International Journal of Current Engineering and Technology
ISSN 2277 - 4106

Available at http://inpressco.com/category/ijcet

Research Article

Implementation of IPTV service delivery through Virtualization

G.Sreenivasulu[a*], P.Babu[a], SD. Afzal Ahmed Syed[a] and N..Penchalaiah[b]

[a]Quba College of Engineering & Tech, Nellore
[b]Audisankara College of Engineering &Technology, Gudur

Accepted 15 September 2013, Available online 01 October 2013, **Vol.3, No.4 (October 2013)**

Abstract

Implementation of IPTV service delivery through Virtualization is of practical interest in many applications such as detecting an IPTV service delivery failures. The intrusion detection is defined as a mechanism for an IPTV service delivery through virtualization to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this paper, we consider this issue according to heterogeneous IPTV service delivery models. Furthermore, we consider two sensing detection models: single-sensing detection and multiple-sensing detection... we seek to lower a provider's costs of real-time IPTV services through a virtualized IPTV architecture and through intelligent timeshifting of service delivery, We provide a generalized framework for computing the amount of resources needed to support multiple services, without missing the deadline for any service. We construct the problem as an optimization formulation that uses a generic cost function. Our simulation results show the advantage of multiple sensor heterogeneous WSN IPTV service delivery through virtualization. We also show that there are interesting open problems in designing mechanisms that allow time-shifting of load in such environments.

Keywords: *Orchestrator, Set Top Box, Video On Demand, Interactive TV, Live TV, Provable data possession (PDP) (or proofs of retrievability (POR))*

1. Introduction

IPTV means delivering enhanced video applications over a managed or dedicated network via Internet Protocol.

In IPTV service, this technology is used as that of Internet Services. In this service the TV channels are encoded in IP format and delivered to TV using a Smart Electrical Electronic Device. The IP TV Service also includes Video on Demand cloud services which is similar to watching Video CDs / DVDs using a VCD / DVD/CD player. Movies,different channels, Instructional Videos and other content shall be available to customers in the IP TV Services.This IPTV through a broadband connection. IPTV is not video over the public Internet.

IPTV describes as multimedia services such as television/video/audio/text/graphics/data delivered over IP based networks managed to provide the required level of quality of service and experience, security, interactivity and reliability.

IPTV virtualization provides the following services:

1. Live TV
2. Video On Demand (VOD)
3. Interactive TV

Interactive television is a form of media convergence, adding data services to traditional television technology.

2. Background

There exist various tools and technologies for multi-cloud, such as PlatformVM Orchestrator, VMware Sphere, and Overt. These tools help cloud providers construct a distributed cloud storage platform for managing clients' data. However, if such an important platform is vulnerable to security attacks, it would bring irretrievable losses to the clients. For example, the confidential data in an enterprise may be illegally accessed through a remote interface provided by a multi-cloud, or relevant data and archives may be lost or tampered with when they are stored into an· uncertain storage pool outside the enterprise. Therefore, it is indispensable for cloud service providers to provide security techniques for managing their storage services.

The IPTV provides the following ways to watch television through over air broadcasts and cable signals. The broadcast TV,an antenna picks up radio waves to transmit pictures and sound to your television set.The cable TV,wires connect to your TV & these wires run from your house to the nearest cable TV station and it acts as one big antenna

- **TV and Content Head End** - Where the TV channels are received and encoded. Also other content (Video's) are stored at Head End. MTNL has signed agreement for this with M/s Aksh Broadband.

*Corresponding author: **G.Sreenivasulu**

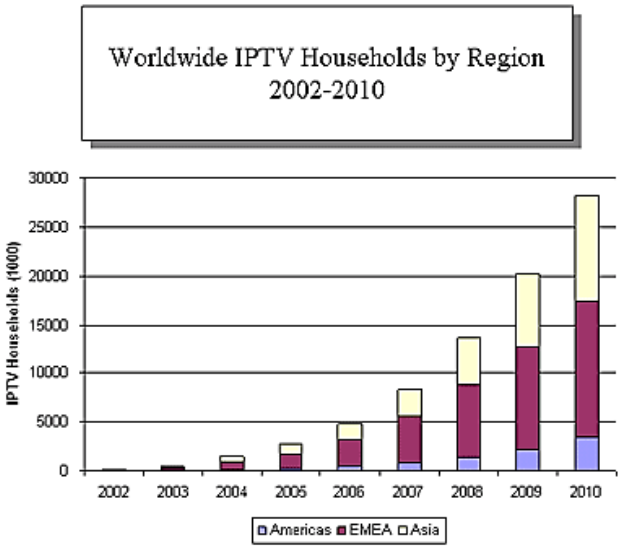
- **Delivery network** - Which is MTNL's Broadband network and MTNL's telephone line. (Landline).
- **Set Top Box (STB)**

