ISSN: 2320-1363

# Acknowledge Based effective and Robust Policy-Based Content Sharing in Public Clouds

A.Ramya*1, R.Anuj*2

M.Tech (Scholar), Dept of CSE, SVECW, Bhimavaram, Dist: W.Godavari, AP, India

Assistant Professor, Dept of CSE, SVECW, Bhimavaram, Dist: W.Godavari, AP, India

**ABSTRACT:**

Cloud Based Technology in these days is the hot cake in the Information Technology Industry, where the research is vast and will be a good opportunistic field in the computer science. If we consider the data and its security is always a concern in the today's date also which leads us to strongly design the product and provide the best, efficient and robust cryptographic technology which is the most important in the mystery of data security. If we consider the classical and these days data transmits mechanism which gives a good clarity in the most influential mater of encryption and decryption. In this paper we try to give the effort towards he glimpse of the data security in the concern of public cloud. Data is the most important component in the entire Information technology industry like electricity inside the cable. Hence, before sharing the data in the public cloud where we have given emphasis on the three major factors; identifying the user i.e. access control, key mapping and lastly the acknowledgement based cryptography technology. Surely; those above points will make sure not only the public cloud but also applicable all types file sharing system except FTP.

**KEYWORDS: Group key management, privacy, identity, cloud computing, policy, encryption, access control.**

## I.INTRODUCTION

The cloud is an enduring new computing paradigm driven by greater specialization and industrialization in the space. Cloud adoption rates have risen rapidly on the back of the tremendous economies of scale that service outsourcing unleashes for users and providers. The popularity of multicast has grown considerably with the wide use of the Internet, as well as the increasing demand

ISSN: 2320-1363

for group-based applications such as online forums, pay per view channels (PPV), various information dissemination services (such as news, weather, or share prices updates), as well as multimedia conferences including video and audio conferencing. The popularity of multicast has grown considerably with the wide use of the Internet, as well as the increasing demand for group-based applications such as online forums, pay per view channels (PPV), various information dissemination services (such as news, weather, or share prices updates), as well as multimedia conferences including video and audio conference. These pre-multicast era applications are called applications that emulate group communication.

In these applications, very simple group communication mechanisms are implemented in the applications themselves, but not supported by the communication system that underlies them. While this seems to outdate the need for a multicast function, its implementation and performance are very simple. These were literally designed to emulate group communication properties in the application itself. One example is Electronic Mail Systems that allow you to send the same message to groups of recipients, who are normally specified through mailing lists.

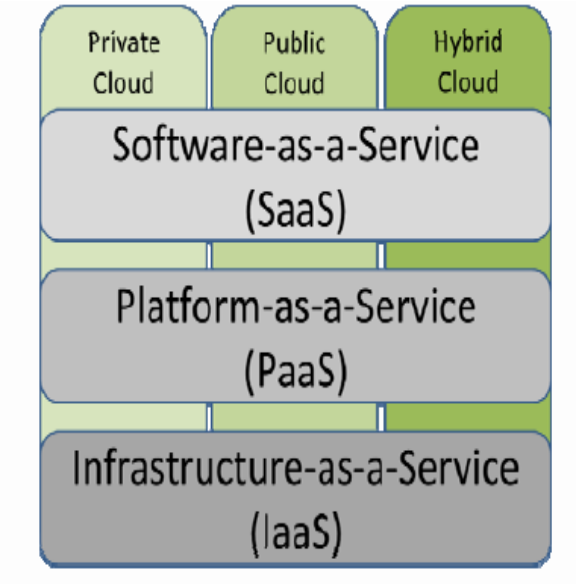


**Fig.1.1 Abstract Model View of Cloud Computing**

Other examples are the distribution of news, chatting on the Internet (such as the Internet Relay Chat (IRC)), as well as game servers that allow web users to play games like Backgammon, Chess and Life together on the Internet.

