9	Real World Web	Specialized Systems	Virtualization for Availability	Ubiquitous Computing
10	Social Software	Servers-Beyond Blades	Mobile Applications	Fabric-Based Infrastructure and Computers

Figure 3. Value Creation of Big Data

Cloud computing is the computing environment that virtualizes and integrates computer resources and is assigned resources as much as user need be and then makes share data easily.

The emergence of cloud service is basically changing the IT economics again. By the standardization and integration of IT resources the cloud techniques make many manual works automated.

The cloud architecture supports flexible consume, self services and pay per use model. Besides the cloud supports in three parts as below and they help the achievement of large scale economics by bringing the core IT infra to the big scale data center.

- supply side reduction: Cost per server of the big scale data center is reduced.
- Demand side count: Total demands for computing make good progress in overall fluctuations and make high the use of server.
- multitenancy efficiency: When changed to the multitenant application program model, the amount of tenants (ex. customers or users) increase and the cost for application program administration and server per tenant is reduced.

The service for cloud computing is called IaaS, PaaS and SaaS, sometimes XaaS by the specific task X. If the specific task is Database, it's DaaS (Database as a Service). If Network, it's NaaS (Network as a Service). This study named StraaS the meaning of Streaming as a Service.

2.3. Scale Out Technique for Streaming Services

Nowadays mass contents from social networks, personal data sharing & backup, IPTV and Video streaming services targeting millions users all over the world increase and also atypical data traffic explodes according to increase of mobile equipment. Accordingly a new foothold in the storage market is prepared. Big Data is the atypical data based on unpredictable exploding files, and one of the storage techniques for the good management of this is the Scale out technique. The scale out technique has appeared to fulfill the necessary performance requirements, which contrasts to the scale up technique. The scale up is the technique adding storage resources by performance demand. However up to certain scale it can raise the capacity but the performance is tied up or degenerated. On the contrary the scale out is the technique expanding separated system linearly by performance requirements and it can expand whenever performance and capacity is needed. A lot of storage companies have released the storage using the scale out technique, though we have to check if the real scale out technique applied or not.

For example the products applied only clustering techniques to many RAID storage systems or only utility techniques to the environment made up of limited expanded file systems and volumes are not sufficient for the Scale out storage. The fundamental concept of the scale out storage is linear expansion of performances, volumes, and throughput by adding storage resources without service interruption. However the structure showing as one file system by simply combining many volumes can be complicated in the big data environment with exploding data in the aspect of not only the limit of the storage volume and performance but also management.

2.4. Technique Trend of Searchable Encryption System

In searchable encryption system (SES), the subject of information referred the document. That is, the document is the information users want to hide. Hence, the user provides information on a server to retrieve documents is called a keyword. In general, the data contained in the document as a set of keywords is defined as Eq. 1:

$$D=\{W_1, W_2, \cdots, W_n\} \tag{1}$$

The searchable encryption system consisting of four steps is pictured in Figure 4.

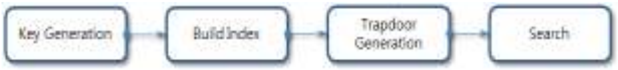


Figure 4. Basic Structure of Searchable Encryption System

The searchable encryption systems of personal information stored in external storage space that occur as a workaround for the many problems have been studied until now. As shown in Figure 5, SES of the users' encryption keys can be classified into public key and private key.

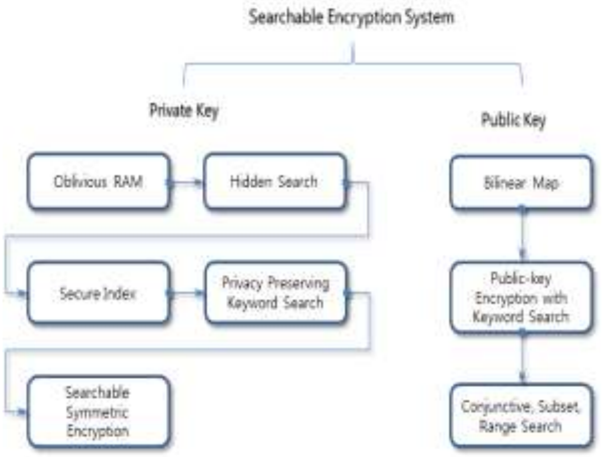

Searchable Encryption System
Private Key
Public Key
Oblivious RAM
Hidden Search
Bilinear Map
Secure Index
Privacy Preserving Keyword Search
Public-key Encryption with Keyword Search
Searchable Symmetric Encryption
Conjunctive, Subset, Range Search

