Secure Sharing of Contents using Broadcast Group Key Management

[1]Vijayasharmila. S, [2]Thulasi. R, [3]Sibhimathy. VS, [4]Nimeshika. R

[1]Assistant Professor, [2,3,4]Students
Information Technology Department
K.L.N College of Engineering, Sivagangai, Tamil Nadu, India.

***Abstract*: An important problem in public clouds is how to selectively share documents based on fine-grained attribute-based access control policies. An approach is to encrypt documents satisfying different policies with different keys using a public-key cryptosystem such as attribute-based encryption (ABE), and/or proxy re-encryption (PRE). However, such an approach has some weaknesses: it cannot efficiently handle adding/revoking users or identity attributes, and policy changes; it requires keeping multiple encrypted copies of the same documents; it incurs high computational costs. A direct application of asymmetric key cryptosystem, where users are grouped based on the policies they satisfy and assigning unique keys for each group, also has similar weaknesses. Without utilizing public-key cryptography and by allowing users to dynamically derive the symmetric keys at the time of decryption, one can address the above weaknesses. Based on this idea, a new key management scheme called broadcast group key management (BGKM) is proposed and then gives a secure construction of a BGKM scheme called ACV-BGKM. The idea is to give some secrets to users based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets and some public information. A key advantage of the BGKM scheme is that adding users/revoking users or updating access control policies can be performed efficiently by updating only some public information.**

***Index Terms*: Searchable encryption, fine-grained search, authorization, dynamic access policy.**

INTRODUCTION:

Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Services (AWS). Organizations of every type, size, and industry are using the cloud for a wide variety of use cases, such as data backup, disaster recovery, email, virtual desktops, software development, and testing, big data analytics, and customer-facing web applications. For example, healthcare companies are using the cloud to develop more personalized treatments for patients. Financial services companies are using the cloud to power real-time fraud detection and prevention. And video game makers are using the cloud to deliver online games to millions of players around the world. The three main types of cloud computing include Infrastructure as a Service, Platform as a Service, and Software as a Service. Each type of cloud computing provides different levels of control, flexibility, and management so that you can select the right set of services for your needs.

MOTIVATION OF THE PROJECT:

A new key management scheme called broadcast group key management (BGKM) is proposed and then gives a secure construction of a BGKM scheme called ACV-BGKM. The idea is to give some secrets to users based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets and some public information. A key advantage of the BGKM scheme is that adding users/revoking users or updating access control policies can be performed efficiently by updating only some public information.

PROBLEM STATEMENT:

With the involvement of third-party cloud services, a crucial issue is that the identity attributes in the access control policies often reveal privacy-sensitive information about users and leak confidential information about the content. The confidentiality of the content and the privacy of the users are thus not fully protected if the identity attributes are not protected. Further, as insider threats are one of the major sources of data theft and privacy breaches, identity attributes must be strongly protected even from access within organizations. Therefore, protecting the identity attributes of the users while enforcing attribute-based access control both within the organization as well as in the cloud is crucial.

LITERATURE SURVEY:

1. Privacy-Preserving Searchable Encryption with Fine-grained Access Control

Author: Payal Chaudhari, Manik Lal Das

Findings:

Searchable encryption facilitates cloud servers to search over encrypted data without decrypting the data. Single keyword-based searchable encryption enables a user to access a subset of documents, which contains the keyword of the user’s interest. In this paper, we present a single keyword-based searchable encryption scheme for the applications where multiple data owners upload their data, and then multiple users can access the data. The scheme uses attribute-based encryption that allows the user to access the selected subset of data from the loud without revealing /her access rights to the cloud server. The scheme is proven adaptively secure against chosen-keyword attacks in the random oracle model. We have implemented the scheme on the Google cloud instance and the performance of the scheme was found to practice in real-world applications.