## II.RELATED WORK

The cloud is essentially the next link in the evolutionary chain after software as a service (delivery of software over the Internet) and grid computing (central pooling and sharing of high-performance These tunnels are particularly useful in many conventional unicast networks where many network routers are not multicast capable. For this to work, both end routers (nearest to a group of multicast hosts) need

ISSN: 2320-1363

to be multicast capable routers, and IP packets that are addressed to a multicast group are tunneled between these multicast routers. In practice, the datagram of a multicast group is encapsulated into another IP datagram by the nearest multicast router, and sent across the network through one (or more) unicast routers as unicast datagram, which then forward it to the next multicast router of another multicast. While the problem of hosts joining seems to be straightforward (if the provision of backward secrecy is not necessary) and distribution of new cryptographic keys can be supported by the old cryptographic keys, group members leaving poses a much more difficult scalability problem. If the provision of forward secrecy is necessary, new keying material must be sent to the remaining group members in a way that excludes the leaving member. One method that can be used is to send the key updates to each group member separately (each of which is protected by an individual key).

This creates a scalability problem if the group is large and/or has a very dynamic group membership group. In this protocol, an existing member leaving a multicast group is conducted with no provision of forward secrecy. This means that when a member leaves a multicast group it requires no further processing.

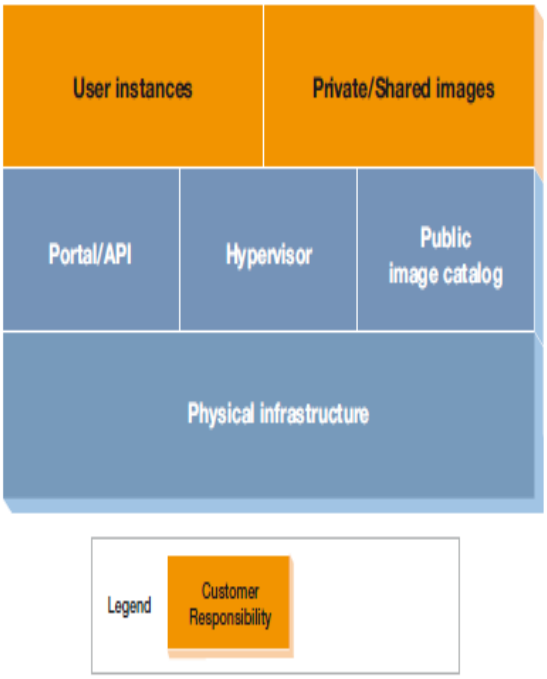


**Fig.2.1 Related Instance of the Hypervisor**

A member is excluded from a group and the reason of leaving is logged in List. We have assumed that there is an established multicast group.

## III.PROPOSED METHODOLOGY

Since providers centrally pool services such as e-mail, database applications or security solutions for a large number of users, they tap into vast economies of scale and can pass these savings on to customers. Users appreciate the simplicity and efficiency of cloud computing. They merely plug right into a sophisticated system – there is no need for

ISSN: 2320-1363

capital investment on their part. Not that cloud computing is entirely effort-free: organizations still need to define the specifications for their business and lay them out in a contract with the provider. Overall, the cloud offers compelling business benefits, provided rigorous security is in place. For identity management, Enterprise relies on the standard Web Identity system that has developed and deployed for all users of systems. This system allows users to create and manage IDs and includes tools for password maintenance. Once a client has signed up for the service, the ID specified during the sign-up process is assigned as the enterprise account administrator. Through the Enterprise self-service portal, the account administrator has the ability to add, delete and modify additional user IDs that can be used to provision cloud resources (instances, images, storage, and so on). It is the client's responsibility to manage all account user IDs based upon their own requirements (for example, approval process for adding an ID, revalidation of IDs, and so on). A new key generation scheme was proposed that allows a set of mutually suspicious members to generate a common secret. The scheme also lets the members generate the common secret without having to expose their individual secrets. In this scheme, we assumed that there is a third party to initiate the key generation procedure. Every key generating member is given an initial pad and a group binding parameter that is the sum of all the pads. Members generate individual shares called fractional keys, use the individual pads to create hidden fractional keys, and exchange the hidden fractional keys. Every member then combines the hidden fractional shares to generate the hidden common key/secret. The group binding parameter is then used to remove the combined effect of all the pads, and extract the new common key/secret. key distribution was proposed that made use of basic concepts from information theory. In doing so, we also showed that the best, or optimal, strategy that minimizes the number of keys to be stored while minimizing the number of updated messages as well, is equivalent to the optimal selection of codeword length. We further showed that the solution obtained using concepts from information theory does not prevent collusion. This point is demonstrated by considering the recent proposal by researchers at IBM Corporation, and showing that their results correspond to optimal selection of codeword length selection but lead to member collusion. We also presented the condition that prevents user collusion from compromising a valid member.