Figure 5. SES Classification by Private Key and Public Key

3. Design of StraaS

Providing streaming services using Cloud Computing base and the data processing technique is named StraaS (Streaming as a Service) as shown in Figure 6.

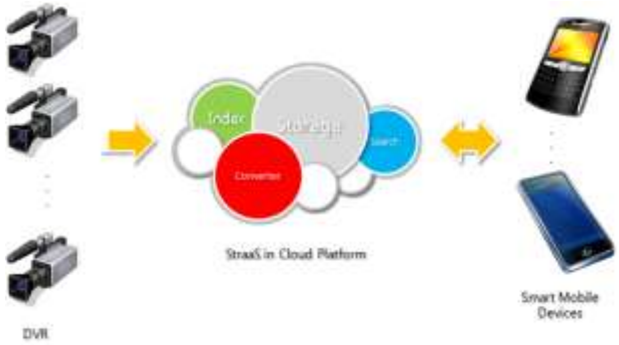


Figure 6. Concept Diagram of StraaS

3.1. The System Design of Streaming as a Service

StraaS supports the security over the cloud computing infra computing, networking, and storage resources of existing streaming service and it means providing data processing technology for various services. The system structure for the streaming service gets the diagram of Figure 8 from IPO model of Figure 7. IPO model is the data processing diagram made up of input, processing, storage and output for processing data into the information.

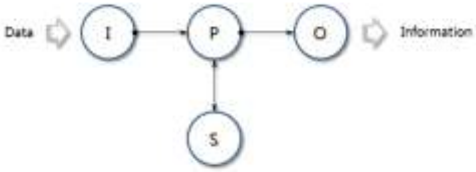


Figure 7. IPO Model

Providing StraaS service, Cloud Computing, networking and storage resources are needed first of all. Networking resources of Cloud Computing connect between the origin & the destination of the streaming media created for supporting the streaming service and Cloud Computing as well as the storage. The cloud computing resources support the services served from the framework like the exchange of the streaming media, certification and encoding/ decoding. The cloud storage resources offer the space for the streaming media. Especially they're divided into the public cloud storage for services and the private cloud storage for archive.

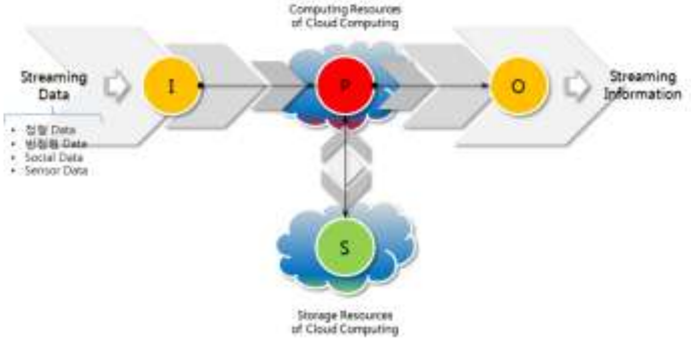


Figure 8. System Concept of StraaS

3.2. Service Function of StraaS

StraaS provides the streaming service based on Cloud Computing, and by managing Cloud Computing flexibly in any limited conditions it can support various real-time services like the exchange of the streaming media, index/ search and compression.

