International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# COPY RIGHT



IJIEMR Transactions, online available on 2nd June 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-3

Title: Privacy secure scheme for cloud based multimedia content storage

Volume 06, Issue 03, Pages: 565 – 572.

Paper Authors

***K.RAJESWARI, M VENKATESH NAIK, M SHIVALAKSHMI.**

*St.Mark Educational Institution Society Group of Institution, Ap, India.


USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

# Privacy secure scheme for cloud based multimedia content storage

**K.RAJESWARI[1], M VENKATESH NAIK[2] M SHIVALAKSHMI[3]**

[1]PG Scholar, CSE, St. Mark Educational Institution Society Group of Institution, AP, India
[2]Assistant Professor, CSE, St. Mark Educational Institution Society Group of Institution, Ap, India
[3]Assistant Professor, CSE, St. Mark Educational Institution Society Group of Institution, AP, India

**Abstract**—We propose a new design for large-scale multimedia content protection systems. Our design leverages cloud infrastructures to provide cost efficiency, rapid deployment, scalability, and elasticity to accommodate varying workloads. The proposed system can be used to protect different multimedia content types, including 2-D videos, 3-D videos, images, audio clips, songs, and music clips. The system can be deployed on private and/or public clouds. Our system has two novel components: (i) method to create signatures of 3-D videos, and (ii) distributed matching engine for multimedia objects. The signature method creates robust and representative signatures of 3-D videos that capture the depth signals in these videos and it is computationally efficient to compute and compare as well as it requires small storage. The distributed matching engine achieves high scalability and it is designed to support different multimedia objects. We implemented the proposed system and deployed it on two clouds: Amazon cloud and our private cloud. Our experiments with more than 11,000 3-D videos and 1 million images show the high accuracy and scalability of the proposed system. In addition, we compared our system to the protection system used by YouTube and our results show that the YouTube protection system fails to detect most copies of 3-D videos, while our system detects more than 98% of them. This comparison shows the need for the proposed 3-D signature method, since the state-of-the-art commercial system was not able to handle 3-D videos.

## 1.INTRODUCTION

Cloud computing is using computing resources (hardware and program) that are delivered as a service over a network (commonly the web). The identify comes from the original use of a cloud-formed image as an abstraction for the difficult infrastructure it comprises in system diagrams. Cloud computing entrusts far flung offerings with a user's data, program and computation. Cloud computing consists of hardware and software resources made to be had on the net as managed third-social gathering services. These services most commonly provide entry to evolved application functions and excessive-end network of the server.

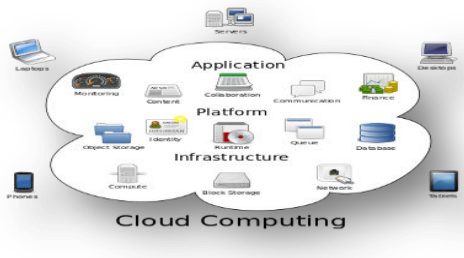


Fig.1.1 Structure of Cloud Computing

### 1.1 How Cloud Computing Works?

The intention of cloud computing is to use usual supercomputing, or excessive-

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

performance computing power, typically used by military and research facilities, to participate in tens of trillions of computations per 2nd, in client-oriented functions equivalent to financial portfolios, to provide personalized know-how, to furnish information storage or to vigor massive, immersive computer games.The cloud computing uses networks of colossal groups of servers mostly jogging low-cost patron pc technology with specialized connections to unfold data-processing chores across them. This shared IT infrastructure comprises giant pools of methods that are linked collectively. Commonly, virtualization strategies are used to maximize the power of cloud computing.

### 1.2 Characteristics and Services Units

The salient characteristics of cloud computing based on the definitions supplied by way of the countrywide Institute of standards and Terminology (NIST) are outlined below:

**1.3.1 On-Demand Self-Carrier:** A patron can unilaterally provision computing capabilities, similar to server time and community storage, as wanted robotically without requiring human interplay with each provider's provider.