The Set Top Box is required at the customer location for converting the IP signal back to TV signal. The STB shall be connected between MTNL Broadband Modem and customer's TV. The STB shall be provided by M/s Aksh in case of existing Triband. M/s Aksh shall also provide single port ADSL modem, in case of IPTV provisioning on either existing landline or on copper pair without landline.

Live TV,VOD and IPTV through virtualization

	Live TV, VOD &ITV	IPTV through virtualization
Data Transfer	Use general internet	Use dedicated, private network
Whole Geographical Reach	Can be access from anywhere in the globe	Limited by service provider
Service quality &Quantity	Not guaranteed	Guarantees high quality audio and video
Data Access Mechanism	A PC with media player	Set-Top-Box most of the time
Content Generation use	Use own content	Provided by existing TV broadcasters

Growth of IPTV



2.1. IPTV through Virtualization Strategy

In recent years, cloud storage service has become a faster profit growth point by providing a comparably low-cost, scalable, position-independent platform for clients' data. Since cloud computing environment is constructed based on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability.

We call such a distributed cloud environment as a multi-

Cloud (or hybrid cloud). Often, by using virtual infrastructure management (VIM) , a multi-cloud allows clients to easily access his/her resources remotely through interfaces such as Web services provided by Amazon EC2. There exist various tools and technologies for multicloud, such as Platform VM Orchestrator, Vmware spheres, and Ovirt. These tools help cloud providers construct a distributed cloud storage platform (DCSP) for managing clients' data. However, if such an important platform is vulnerable to security attacks, it would bring irretrievable losses to the clients.

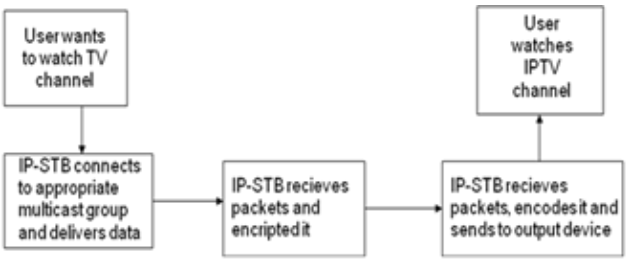
Provable data possession (PDP) (or proofs of retrievability (POR)) is such a probabilistic proof technique for a storage provider to prove the integrity and ownership of clients' data without downloading data. The proof-checking without downloading makes it especially important for large-size files and folders (typically including many clients' files) to check whether these data have been tampered with or deleted without downloading the latest version of data. Thus, it is able to replace traditional hash and signature functions in storage outsourcing. Various PDP schemes have been recently proposed, such as Scalable PDP and Dynamic PDP. However, these schemes mainly focus on PDP issues at untrusted servers in a *single* cloud storage provider and are not suitable for a multi-cloud environment.

2.2 IPTV Services

IPTV virtualization provides the following services

1. Live TV
2. Video On Demand (VOD)
3. Interactive TV

IPTV-STB Operation

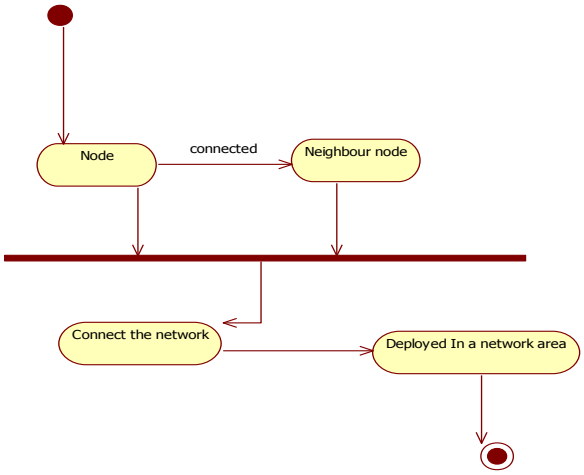


Interactive television is a form of media convergence, adding data services to traditional television technology.