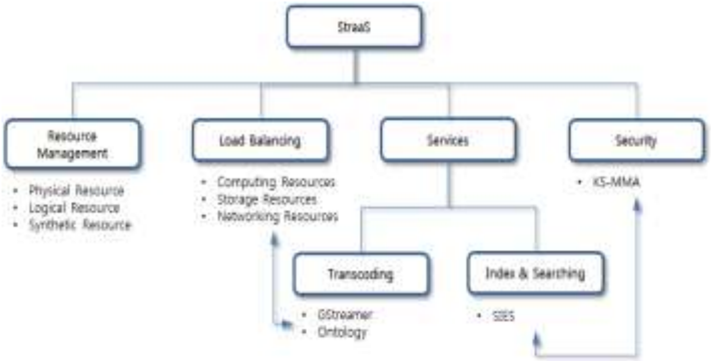


Figure 9. Function Diagram of StraaS Service

3.3. Transcoding of Media

StraaS carries out the data center role of the streaming media.

It recognizes various streaming medium from many places and resources of the device consuming streaming media and offers real time conversion of proper streaming media format using Cloud Computing resources. The conversion of streaming media is developed by GStremer tools [8], and the open source and the overview of GStreamer is shown in the figure 10.

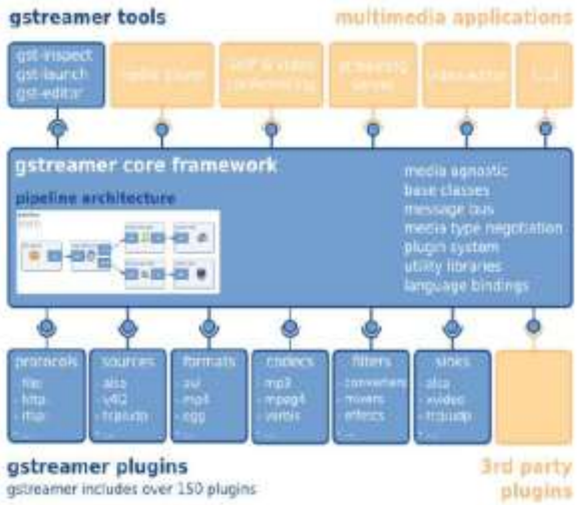


Figure 10. Overview of GStreamer

3.4. Index and Pattern Information

The SIES of StraaS extracts the image keyword and 1st index in steaming media by Content-based image retrieval (CBIR) technique as shown in Figure 11. In Figure 11, the poster cut is the collection of image keywords. The extracted images are called image keywords because each image in such an image array is referenced by one index or address of one part of streaming media. And the access control of poster cut needs user's authentication.

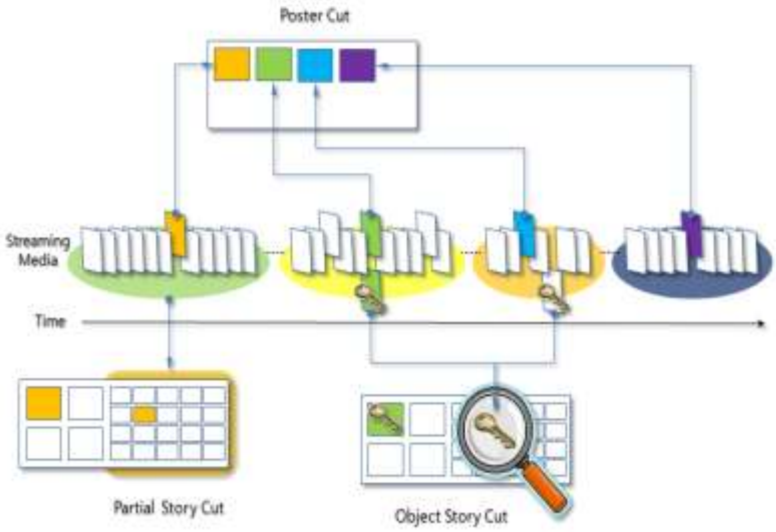


Figure 11. Indexing process of StraaS

In pre-subsection, we describe the process of 1^{st} index and image keyword extracted one part of streaming media. Figure12 shows the streaming media and extracted image keyword in one part of streaming media