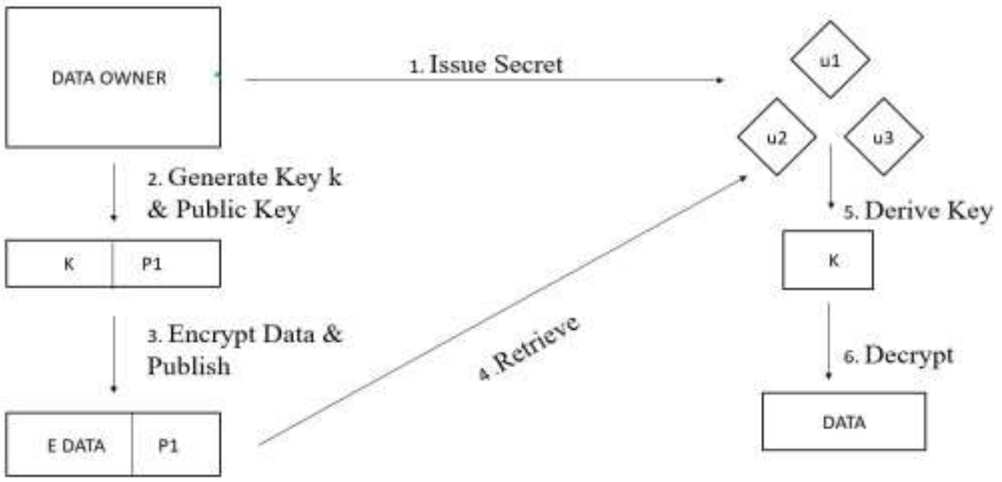
2. A2 BSE: Anonymous Attribute-Based Searchable Encryption
Author: Payal Chaudhari, Manik Lal Das
Findings:
Attribute-Based Encryption (ABE) allows fine-grained access control along with data confidentiality. Anonymous Attribute-Based Encryption (AABE) supports hiding the access control policies within ciphertext so that the receiver's information remains unknown to the public. Keyword-based query search over encrypted storage has become a challenging research problem when (i) the search query should not reveal the user identity and (ii) the search procedure should be able to verify whether the access policy is associated with the cipher document matches with the user's access rights. In this paper, we present an anonymous attribute-based searchable encryption (A2BSE) scheme that allows the user to retrieve only a subset of documents, containing the keyword(s) that satisfies the user's search query and for which the user is having sufficient access rights. In the A2BSE scheme, the search operation does not reveal the user's identity. The A2BSE scheme is secure under the selective ciphertext policy with a chosen-plaintext attack and the selective ciphertext policy with chosen keyword attack. The A2BSE scheme is efficient in comparison to existing AABE schemes.

3. Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage
Author: Kaitai Liang and Willy Susilo
Findings:
To date, the growth of electronic personal data leads to a trend that data owners prefer to remotely outsource their data to clouds for the enjoyment of the high-quality retrieval and storage service without worrying about the burden of local data management and maintenance. However, secure share and searching for outsourced data is a formidable task, which may easily incur the leakage of sensitive personal information. Efficient data sharing and searching with security is of critical importance. This paper, for the first time, proposes a searchable attribute-based proxy re-encryption system. When compared to existing systems only supporting either searchable attribute-based functionality or attribute-based proxy re-encryption, our new primitive supports both abilities and provides a flexible keyword update service. Specifically, the system enables a data owner to efficiently share his data to a specified group of users matching a sharing policy meanwhile, the data will maintain its searchable property but also the corresponding search keyword(s) can be updated after the data sharing. The new mechanism applies to many real-world applications, such as electronic health record systems. It is also proved that chosen ciphertext is secure in the random oracle model.

