ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Improved Security and Privacy In: A Media Cloud Computing Middleware for Content Management Using Cloud Material Protection Algorithm

R.Bhagya[1], Chitradevi [2]

Student, Department of Computer Science and Engineering, Roever Engineering College, Perambalur, India[1]

Assistant Professor, Department of Computer Science, Thanthai Hans Roever College, Perambalur, India[2]

ABSTRACT: Cloud computing is becoming a key element in service provision, allowing access to resources across internet transparently without the hassle of investing hardware resources nor maintaining or managing them. At present, sharing of media files with friends and families get admired worldwide. UPNA or DLNA are protocols designed to share content between devices within home network. It lacks the mechanism to share content outside the home domain and it doesn't support advanced search capabilities. To alleviate the above problem, we propose Media Cloud, a middleware instantiated in set-top boxes to manage media transparently allowing uniform access to multimedia content belonging to different home. In addition, construction of cloud computing and security mechanism of material protection calculating method, namely, Global Authentication Register System (GARS), to reduce cloud material outflow risk.

KEYWORDS: UPnp,DLNA,GARS,TTP

I. INTRODUCTION

Cloud computing is a new paradigm that offers scalability, reliability, availability when accessing resources across Internet. Moreover cloud computing is expected to abstract the details of the underlying infrastructure even when they are complex. The term "cloud" is a metaphor for the Internet, the network over which different organizations join to dynamically offer scalable resources. Media management is among the most outstanding aspects of cloud computing, since the cloud makes possible to retain and share large amounts of digital media. Cloud computing might be a good solution for processing content in distributed environments. Current home devices can produce, store and deliver high quality media that can be finally distributed towards social networks and communities where constituent members might be family or friends. However, there is no infrastructure to keep data under control or even find a concrete media in the home environment or outside it. Media cloud has been designed to cope with this problem letting users constitute cloud with friends even if media is located outside their domains.

II. RELATED WORK

Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment. UPnP is intended primarily for residential networks without enterprise-class devices. The UPnP technology is promoted by the UPnP Forum, a computer industry initiative to enable simple and robust connectivity to stand-alone devices and personal computers from many different vendors. The Forum consists of over eight hundred vendors involved in everything from consumer electronics to computing. The concept of UPnP is an extension of plug-and-play, a technology for dynamically attaching devices directly to a computer, although UPnP is not directly related to the earlier plug-and-play technology. UPnP devices are "plug-and-play" in that when connected to a network they automatically establish working configurations with other devices.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

DLNA refers to Digital Living Network Alliance. The DLNA standard is used for sharing music, photos and video over an existing home network. For example, by using DLNA you could stream video from your phone to a compatible TV-set using a Wi-Fi network. Compared to the existing models, proposed model of media cloud consist contains the following features 1.Allows multiple users across different home network to share/access content,2.Encryption and decryption of sharing files.3.Security over out flow of user generated media files.

III. MEDIA CLOUD ARCHITECTURE

1. Home Network

A Home network or home area network is a residential local area network (LAN). It is used for communication between digital devices typically deployed in the home, usually a small number of personal computer and accessories, such as computers and mobile computing devices. In the home networks they use UPnP and DLNA protocols to share the media content with their families and friends**.**