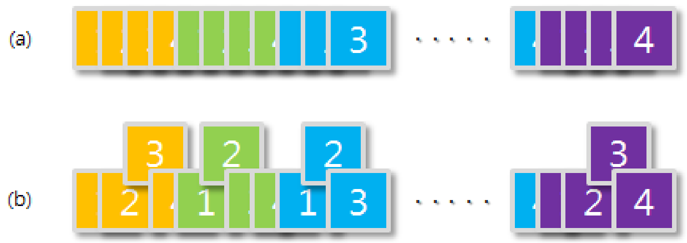


Figure 12. (a) Streaming media, (b)Extracted image keyword in streaming media

Figure 13 and Figure 14 show the encryption and decryption process of streaming media by 1st key and 2nd key groups. And Figure 8 shows the poster cut area for image keyword extraction on streaming media by CBIR technique. CBIR is the application of computer vision techniques to the image retrieval problem, that is, the problem of searching for digital images in large databases. "Content-based" means that the search will analyze the actual contents (refer to colors, shapes, textures, or any other information) of the image rather than the metadata such as keywords, tags, and/or descriptions associated with the image.

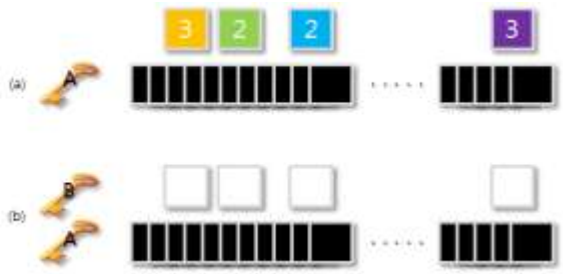


Figure 13. Encryption of streaming media and image keyword

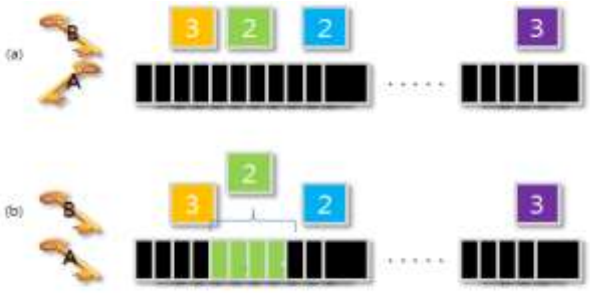


Figure 14. Decryption of Image Keyword and One Part of Streaming Media

3.5. Save/Backup – Scale Out Shoring Place of the Cloud Storage

The saving and backup of StraaS largely subdivides into primary and secondary saving. Primary place is for offering services, while secondary place is for backup.

(1) Primary save - storage for services

It's the primary storage for offering StraaS services and uses Azure of MS, the public cloud and taking computing, storage and networking for the streaming service.

StraaS services uses Azure of MS, the public cloud as the primary storage and takes computing, storage and networking for the streaming service.

(2) Secondary save - storage for archive.

The streaming media not used for a while operates backup and other provisioning functions using Private Cloud based on self developed open source and builds Private Cloud using OpenStack [9], the open source of cloud computing systems.

3.6. The Network and Provisioning Function

Describe the networking and provisioning function of StraaS.

(1) Network function

In order to support smooth management of StraaS, the network resources are more important than cloud computing resources.

(2) Provisioning function

Provisioning functions for smooth management of StraaS are largely computing and storage resources.

4. Security of StraaS

In the present computing environment the encoding is much more important than ever before.

More and more applications and protocols protect the system from malicious attacks using the encoding technique. The encoding guards saved or transferring data, creates personal information, checks data integrity, protect contents from any use without permission, operates the payment system, builds double certification and prevents wiretapping.

The powerful encoding protects confidentialness of information and proofs the legality of user, streaming services or messages. In case of weak encoding companies may have resources and secrets stolen or fall behind in the competition.

The security services of StraaS are as below.

- encoding/ decoding of streaming media
- division/ duplication of streaming media
- KS-MMA & SIES

4.1. encoding/decoding and division/duplication

All the streaming medium transferred to the StraaS data center are encoded and duplicated in the container way, and then dispersed and saved in the Scale out storage. The encoding/ decoding of streaming media needs a lot of computing resources. The strength of StraaS service is real time handling of the encoding/ decoding using abundant computing resources of the Cloud infra.