4. DABKS: Dynamic Attribute-based Keyword Search in Cloud Computing
Author: Baishuang Hu , Qin Liu, Xuhui Liu, Tao Peng, Guojun Wang, Jie Wu
Findings:
Due to its fast deployment and scalability, cloud computing has become a significant technology trend. Organizations with limited budgets can achieve great flexibility at a low price by outsourcing their data and query services to the cloud. Since the cloud is outside the organization's trusted domain, existing research suggests encrypting data before outsourcing to preserve user privacy. Two main problems that the cloud user faces while searching over encrypted data are how to achieve a fine-grained search authorization and how to efficiently update the search permission. The existing attribute-based keyword search (ABKS) scheme addresses the first problem, which allows a data owner to control the search of the outsourced encrypted data according to an access policy. This paper proposes a dynamic attribute-based keyword search (DABKS) scheme that incorporates proxy re-encryption (PRE) and a secret sharing scheme (SSS) into ABKS. The DABKS scheme, which allows the data owner to delegate policy updating operations to the cloud, takes full advantage of cloud resources. We conduct experiments on real data sets to validate the effectiveness and efficiency of our proposed scheme.

PROPOSED SYSTEM:
Without utilizing public-key cryptography and by allowing users to dynamically derive the symmetric keys at the time of decryption, one can address the group key management issues. Based on this idea, a new GKM scheme called broadcast GKM(BGKM) then gives a secure construction of the BGKM scheme and formally proves its security. A key advantage of the BGKM scheme is that adding users/revoking users or updating access control policies can be performed efficiently and only requires updating the public information.

SYSTEM ARCHITECTURE:



ADVANTAGES:

- Maximum trust
- Key indistinguishability
- Key independence
- Forward secrecy
- Backward secrecy and
- Minimal computational, space, and communication costs.

LIMITATIONS:

- **Scalability:** Managing a large number of encryption keys.
- **Security:** Vulnerability of keys from outside hackers, malicious insiders.
- **Availability:** Ensuring data accessibility for authorized users.
- **Heterogeneity:** Supporting multiple databases, applications and standards.
- **Governance:** Defining policy-driven access control and protection for data.

SYSTEM REQUIREMENTS:

SOFTWARE REQUIREMENTS:

Operating system	: Windows XP.
Coding Language	: ASP.Net with C#.
Data Base	: SQL Server 2005

HARDWARE REQUIREMENTS:

System	: Pentium IV 2.4 GHz.
Hard Disk	: 40 GB.
Floppy Drive	: 1.44 Mb.
Monitor	: 15 VGA Colour.
Mouse	: Logitech.
RAM	: 512 Mb

CONCLUSIONS:

Broadcast group key management (BGKM) has been studied and proved the security of the BGKM scheme, ACV-BGKM scheme. Optimizations to significantly improve the performance of the ACV-BGKM scheme have been done. Based on the BGKM scheme, an approach to support attribute-based access control is proposed while preserving the privacy of users' identity attributes for sharing documents in an untrusted cloud storage service. It is supported by a new group key management scheme which is secure and allows qualified users to efficiently extract decryption keys for the portions of documents they are allowed to access, based on the subscription information they have received from the data owner. The scheme efficiently handles joining and leaving of guaranteed, with guaranteed security. Experimental results show that users efficiently derive decryption keys, and the data owner can efficiently a large number of users.

REFERENCES:

BASE PAPER:

https://ieeexplore.ieee.org/document/8607030/authors#authors

ADDITIONAL REFERENCES:

[1] R. Richardson, "CSI Computer Crime and Security Survey," http://www.ppclub.org/CSIsurvey2008.pdf, Computer Security Institute, Tech. Rep., 2008.

[2] Y.Challal and H.Seba, "Group key management protocols: A novel taxonomy," International Journal of Information Technology, vol. 2, no. 2, pp. 105–118, 2006.

[3] H. Chu, L. Qiao, K. Nahrstedt, H. Wang, and R. Jain, "A secure multicast protocol with copyright protection," SIGCOMM Comput. Commun. Rev., vol. 32, no. 2, pp. 42–60, 2002.

[4] C. Wong and S. Lam, "Keystone: a group key management service," in International Conference on Telecommunications, ICT, 2000.

[5] H. Harney and C. Muckenhirn, "Group key management-protocol(GKMP) specification," Network Working Group, United States, Tech. Rep., 1997.