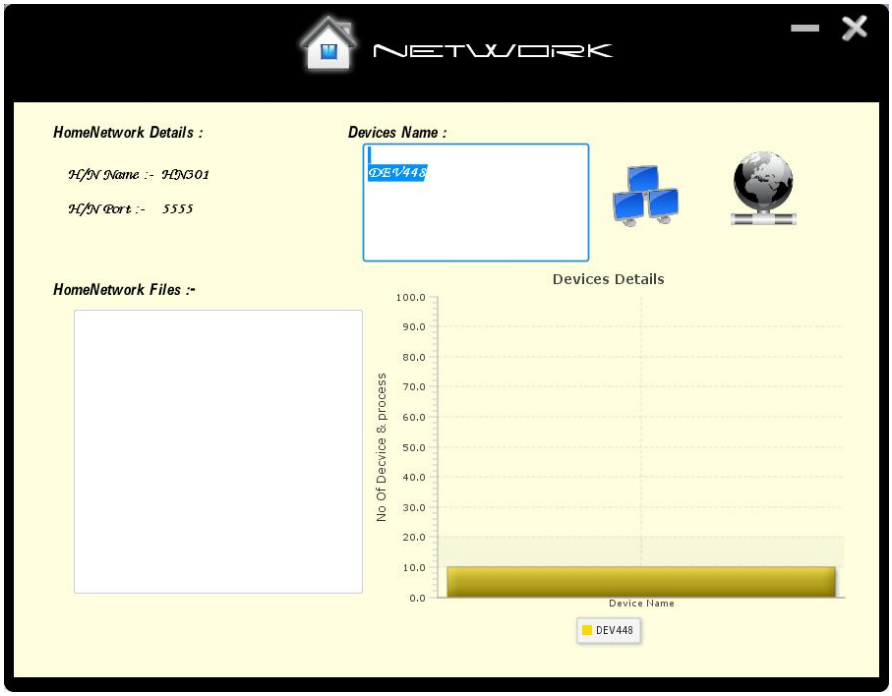

Figure 1: Home Network Module. This figure shows Home network Details and which are the devices connected with the home network.

2. Media Cloud

Media Cloud is a middleware for enabling media-centered cooperation among home networks. Media Cloud is the bridge to an open architecture that allows users to join their home equipments to constitute a cloud. Media Cloud abstracts the underlying complexity to provide a new content distribution model that simplifies classifying, searching and accessing user-generated and commercial content within the home networks. In the Media Cloud consist of two modules: The Media Indexer and The Foreign Content Aggregator. Aside those modules there is a security layer which enforces security policies and filter contents.

3. Media Indexer

The Media Indexer discovers devices located in the home domain and interrogates them to gather information about the contents they retain. It uses content information to produce an index that will be used by the Foreign Content

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Aggregator to facilitate search operations. The Media Indexer has two functional blocks: The Content Indexer and The Home Domain Manager.