ISSN: 2320-1363

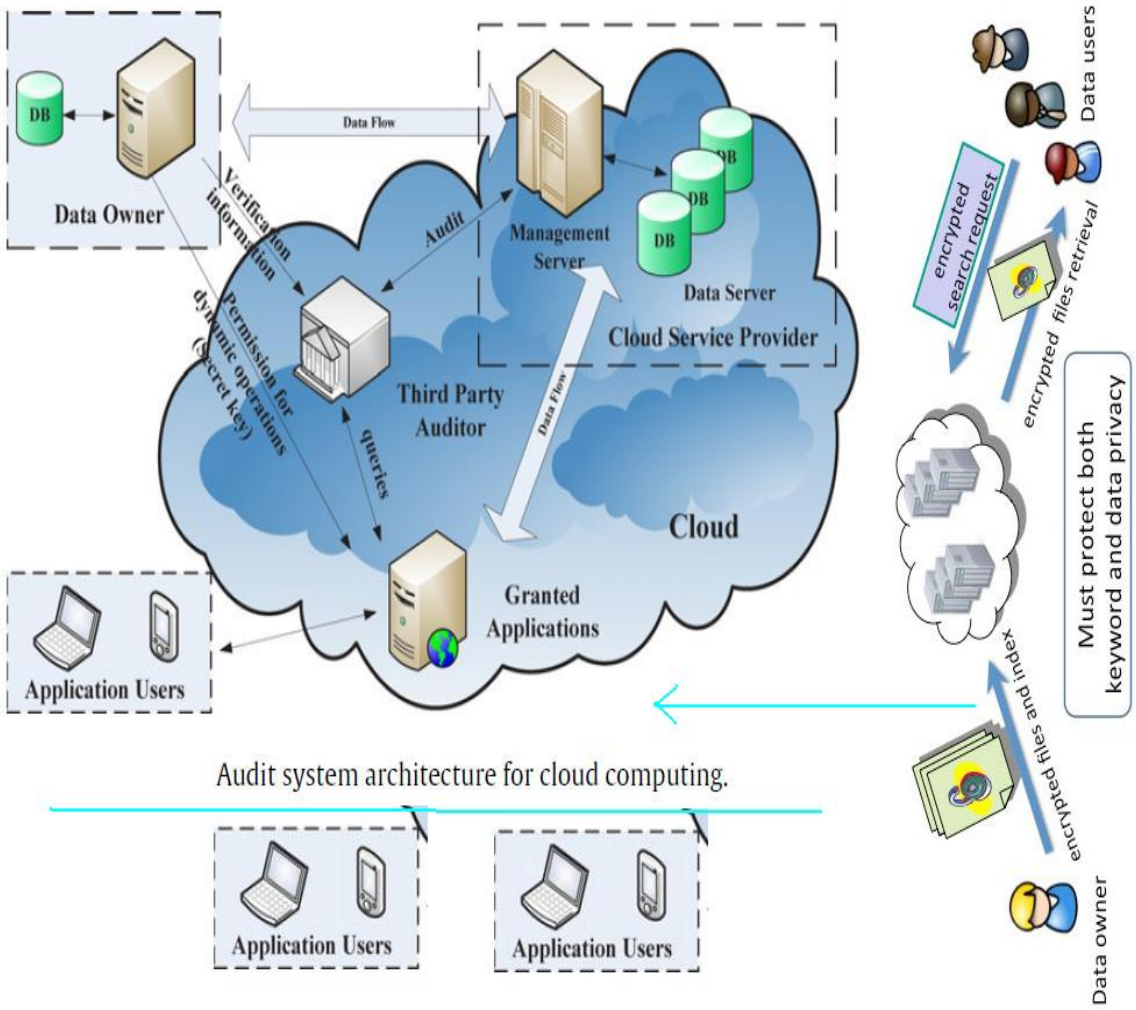


**Fig. 3.1 Architecture Model View of the privacy Based Data Security in Public Cloud**

We then showed that the use of entropy also allows one to group members into clusters with each cluster having equal probability of being. These tunnels are particularly useful in many conventional unicast networks where many network routers are not multicast capable. For this to work, both end routers (nearest to a group of multicast hosts) need to be multicast capable routers, and IP packets that are addressed to a multicast group are tunneled between these multicast routers. In practice, the datagram of a multicast group is encapsulated into another IP datagram by the nearest multicast router, and sent across the network through one (or more) unicast routers as unicast datagram, which then forward it to the next multicast router of another multicast group.