3. IPTV distributed cloud environment

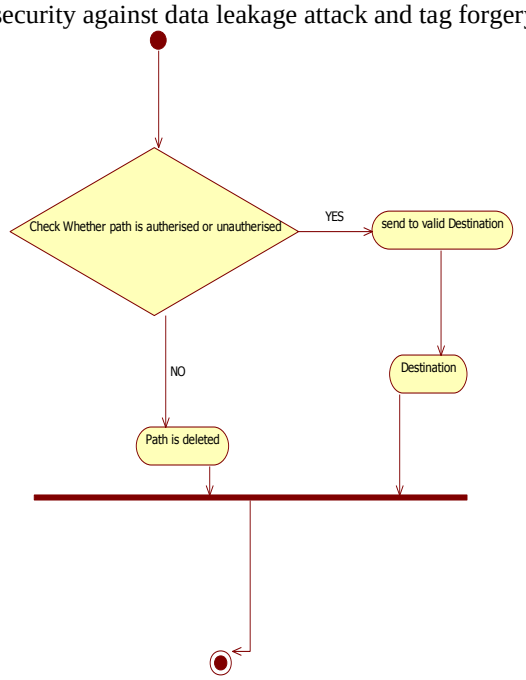
In the paper , we address the problem of data possession in distributed cloud environment for the following aspects : high security, transparent verification ,and high

performance. To achieve these goals, we first propose a verification framework for multi-cloud storage along with two fundamental techniques: hash index hierarchy(HIH) and homomorphic verifiable response(HVR).



We then demonstrate that the possibility of construction a cooperative PDP(CPDP) scheme without compromising data privacy based on modern cryptography techniques, such as interactive proof system(IPS).We further introduce an effective construction of CPDP scheme using mentioned structure.

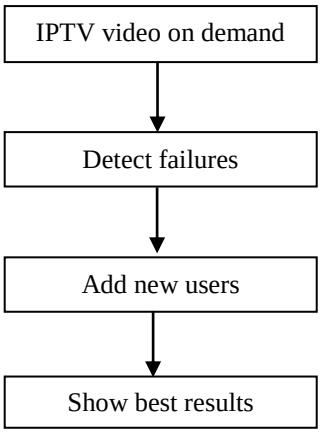
Moreover, we give a security analysis of our CPDP scheme from the IPS model. We prove that this construction is a multi-prover zero-knowledge proof system(MP-ZKPS) which has completeness, knowledge soundness, and zero-knowledge properties. These properties ensure that CPDP scheme can implement the security against data leakage attack and tag forgery attack.



To improve the system performance with respect to our scheme, we analyze the performance of probabilistic queries for detecting abnormal situation. This probabilistic method also has an inherent benefit I reducing computation and communication overheads. Then , we present an efficient method for the selection of optimal parameter values to minimize the computation overheads of CSPs and the client's operation. In addition , we analyze that our scheme is suitable for existing distributed cloud storage system. Finally our experiments show that our solution introduces very limited computation and communication overheads.

4. Implementation of IPTV

To check the availability and integrity of outsourced data in cloud storages, researchers have proposed two basic approaches called Provable Data Possession and Proofs of Irretrievability. Ateniese et al. first proposed the PDP model for ensuring possession of files on un-trusted storages and provided an RSA-based scheme for a static case that achieves the communication cost. They also proposed a publicly verifiable version, which allows anyone, not just the owner, to challenge the server for data possession. They proposed a lightweight PDP scheme based on cryptographic hash function and symmetric key encryption, but the servers can deceive the owners by using previous metadata or responses due to the lack of randomness in the challenges. The numbers of updates and challenges are limited and fixed in advance and users cannot perform block insertions anywhere.



Advantages of IPTV

1. Provable data possession is a technique for a storage provider to prove the integrity and ownership of clients' data without downloading data.
2. It mainly focuses on PDP issues at un-trusted servers for a multi cloud storage provider and is suitable for a multi-cloud environment.
3. Scalable to support storage of data across several CSP's
4. Provides multi-prove zero-knowledge proof system
5. Introduces lower computation and communication overheads in comparison with non-cooperative approaches.

Future Work

As part of future work, we would extend our work to explore more effective CPDP constructions. Finally, it is

still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. We would explore such a issue to provide the support of variable-length block verification

Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems.

Software will definitely undergo change once it is delivered to the customer. There are many reasons for the change. Change could happen because of some unexpected input values into the system. In addition, the changes in the system could directly affect the software operations. The software should be developed to accommodate changes that could happen during the post implementation period.