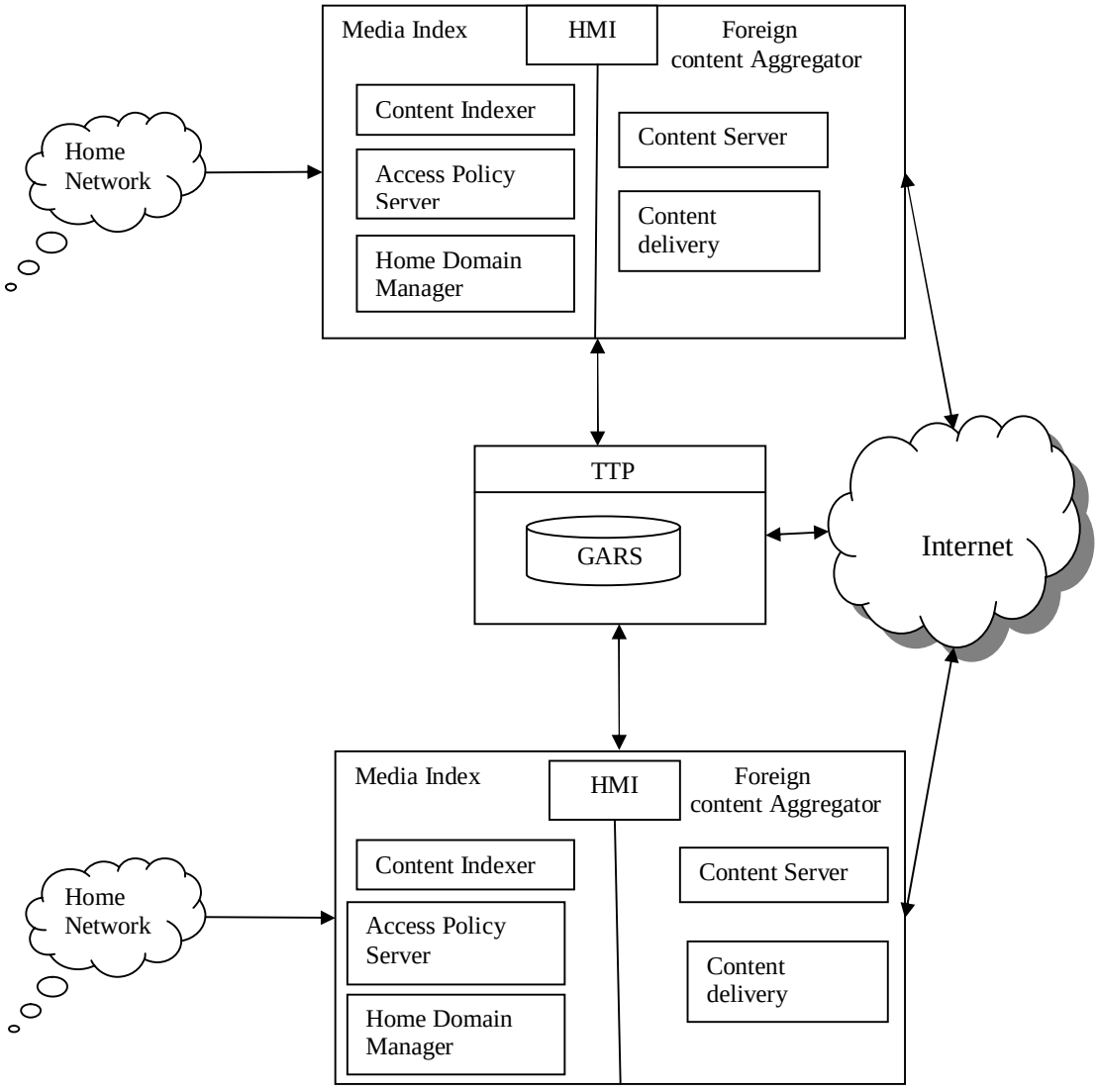

Figure 2: Media Cloud architecture. The figure shows two functional modules, the Media Indexer and the Foreign Content Aggregator.

3.1. Content Indexer

The Content indexer collects information about the content as media type, creation date, metadata, and user's annotations. It also registers access information as the hardware identifier or the network address of the device holding that content, Protocols that can be used to access the content. With that information, it builds an index and stores it in the Home media indexes (HMI) database. Content indexer processes a media file, as a photo or video, it needs cooperation for the devices, for instances, to provide information about the media file.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

This procedure requires device to implement a metadata extraction services accessible by ,for instance, DLNA or UPnp .Even though that is the preferred way, the content indexer can fetch the media file from the device or part of it, since the beginning usually contains the metadata, to process it. content indexer in charge of building an index for content using content metadata, social network feeds and internet related content. it is possible to use many different quires as phrase, wildcard, proximity, or range quires.

3.2. Access Policy Server is the security component of the Media Cloud that provides authorization services and facilitates tracking and control of media files. The access policy server acts as Policy Decision Point (PDP) which accepts access control requests, validates against the policy defined held in policy repository, makes decisions by using TTP server and returns the access control responses.

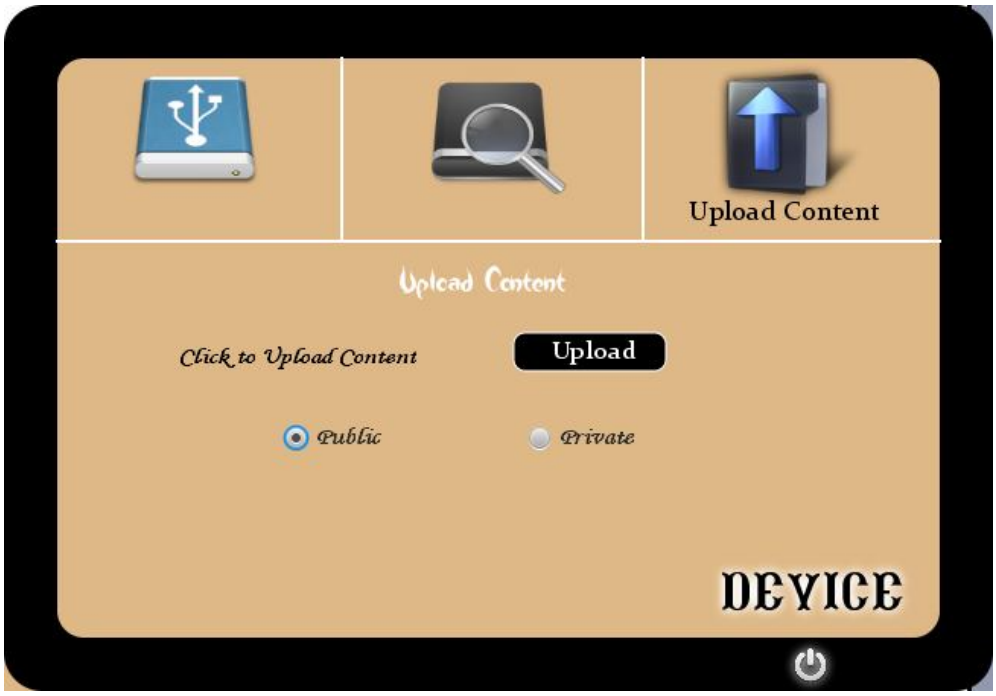

Figure 3:This figure shows the user can defined their policy to the uploading contents whether it can be Public or Private.