ISSN: 2320-1363

Key updates must be done securely, since a new set of key materials may need to be distributed whenever a key compromise is suspected, the current keys expire, or whenever there is a change in group membership. Group members need to be informed by the managing entity(s) whenever there is a change in the key materials that they are using and when key updates are on the way. The re-keying process should be conducted without disrupting any ongoing communication.

## IV.EVOLUTION AND ANALYSIS

Re-keying due to group membership change is contained. In general, scalability problems are reduced by designing the architecture in such a way that any changes in group membership in a particular area do not go beyond that area, and other areas are not affected by the change. For example, during the new member joining protocol (with provision for backward secrecy) only the area key where the new join occurs needs to be re-keyed. We have assumed that freshness of messages received is provided using some forms of time variant parameter such as a time stamp. Thus, if an adversary intercepts and later re-sends the message with an old time stamp, the intended recipient of the data would know that the time stamp received

## V.CONCLUSION AND FUTUR WORK

In today's evolving information economy, cloud computing offers immense opportunity. Whether companies have started their cloud journey or not, security concerns remain the largest inhibitor to adoption. Concerns around control, data privacy, and security abound. However, the technology and expertise required to build a trusted cloud is closer than imagined. Progressive CSOs are embracing a new strategic role as a true business enabler in partnership with business leaders, to make sure that the trusted cloud becomes a reality and enterprises can capitalize on cloud technology**.** A particular security service that is specific to multicast group communication is the provision of confidentiality with respect to backward and forward secrecy.

## VI.REFERENCES

[1] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A Privacy- Preserving Approach to Policy-Based Content Dissemination," Proc. IEEE 26th Int'l Conf. Data Eng. (ICDE '10), 2010.

[2]"LibertyAlliance," http://www.projectliberty.org/, 2013.

[3] "OpenID," http://openid.net/, 2013.

[4] "Microsoft Windows CardSpace," http://msdn.microsoft.com/ en-us/library/aa480189.aspx, 2013.

ISSN: 2320-1363

[5] "Higgins Open Source Identity Framework," http://www. eclipse.org/higgins/, 2013.

[6] R. Richardson, "CSI Computer Crime and Security Survey," http://www.ppclub.org/CSIsurvey2008.pdf, technical report, Computer Security Inst., 2008.

[7] Y. Challal and H. Seba, "Group key Management Protocols: A Novel Taxonomy," Int'l J. Information Technology, vol. 2, no. 2, pp. 105-118, 2006.

[8] H. Harney and C. Muckenhirn, "Group key Management Protocol (GKMP) Specification," technical report, Network Working Group, United States, 1997.

[9] H. Chu, L. Qiao, K. Nahrstedt, H. Wang, and R. Jain, "A Secure Multicast Protocol with Copyright Protection," SIGCOMM Computer Comm. Rev., vol. 32, no. 2, pp. 42-60, 2002.

[10] C. Wong and S. Lam, "Keystone: A Group Key Management Service," Proc. Int'l Conf. Telecomm. (ICT), 2000.

[11] A. Sherman and D. McGrew, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees," IEEE Trans. Software Eng., vol. 29, no. 5, pp. 444-458, May 2003.

[12] G. Chiou and W. Chen, "Secure Broadcasting Using the Secure Lock," IEEE Trans. Software Eng., vol. 15, no. 8, pp. 929-934, Aug. 1989.

[13] S. Berkovits, "How to Broadcast a Secret," Proc. 10th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT '91), pp. 535-541, 1991.

[14] X. Zou, Y. Dai, and E. Bertino, "A Practical and Flexible Key Management Mechanism for Trusted Collaborative Computing," Proc. IEEE INFOCOM, pp. 538-546, Apr. 2008.

[15] A. Shamir, "How to Share a Secret," Comm. ACM, vol. 22, no. 11, pp. 612-613, 1979.

[16] E.F. Brickell, "Some Ideal Secret Sharing Schemes," Proc. Workshop the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '89), pp. 468-475, 1990.

[17] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A Privacy- Preserving Approach to Policy-Based Content Dissemination," Proc. IEEE 26th Int'l Conf. Data Eng. (ICDE '10), 2010