International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 8 (2015) pp. 20613-20620

http://www.ripublication.com

Review Of Suitable Encryption For Cloud To Achieve Data Privacy And Access Control

A.Revathi and Dr. Paul Rodrigues

Assistant Professor,
PERI Institute of Technology, Chennai, Tamilnadu, India.
Professor and Principal,
DMI College of Engineering, Chennai, Tamilnadu, India.

Abstract

The computing industry has grown from mainframe computers to grid computing and to cloud computing. A hype has been created by cloud computing. Cloud computing is evolved from grid computing, autonomic and utility computing. It fosters a virtualized plinth with elastic resources on demand by provisioning hardware, software, and data sets dynamically. Though cloud computing advantages its low cost and simplicity to benefit users and providers, Security and privacy stands as an open challenge to the research community. The main aim of this is paper to address the challenges in cloud computing and to present a detailed analysis of various techniques employed to ensure the secrecy of the data stored in the cloud and the accessibility of the data.

Index Terms— Access Control, Cloud Computing, Encryption, Security, Privacy. Key revocation.

I. INTRODUCTION

In recent time much importance is paid to cloud computing research. With internet connection the user can outsource both data and computations to cloud. A cloud can host variety of different workloads, including batch –style backend jobs and interactive and user facing applications. Cloud computing applies a virtualized platform with elastic resources on demand by provisioning hardware, software, and data sets dynamically. Cloud Computing has fascinated the giant companies like Google, Microsoft, and Amazon and considered as a great influence in today's Information Technology industry.

Business owners are attracted to cloud computing concept because of several features. This paper provides a better understanding of the cloud computing and identifies important Security and privacy issues in this burgeoning area of computer science.

Cloud Computing - Overview

Cloud model is composed of three service models, four deployment models and five vital characteristics.

Characteristics of cloud computing

Cloud computing exhibit five essential characteristics

1. **On-demand self-service**. A consumer can unilaterally provision computing capabilities.
2. **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
3. **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
4. **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.
5. **Measured service**. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

Deployment models

1. **Public cloud:** In Public cloud the computing infrastructure is hosted by the cloud vendor at the vendor's premises. The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations.
2. **Private cloud:** The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Some experts consider that private clouds are not real examples of cloud computing. Private clouds are more expensive and more secure when compared to public clouds. Private clouds are of two types: On-premise private clouds and externally hosted private clouds. Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than On-premise private clouds.
3. **Hybrid cloud:** Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud. A related term is Cloud Bursting. In Cloud bursting organization use their own computing infrastructure for normal usage, but access the cloud for high/peak

load requirements. This ensures that a sudden increase in computing requirement is handled gracefully.

4. **Community cloud**: It involves sharing of computing infrastructure in between organizations of the same community. For example all Government organizations within the state of California may share computing infrastructure on the cloud to manage data related to citizens residing in

Service models

Based upon the services offered, clouds are classified in the following ways:

1. **Infrastructure as a service (IaaS):** It involves offering hardware related services using the principles of cloud computing. These could include some kind of storage services (database or disk storage) or virtual servers. Leading vendors that provide Infrastructure as a service are Amazon EC2, Amazon S3, Rackspace Cloud Servers and Flexiscale.
2. **Platform as a Service (PaaS):** It involves offering a development platform on the cloud. Platforms provided by different vendors are typically not compatible. Typical players in PaaS are Google's Application Engine, Microsofts Azure, Salesforce.com's force.com.
3. **Software as a service (SaaS):** It includes a complete software offering on the cloud. Users can access a software application hosted by the cloud vendor on pay-per-use basis. This is a well-established sector. The pioneer in this field has been Salesforce.coms offering in the online Customer Relationship Management (CRM) space. Other examples are online email providers like Googles gmail and Microsofts hotmail, Google docs and Microsofts online version of office called BPOS (Business Productivity Online Standard Suite).

The remainder of this paper is organized as follows: Section II presents some of the Security Challenges in cloud adoption. In section III, we describe Survey on encryption techniques for cloud followed by survey on Predicate Encryption Techniques in section IV. Finally we conclude this paper in section V along with references.

II SECURITY CHALLENGES IN CLOUD ADOPTION

Some of the major concern which prevents many companies to go into cloud are

i) Lack of control of outsourced data
ii) Lack of trust
iii) Multitenancy

- **Lack of control:**

In cloud the data, applications and resources are placed with provider. The access control rules, security policies and user identity are managed by the cloud provider. Hence user depends on Cloud service Provider(CSP) to make sure

- Data security and privacy
- Availability of Resource
- Supervising and revamping of services/resources.

By applying suitable authentication techniques and access control mechanisms the customers of cloud service may retain control over the data.

- **Lack of Trust:**

In cloud the third party, that is the CSP is trusted for data integrity. Trusting a third party means taking Risk. Trust and Risk are opposite sides of the same coin. Using Service level Agreements (SLA's) and by enhancing rules and regulation Trust level may be increased.