3.3. Home domain Manager

Home domain manger deals with the different network devices present in the home network. it relies on a plug-in system for supporting different devices and protocols, and it can be extended to support upcoming technologies. When content are requested from the home network or from the cloud the HDM retrieves the access information fields from the Access Policy server and instantiates

4. Foreign Content Aggregator

The Foreign Content Aggregator handles cloud communications. It makes content stored in devices at the home network available to other Media Cloud instances through Internet. The module is composed by a Content Server and a Content Delivery module. The Content Server facilitates foreign clients to search within the HMI database. The Content Delivery module sends content to other Media Cloud instances located outside the home domain. The authentication is handled by the Security Layer which includes access policy server and third party of trust after a foreign client is successfully authenticated and authorized. The Content Server Module enables users outside the domain to search content within the HMI database. The Content Delivery Module delivers the content

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

to the requesting node outside the home domain.

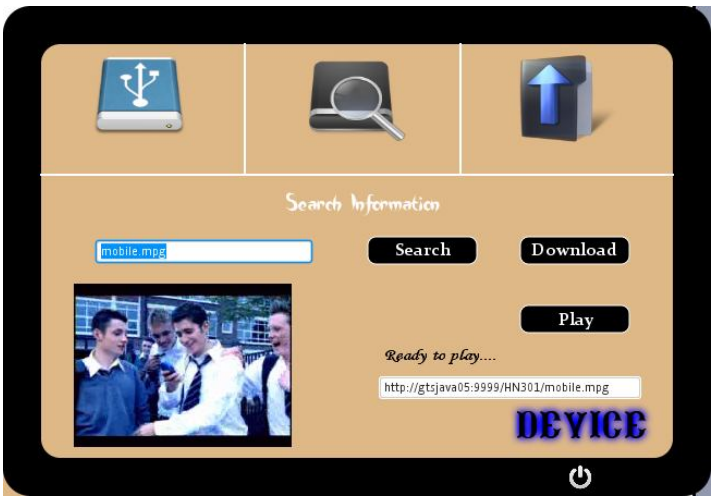

Figure 4:Content Delivery Module.Deliver content to the foreign devices.

5. GARS on Third Party of Trust

Security in media cloud is maintained using access server policy. Authentication in media cloud is handles at each user level, associated with their roles and we applied role based authentication mechanism. only if the authentication mechanism is successful the user were allowed to access the multimedia content. the authorized user can view the indices created and stored in the HMI database. As we follow the algorithm it is mentioned in Mathematical Problems in engineering volume 2013,Airticle ID 871430 ,To establish global authentication Register system (GARS) on third party clouds of trust (TTP) Provides the subscriber's premises and clouds both sides separately carries out a disposal registration certification service, but Public cloud part establishes right of privacy frame and model in the public cloud, and the encryption mechanism uses the GARS calculating method of this research and makes processing and protection on the privacy material and security.

Data Transmission Flow. FIGURES 5 AND 6 ARE SUBSCRIBER'S PREMISE/CLOUDS AND TTP PROOF PROCEDURE DATA TRANSMISSION

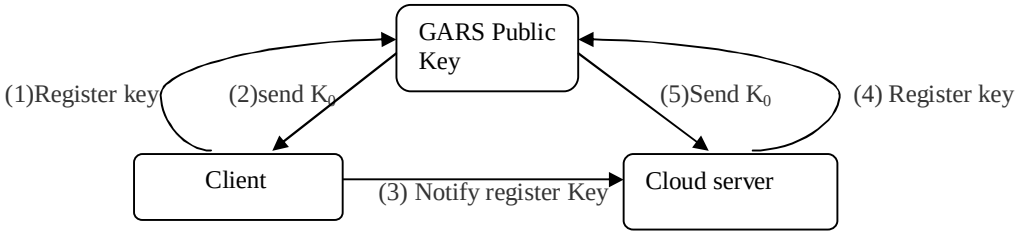

Figure 5: optimization model of cloud computing(initialization)

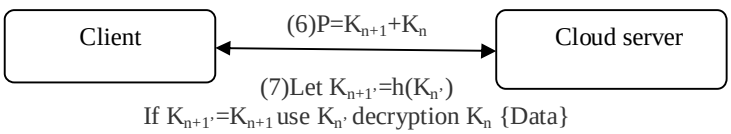

Figure 6: optimization model of cloud computing(after TTP authorizes)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

The Calculating Method Parameter Definitions : C: Client , S: Server.
K_n : Authentication basis code.(K_0 obtains initial authentication basis code by GARS).
H : Hash Function.
$K_{n+1}=h(K_n)$:Encryption Key(transmission end).
$K_{n+1'}=h(K_{n'})$:Encryption Key(receiving end).
$P= K_{n+1}+K_n\{Data\}$:Encryption seal Material(Package).