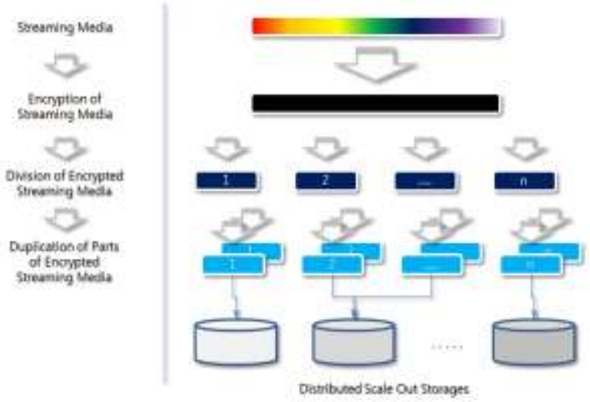

Streaming Media
Encryption of Streaming Media
Division of Encrypted Streaming Media
Duplication of Parts of Encrypted Streaming Media
1
2
...
n
Distributed Scale Out Storages

Figure 15. Encryption and Division/Duplication of Streaming Media

(1) The encryption of streaming media

The encoding is performed to prevent any use of streaming media without permission. Because creating part and saving/ administrating part of streaming media are separated, the decoding of encoded streaming media is possible only by a mutual agreement, when multilateral adjustment certification is used.

(2) The dispersion and duplication of streaming media

To prevent the loss of streaming media in divided containers, it's duplicated and saved separately.

(3) Image search and decoding of streaming media

To prevent any use without permission and access control of streaming media, search and decoding is performed only in case of certification and access control by KS-MMS. When the certification is completed and the authority is given, image search of streaming media without decoding becomes possible by searchable image encoding system. Encoded streaming media is divided, duplicated and saved separately, and for the case of fail in the first search only when the second search of duplicated dispersed saved streaming media, perfect decoding of streaming media can be completed.

4.2. Multilateral Adjustment Certification of Streaming Data

In the general access control of streaming media (A) or (B) in figure16 will take majority cases, and these cases have problems like privacy in the aspect of security, DRM (Digital Rights Management), distribution and charge of digital contents. These problems not ending in the first hand, secondary and tertiary ramifications have occurred, what becomes social issues. The proposal for solving these problems is as shown in Figure 17.

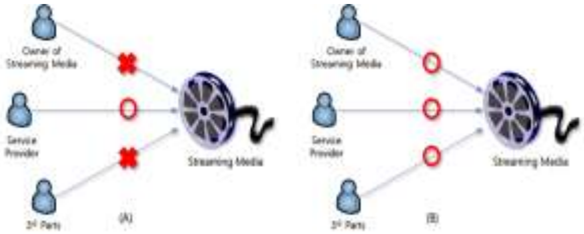


Figure 16. General access control of streaming media

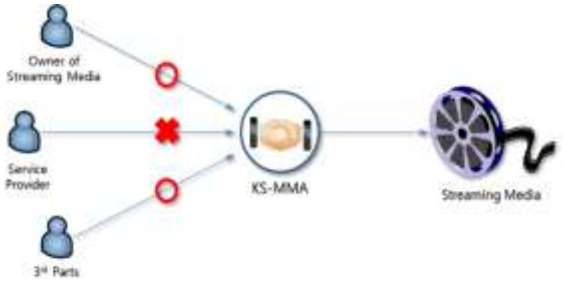


Figure 17. Access Control of Streaming Media by Proposed KS-MMA

The encoded streaming media saved separately in the StraaS data center should be integrated and encoded to the container. The encoded streaming media decoded through the key creation by the multilateral matching certification and it roles as in figure 17. In the multilateral matching certification, the key for decoding will be created through the agreement of random user, and that's shown in Figure 18.

The multilateral adjustment certification system is entrusted the authority by KS-MMA and creates the key for decoding and access control, even though the majority of users among all the consulted users don't agree. For the system management user certification is needed and users are assigned ID and relevant role. Also assigned ID uses multilateral adjustment as the certification process for the authority of the upper role. If over 50% of the lower role make consultation, 2 out of 3 people agree as in Figure 1, the certification is provided for the upper role. In the upper role's absence, by the agreement of ID2 and ID3 equivalent to over 50%, combining B and C of ID2 with A and C of ID3 can make confirm the upper role.