**1.3.2 Extensive Network Entry:** Capabilities are on hand over the network and accessed through general mechanisms that promote use with the aid of heterogeneous thin or thick client systems (e.g., cellular phones, laptops, and PDAs).

**1.3.3 Resource Pooling:** The supplier's computing assets are pooled to serve a couple of buyers utilizing a multi-tenant mannequin, with exceptional physical and virtual resources dynamically assigned and reassigned in step with patron demand. There's a experience of location-independence in that the purchaser more commonly has no manipulate or potential over the precise place of the provided assets however is also ready to specify vicinity at a better degree of abstraction (e.g., country, state, or knowledge center).

**1.3.4 Rapid Elasticity:** Capabilities can be quickly and elastically provisioned, in some cases mechanically, to speedily scale out and quickly released to rapidly scale in. To the purchaser, the capabilities on hand for provisioning commonly appear to be unlimited and will also be purchased in any wide variety at any time.

**1.3.5 Measured Service:** Cloud programs mechanically manage and optimize useful resource use with the aid of leveraging a metering potential at some level of abstraction right to the form of service (e.g., storage, processing, bandwidth, and lively consumer accounts). Useful resource utilization can be managed, managed, and stated offering transparency for each the provider and consumer of the utilized service.


Fig.1.3 Characteristics of Cloud Computing

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

### 1.3 Services Models

Cloud Computing includes three distinct service models, namely Infrastructure-as-a-service (IaaS), Platform-as-a-provider (PaaS), and application-as-a-service (SaaS). The three service models or layer are accomplished by an finish user layer that encapsulates the end person standpoint on cloud offerings. The mannequin is shown in determine beneath. If a cloud person accesses offerings on the infrastructure layer, for instance, she will be able to run her possess functions on the assets of a cloud infrastructure and stay accountable for the help, maintenance, and protection of those functions herself. If she accesses a service on the appliance layer, these tasks are often looked after by using the cloud provider supplier.Multi-authority which seems in some way contradictory to the long-established goal of distributing manipulate over many probably entrusted writer-it. In addition, in that construction, the use of a steady GID allowed the authorities to combine their knowledge to construct a full profile with all of a user's attributes, which unnecessarily compromises the privatives of the user. In this paper, we endorse an answer which eliminates the depended on valuable authority, and protects the customers ' privatives with the aid of stopping the authorities from pooling their know-how on specified customers, for this reason making ABE extra usable in follow.This chapter presents a threshold multi authority fuzzy identity centered encryption (MA-FIBE) scheme and not using a primary authority for the first time. An encrypt or can encrypt a message such that a user might simplest decrypt if he has at the least d okay of the given attributes about the message for a minimum of $t+1$, $t \leq n/2$ sincere authorities of all the n attribute authorities

### 2.1 Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

As more sensitive knowledge is shared and saved through 0.33-get together web sites on the net, there will likely be a must encrypt data saved at these web sites. One difficulty of encrypting knowledge is that it may be selectively shared most effective at a rough-grained degree (i.e, giving a different occasion your confidential key). Strengthen a new cryptosystem for best-grained sharing of encrypted data that we name Key-coverage Attribute-founded Encryption (KP-ABE). In our cryptosystem, cipher texts are labeled with units of attributes and confidential keys are related to entry buildings that manipulate which cipher texts a consumer is able to decrypt.

### 2.2 Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

Attribute situated encryption (ABE) [13] determines decryption capability based on a person's attributes. In a multi-authority ABE scheme, a couple of attribute-authorities reveal fluctuate-ent sets of attributes and challenge corresponding decryption keys to users, and encryptions can require that a user obtain keys for right attributes from each authority be-fore decrypting a message. Chase [5] gave a multi-authority ABE scheme utilizing the

ideas of a trusted primary authority (CA) and global identifiers (GID). Nonetheless, the CA in that building has the vigor to decrypt every cipher text, which seems in some way contradictory to the long-established goal of distributing manipulate over probably entrusted writers.