The GARS calculating method. GARS calculating method steps are as follows.
Step 1: the client sends out request register key to GARS.C-TTP: Request Register Key.
Step 2: GARS Transmits one group of key:K_0 to give client. TTP-c: Send Public key:K_0.
Step 3: Client informs Cloud server Register Key. C-s:Notify Register Key.
Step 4: Cloud server sends out Request Register Key to GARS. s-ttp Request Register Key.
Step 5: GARS transmits the same group key:K_0 to give cloud server. TTP-s:Send Register Key.
Step 6: The subscriber's premise uses K_0 to Produce one group of authentication encryption key:$K_1(K_1=h(K_0))$transmission encryption material ($P=K_1+K_0\{Data\}$) to cloud server. C→S:$K_{n+1}=h(K_n)$,$P=K_{n+1}+K_n\{Data\}$.
Step 7: Cloud server receives the encryption material and uses original K_n', Hash function obtain K_{n+1}', confirmation Comparison step 6 K_{n+1} weather is equal to step 7 $K_{n+1'}$;if equal, then it uses K_n to decipher the material. S:use K_n create $K_{n+1'}(K_{n+1'}=h(K_n))$.if $K_{n+1'}=K_{n+1}$→identify C then use $K_n\{Data\}$ S-c:$K_{n+1}=h(K_n)$,$P=K_{n+1}+K_n\{Data\}$.

Note. (1) If the Server end must transmit material to return to the Client end, then similarly use Steps 6 and 7, Server and Client role exchange.

(2) If material authentication mistake, by the subscriber's premise were decided whether needs to duplicate the Step 1 to Step 5 to authenticate.

IV. RESULT ANALYSIS OF GARS

Cloud material protection algorithm (GARS) which takes the technical theory of symmetrical encryption as the foundation, applies GARS in the information security of cloud computing. GARS has used the third party authentication mechanism trust, contains using Hash function and AES/DES data encryption technology characteristics, and coordinates the completed GARS flow to effectively protect security of cloud material and readability of stolen material.Figure-3 is Client/Server both sides authenticate Http Response Time after authentication;we may see that it take approximately 7 seconds to carry out analog transmission material 50 times response time to complete. Figure 5 is GARS one time authenticates Http Response Time; we may see that it takes 22 seconds to carry out the analog transmission material 50 time response time to complete.

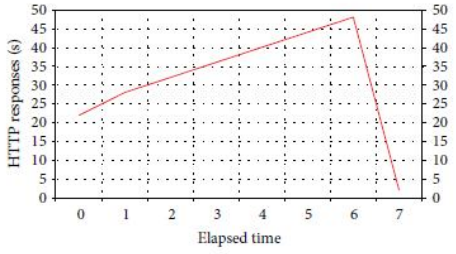

Figure 7: Both sides authenticate Http Response Time.

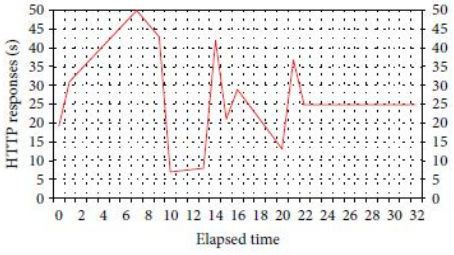

Figure 8: The three parties authenticate Http Response Time.

By way of the above results analysis of experimental data is stated as follows. (1) Client/Server/TTP one time authentication flow (5 steps): data are made by the simulation implementation in carrying out 50 times Client/Server to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

TTP authentication flow in which the finish time is 22 seconds, and authentication time on average is 0.44 second each time. (2) Client/Server both sides authentication flow (2 steps): after carrying out TTP authentication, Client/Server does not need to make the authentication with TTP again so long as carries out Client/Server both sides authentication flow in carrying out 50 times Client/Server both sides authentication flow in which the finish time is 8 seconds, and authentication time on average is 0.16 second each time. (3) Client/Server/TTP tripartite authentication flow(7 steps):this empirical datum needs to carry out the time needed of tripartite authentication for the simulation in which each time is 33 seconds, and authentication time on average is 0.66 second each time.