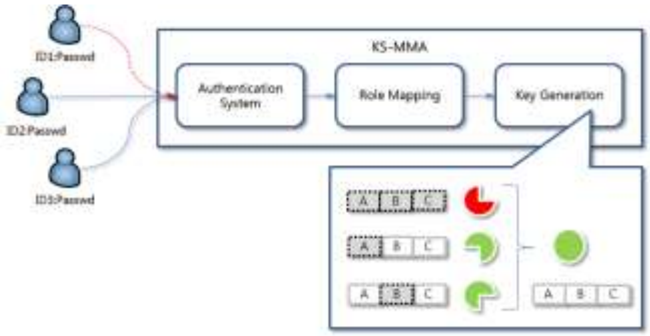


Figure 18. Concept Diagram of Key Generation Process by KS-MMA

4.3. Searchable Image Encryption System (SIES)

The proposed SIES has extended the streaming media and the image keyword from the document and the keyword in cloud computing. That is, SIES has redefined to extend Eq. 2 instead of Eq. 1 of SES.

$$\text{Straming Media} = \{\text{IMG}_1, \text{IMG}_2, \cdots, \text{IMG}_n\} \qquad (2)$$

It is able to search streaming media by image keyword from searching documentation. Additionally, the SIES can support the authentication and privacy of users.

5. Application Model of StraaS

We propose applications and business models using StraaS service and it's not restricted.

5.1. Expansion of Existing Service

EBS broadcasting offers educational streaming services and supports certain streaming media format based on PC and some tablets. Briefly we can raise the use of digital contents from EBS site, and provide added functions for digital media consume. For example in Apple's iPad2 to use streaming services we have to download the media from EBS site to our PC and then convert into the media format refreshable in iPad2. The converted media should be transferred to iPad2 through iTunes. StraaS can shorten these complicated process, and make various conversion suitable for PC, mobile, tablet and cellphone for the consume of streaming media using ontology in nearly real time.

5.2. Infra Integration Function of StraaS

Infra integration function of StraaS can make produce streaming media corresponding to the story about arbitrary entities by integrating created medium from devices capturing distributed images and videos in an area. Figure 19 is the diagram for the service using meta information of streaming media, and Figure 20 shows the applied example.