### 2.3 Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority

An attribute headquartered encryption scheme (ABE) is a cryptographic primitive where each consumer is recognized by using a suite of attributes, and a few perform of these attributes is used to examine the capacity to decrypt each and every cipher text. Chase proposed the first multi authority ABE scheme in TCC 2007 as an answer to an open drawback awarded through Sahai and Waters in EUROCRYPT 2005. Nonetheless, her scheme needs a fully trusted vital authority which can decrypt every cipher text in the process. This relevant authority would endanger the whole method if it's corrupted.

### 2.4 Multi-Authority Attribute-Based Encryption with Honest-But-Curious Central Authority

An attribute-founded encryption scheme able of dealing with a couple of authorities was just lately proposed via Chase. The scheme is developed upon a single-authority attribute-situated encryption scheme provided earlier via Sinai and Waters. Chase's construction uses a depended on central authority that's inherently ready of decrypting arbitrary cipher texts created inside the approach. We gift a multi-authority attribute-situated encryption scheme where only the set of recipients outlined by way of the encrypting occasion can decrypt a corresponding cipher text. The critical authority is viewed as 'honest-however-curious': on the one hand, it actually follows the protocol, and however, it's curious to decrypt arbitrary cipher texts for this reason violating the intent of the encrypting party.

## 3.1 Existing System

Existing techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it.

- Few years later, Fuzzy Identity-Based Encryption is proposed, which is also known as Attribute-Based Encryption (ABE).
- The work by Lewko *et al.* and Muller *et al.* are the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple ones.
- Lewko *et al.* use a LSSS matrix as an access structure, but their scheme only converts the AND, OR gates to the LSSS matrix, which limits their encryption policy to Boolean formula, while we inherit the flexibility of the access tree having threshold gates.
- Muller *et al.* also supports only Disjunctive Normal Form (DNF) in their encryption policy.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

### 3.2 Disadvantages of Existing System

- The identity is authenticated based on his information for the purpose of access control.
- Preferably, any authority or server alone should not know any client's personal information.
- The users in the same system must have their private keys re-issued so as to gain access.
- In this setting, each authority knows only a part of any user's attributes, which are not enough.
- The sender of a message can specify an identity such that only a receiver

### 3.3 Proposed System

- The data confidentiality, less effort is paid to protect users' identity privacy during those interactive protocols. Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes.
- In this propose Annoy Control and Annoy Control-Fallow cloud servers to control users' access privileges without knowing their identity information. In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity. The scheme proposed by Chase et al. considered the basic threshold-based KP-ABE. Many attribute based encryption schemes having multiple authorities have been proposed afterwards.
- In our system, there are four types of entities: *N Attribute Authorities* (denoted as *A*), *Cloud Server*, *Data Owners* and *Data Consumers*. A user can be a Data Owner and a Data Consumer simultaneously.

### 3.4 Advantages of Proposed System

- The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in *Annoy Control* and no information is disclosed in *Annoy Control-F*.
- The proposed schemes are tolerant against authority compromise, and compromising of up to $(N-2)$ authorities does not bring the whole system down.
- We provide detailed analysis on security and performance to show feasibility of the scheme *Annoy Control* and *Annoy Control-F*.
- We firstly implement the real toolkit of a multi authority based encryption scheme *Annoy Control* and *Annoy Control-F*

### 3.5 System Architecture

The system supports different types of multimedia content and can effectively utilize varying computing resources. Method for creating signatures for videos. This method creates signatures that capture the depth in stereo content without computing the depth signal itself, which is a computationally expensive process. New design for a distributed matching engine for high-dimensional multimedia objects. This design provides the primitive function of

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

finding -nearest neighbors for large-scale datasetsIn our system, there are four types of entities: *N Attribute Authorities* (denoted as *A*), *Cloud Server*, *Data Owners* and *Data Consumers*. A user can be a Data Owner and a Data Consumer simultaneously