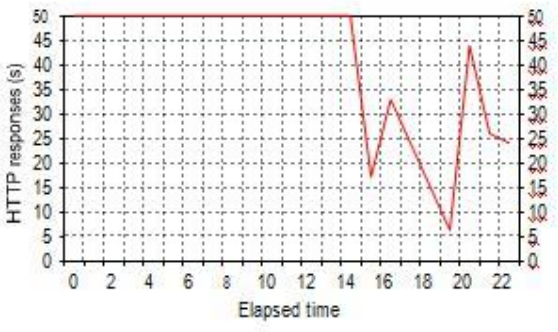

Figure 9:Authentication Http Response Time one time

IV. CONCLUSION AND FUTURE WORK

GARS utilization can protect the material security, in potency, because after GARS carrying out one time authentication, only needs user and cloud make both sides authentication flow; it has the obvious performance in the potency with currently general procedure of the authentication flow. Efficiently protect the user content from other also out flow is protected in the media cloud. Media Cloud achieves transparency and provides a secured, economically effective and manageable solution for bringing cloud computing paradigm to content management among federated home networks. It supports different devices by performing content adaption and enhances cooperation among different home networks facilitating an easy to manage solution.

REFERENCES

1 . Daniel Diaz-Sanchez, Florina Almenarez, Andres Martin, Davide Proserpio and Patricia Arias Cabarcos, "Media Cloud:An Open Cloud Computing Middleware for Content Management",IEEE Trans. On *Consumer Electronics*, Vol 57, No. 2, May 2011.
2 . Mariano Rico, Oscar Corcho, Víctor Méndez and José Manuel Gómez-Pérez, "A Semantically Enhanced UPnP Control Point for Sharing Multimedia Content", IEEE *Internet Computing*, December 2011.
3. Chih-Yung and jih-Fu tu ,"A Novel Cloud Computing Algorithm of Security and Privacy" Hindawi Publishing corporation Mathematical Problems in engineering volume 2013,Aircle ID 871430.
4. M. Armbrust, A. Fox, R. Griffith et al., "Above the Clouds: A Berkeley View of Cloud Computing", 2011.
5. L. Gu and S.-C. Cheung, "Constructing and testing privacy-aware services in a cloud computing environment—challenges and opportunities," in Proceedings of the 1st Asia-Pacific Symposium on Internetware (Internetware '09), October 2009.
6. M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in Proceedingsof the IEEE International Conference on Cloud Computing (CLOUD '09), pp. 109–116, September 2009.
7. M. Mowbray and S. Pearson, "Aclient-based privacy manager for cloud computing," in Proceedings of the 4th InternationalICST Conference on Communication System Software and Middleware (COMSWARE '09), Dublin, Ireland, June 2009.
8. S. Pearson, "Taking account of privacy when designing cloud computing services," in Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing (CLOUD'09), pp. 44–52, Vancouver, Canada, May 2009.
9. Kapotas.S.K, Varsaki.E.E, and Skodras.A.N,(2007) "Data Hiding in H- 264 Encoded Video Sequences," in IEEE 9th Workshop on Multimedia Signal Processing, MMSP.
10. Sarkar.A, Madhow.U, Chandrasekaran.S, and Manjunath.B.S,(2007) "Adaptive MPEG-2 Video Data Hiding Scheme," in Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents IX.
11. Schlauweg.M, Profrock.D, and Muller.E, (2008)"Correction of Insertions and Deletions in Selective Watermarking," in IEEE International
12. Conference on Signal Image Technology and Internet Based Systems, SITIS '08.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

13. Solanki.K, Jacobsen.N, Madhow.U, Manjunath.B.S, and Chandrasekaran, (Dec. 2004) "Robust image-adaptive data hiding using erasure and error correction," IEEE Transactions on Image Processing, vol. 13.
14. K. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, (Oct. 2009) "Complete video quality-preserving data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 19.

BIOGRAPHY

R.Bhagya, B.Tech(I.T).,Pursuing first year M.E Computer Science and Engineering in Roever Engineering College, Perambalur. Her area of interest is cloud computing.

Ms.B.Chitradevi, M.sc.,M.Phil.,B.Ed.,(Ph.D)., Assistant Professor, Department of Computer Science, Thanthai Hans Roever college,Perambalur-621212.