1. Verify that the entries are of the correct format
2. No duplicate entries should be allowed
3. All links should take the user to the correct page.

6. Conclusion

We presented the construction of an efficient PDP scheme for distributed cloud storage. Based on homomorphism verifiable response and hash index hierarchy, we have proposed a cooperative PDP scheme to support dynamic scalability on multiple storage servers. We also showed that our scheme provided all security properties required by zero knowledge interactive proof system, so that it can resist various attacks even if it is deployed as a public audit service in clouds. Furthermore, we optimized the probabilistic query and periodic verification to improve the audit performance. Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems

References

Vaneet Aggarwal, Vijay Gopalakrishnan, Rittwik Jana, K. K. Ramakrishnan, Vinay A. Vaishampayan , Optimizing Cloud Resources for Delivering IPTV Services through Virtualization, AT&T Labs – Research, 180 Park Ave, Florham Park, NJ, 07932

B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster (2009), Virtual infrastructure management in private and hybrid clouds, *IEEE Internet Computing*, vol. 13, no. 5, pp. 14–22.

G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song (2007), Provable data possession at untrusted stores, in *ACM Conference on Computer and Communications Security*,

P. Ning, S. D. C. di Vimercati, and P. F. Syverson (2007), Eds. *ACM*,pp. 598–609.

A. Juels and B. S. K. Jr. (2007), Pors: proofs of retrievability for large files, in *ACMConference on Computer and Communications Security*

G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik (2008), Scalable and efficient provable data possession, in *Proceedings of the 4th international conference on Security and privacy in communication netowrks*, SecureComm, pp. 1–10.

C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia (2009), Dynamic provable data possession, in *ACM Conference on Computer and Communications Security*, pp. 213–222.

H. Shacham and B. Waters (2008), Compact proofs of retrievability, in ASIACRYPT, ser. Lecture Notes in Computer Science, *J. Pieprzyk*, Ed., vol. 5350. Springer, pp. 90–107.

Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou (2009), Enabling public verifiability and data dynamics for storage security in cloud computing, in *ESORICS, ser. Lecture Notes in Computer Science*, vol. 5789. Springer, pp. 355–370.

Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau (2011), Dynamic audit services for integrity verification of outsourced storages in clouds, in *SAC*, pp. 1550–1557.

K. D. Bowers, A. Juels, and A. Oprea (2009), Hail: a high-availability and integrity layer for cloud storage, in *ACM Conference on Computer and Communications Security*, pp. 187–198.

Y. Dodis, S. P. Vadhan, and D. Wichs (2009), Proofs of retrievability via hardness amplification, in *TCC, ser. Lecture Notes in Computer Science*, vol. 5444. Springer, pp. 109–127.

L. Fortnow, J. Rompel, and M. Sipser (1988), On the power of multiprover interactive protocols, in *Theoretical Computer Science*, pp. 156–161.

Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen (Oct 2011), Collaborative integrity verification in hybrid clouds, in *IEEE Conference on the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom*, Orlando, Florida, USA, 15-18, pp. 197–206.

M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2009), Above the clouds: A berkeley view of cloud computing, *EECS Department, University of California, Berkeley, Tech*. Rep.

D. Boneh and M. Franklin (2001), Identity-based encryption from the weil pairing, in *Advances in Cryptology* (CRYPTO'2001), vol. 2139 of LNCS, , pp. 213–229..

O. Goldreich (2001), Foundations of Cryptography: Basic Tools. *Cambridge University Press.*.

G.Sreenivasulu, received the PG degree in Master of Computer Applications from SV University,2006..and pursing M.Tech in QCET(2011-2013) .He participated in national level conference on Implementation of IPTV services through virtualization at ASCET, Gudur

P.Babu received the PG degree in Master of Computer Applications from SV University and also received Mphil Degree. At present he is working as associate.professor in quba college of engineering and technology. he is dedicated to teaching field from the last 8 years.

SD.Afzal Ahmed syed received the M.Tech degree in computer science and Engineering from JNTU Ananthapur. At present he is working as associate.professor in quba college of engineering and technology. he is dedicated to teaching field from the last 8 years.

Prof.N.Penchalaiah Research Scholar in SV University, Tirupati and Working as Professor in CSE Dept,ASCET,Gudur. He was completed his M.Tech in Sathyabama University in 2006. He has 11 years of teaching experience. He guided PG & UG Projects. He published 5 National Conferences and 10 Inter National Journals.