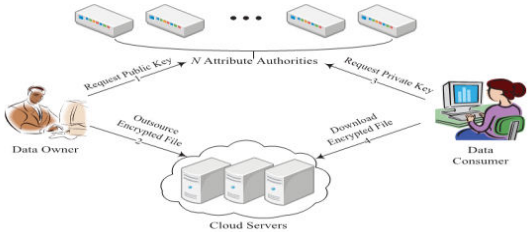


Fig.3.5.1 System Architecture

Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

**Execution Results:**


Fig 7.2.1 Home Page

The above Fig 7.2.1 shows the home page of the cloud data access privilege and anonymity with fully anonymous attribute based encryption.

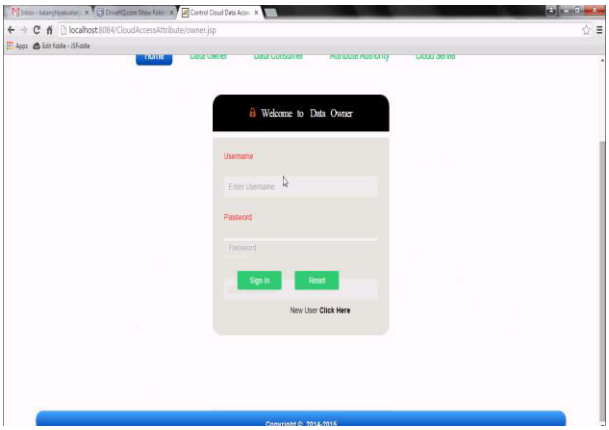


Fig 7.2.2 Data Owner Window Login Page

The above Fig 7.2.2 shows a form for data owner who can already get a authentication from authority. To enter their user name and password and sign in to cloud for uploading their files.


Fig 7.2.3 Data Owner Logged Windo

The above fig 7.2.3 shows the data owner's logged account, where he can change the password because previously logged by system generated password for the security purpose. After that data owner will request the Attribute authority for uploading the data in the cloud.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

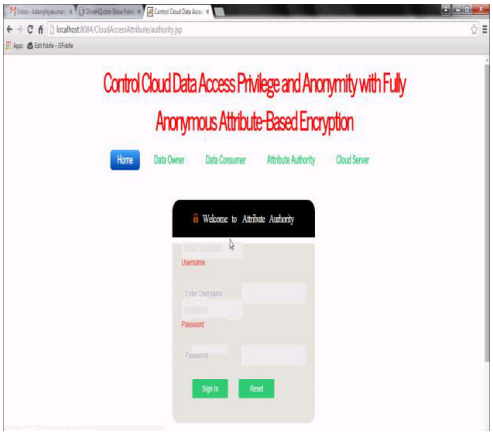


Fig 7.2.4 Cloud Access Attribute for Authority

The above Fig 7.2.4 shows that the login form for authority who can give the authentication for the Data Owne

## Conclusion

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. More importantly, our system can tolerate up to N − 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that Annoy-Control both secure and efficient for cloud storage system. The AnonyControl-F
directly inherits the security of the Annoy Control and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes who support efficient user revocation is one of our future works.

## References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE SP, May 2007, pp. 321–334.

[5] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[6] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-

authority attribute-based encryption," in Proc. 16th CCS, 2009, pp. 121–130.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[8] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in Proc. IEEE 7th SOSE, Mar. 2013, pp. 573–577.

[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2895–2903.

[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[12] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," Bull. Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009.

[13] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext-policy attribute-based encryption with accountability," in Proc. 6th ASIACCS, 2011, pp. 386–390.

[14] H. Ma, G. Zeng, Z. Wang, and J. Xu, "Fully secure multi-authority attribute-based traitor tracing," J. Comput. Inf. Syst., vol. 9, no. 7, pp. 2793–2800, 2013