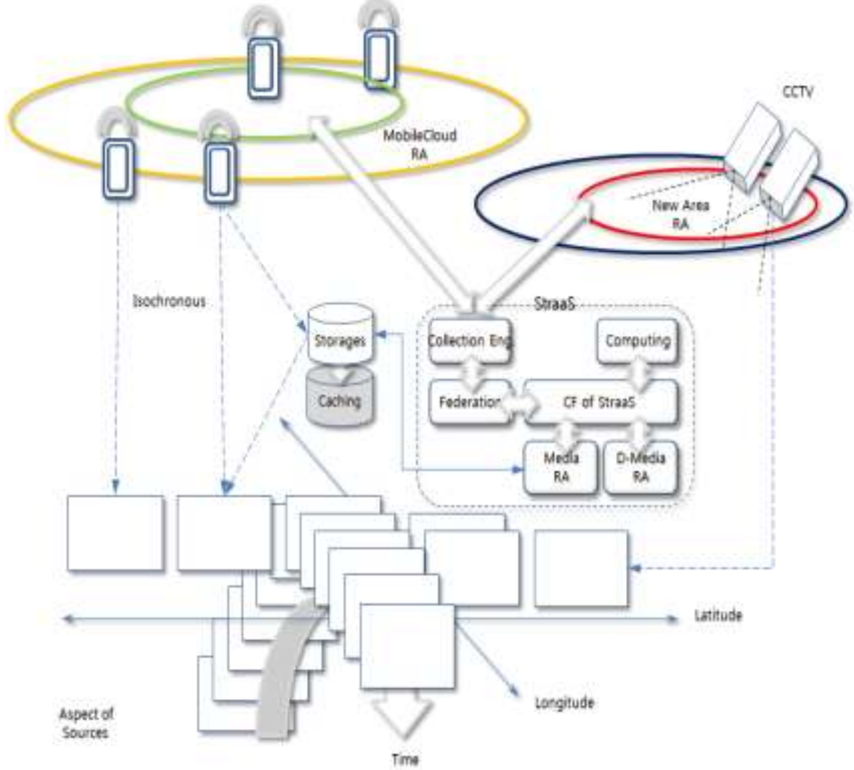


Figure 19. Service support using meta information of time and location data

Location
Time

Figure 20. New Application Service Support by Meta Information of StraaS

6. Conclusion

This paper designed StraaS services supporting streaming services and security based on cloud computing. It defined Streaming as a Service (StraaS) for supporting streaming services based on Cloud Computing, and described various functions and security function for supporting StraaS service.

Especially as the security function for Cloud Computing and streaming service KS-MMA provides access control by multilateral adjustment certification and SIES is possible to provide privacy of streaming media.

Wherever Times New Roman is specified, Times Roman, or Times may be used. If neither is available on your word processor, please use the font closest in appearance to Times New Roman that you have access to. Please avoid using bit-mapped fonts if possible. True-Type 1 fonts are preferred.

References

[1] McKinsey, “Big Data: The next frontier for innovation, competition, and productivity”, **(2011)**.
[2] Gartner, http://www.gartner.com.
[3] P. Golle, J. Staddon and B. Waters, “Secure Conjunctive Keyword Search over Encrypted Data”, Proceedings of Applied Cryptography and Network Security Conference, **(2004)** June 6-10, College Park, Maryland.
[4] B. Waters, D. Balfanz, G. Durfee and D. Smetters, “Building an Encrypted and Searchable Auditlog”, NDSS, **(2004)**.
[5] R. Ostrovsky and W. Skeith, “Private Searching on Streaming Data”, Cryptology, vol. 20, no. 4, **(2007)**.
[6] J. Bethencourt, H. Chan, A. Perrig, E. Shi and D. Song, “Anonymous Multi-Attribute Encryption with Range Query Conditional Decryption”, Technical Report, C.M.U., **(2006)**.
[7] N. S. Jho and D. W. Hong, “Technical Trend of the Searchable Encryption system”, Electronic and Telecommunications Trends, vol. 23, no. 4, **(2008)**.
[8] GStreamer, http://www.gstreamer.net.
[9] OpenStack, http://www.openstack.org.
[10] S. K. Eun, “Cloud Computing Security Technology Trends”, Review Security and Cryptology, vol. 20, no. 2, **(2010)**.
[11] G. Zhang and Q. Xu, “Secret Key Awareness Security Public Key Encryption Scheme”, vol. 5, no. 4, **(2011)**.

Authors

Byung Rae Cha

ByungRae Cha is a research professor at school of Information Communications, and Super Computing & Collaboration ENvironment Technology (SCENT) center, GIST, Korea. He received the Ph.D. degree in computer engineering from Mokpo National University in 2004 and the M.S. degree in Computer Engineering from Honam University in 1997. Prior to becoming a research professor at GIST, he has worked as a research professor in dept. of information and communication eng., Chosun University, and professor in dept. of computer engineering, Honam University, Korea. His research interests include Computer Security of IDS and P2P, Neural Networks Learning, Future Internet, Cloud Computing, and NFC.

Soo Bong Park

Soo Bong Park is a professor in dept. Of Information & Communication Eng. Dong Shin Univ. He received the B.S., M.S., and Ph.D. degree in the ChoSun Univ., Gwngju, KOREA His research interests in Image Processing and Optical communication. He is a member of IEICE, IEEK, and KISC.

Yoo Kang Ji

Yoo Kang Ji was bone in Naju, Republic of KOREA, on Sep. 21. 1975. He received the B.S., M.S., and Ph.D. degree in the Dept. of Information & Communication Eng. from DongShin Univ., Naju, Jeonnam, KOREA in 2000, 2002, and 2006. respectively. He has worked professor in dept. of information & Communication Eng. DongShuin Univ. Mar. 2006 to Aug. 2009 His research interests in Mobile S/W, Networked Video and Embedded System. He is a member of IEICE, IEEK, KISC, and SERSC.