- **Multitenancy:**

Multitenancy is the key attribute of cloud computing which allows multiple tenants to share the common set of resources at the same time. Strong isolation techniques are required to isolate different tenants.

We address some of the key challenges the data base owner and user face when they go for cloud.

Challenges faced by Data base owner:

- Securing outsourced data from theft by hackers or malfunctioning cloud server is a larger challenge..
- Protecting the outsourced data from exploitation by the cloud server is the other challenge.
- To be aware of fine-grained access control for users is difficult to achieve.

Challenges faced by user

- The user should query the cloud server, without revealing query details.
- Hiding the query contents from the database owner is the other issue.
- Hiding the query contents while assuring database owner the hidden contents are authorized by some certificate authority (CA).

To keep user data confidential, all data must be encrypted before transmitting into cloud. Existing Standard Encryption algorithms enforce some limitation on searching. It needs the whole document must be downloaded from cloud and then decrypt before query them. This reverses the benefits of cloud. A more attractive solution is to apply searchable encryption technique which allow the user to query the cloud database directly without decrypting them. In our next section we describe some of latest searchable encryption techniques for cloud computing.

III SURVEY ON ENCRYPTION TECHNIQUES FOR CLOUD

The following figure shows how search operations have been performed on outsourced data. Searchable encryption saves enormous network bandwidth and computation capacity for uses by supporting keyword search over encrypted data in the cloud server.

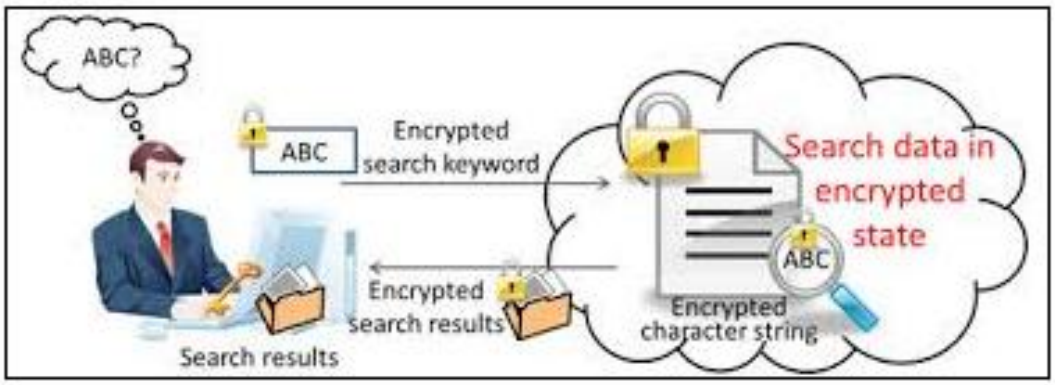

Fig 3.1 Search on encrypted data

High level of security is offered by conventional cryptosystems and they are mathematically strong. But they are inefficient to allow a large group of individuals to decrypt the data,. This is because they fix the target recipient beforehand and exchange secret keys to them in advance. These swallow the promising benefits of security, flexibility and efficiency which the cloud should provide. Visualize the following scenario: A project manager wants to share some data of a subtask with those who are working on it and with the managers of the project from the different companies. As the employees will leave or join in random time it is difficult to exchange keys among them. In 1984 Adi Shamir proposed a new cryptographic primitive called Identity Based encryption and the same was enhanced by Boneh–Franklin in 2001 which addresses the above issue. But IBE suffer by inherent key escrow and key revocation problem. Attribute-based encryption (ABE), a descendent of IBE proposed by Sahai and Waters is projected for one to-many encryption in which ciphertexts are encrypted for those who are able to fulfill certain requirements. Attribute-based encryption can be seen as a generalization of Identity-based Encryption. IBE uses a single attribute for key generation whereas ABE combines multiple attributes. The native ABE requires there should be at least k attributes out of n must be common between cipher text and the key the user posses. ABE derives two more flavors to remove threshold on common attributes. They are as follows.

i) CP-ABE.: Access policy is embodied in to ciphet text
ii) KP-ABE: access policy is embedded in to Secret key

KP-ABE is less secure than CP-ABE. Ciphertext policy - Attribute-Based Encryption (CP-ABE), solves key-escrow problem. The major drawback of ABE in cloud environment is that it reveals the key (KP-ABE) and attributes(CP-ABE) to the central authority. In predicate Encryption(PE) scheme the secret keys are associated with predicates and ciphertexts are bound to key attributes. A secret token, generated by the secret key owner corresponding to a predicate, can be given to a person as a search privilege. This person can make a search query through this secret token. The cloud server receives the search query from the secret key owner or from the above person, and then searches the matched ciphertexts if and only if the set of attributes of

the ciphertexts satisfies the predicate of the secret token ie if f(a)=1 then decryption will be successful. ABE also state the same requirement for decryption but fails to provide privacy for key attributes. PE technique ensures *"Attribute hiding"*. Predicate Encryption plays a more role in todays cloud environment. In our next section we conduct a detail survey on Predicate Encryption scheme.

Key Revocation Problem:

Within the context of PE key revocation is applicable to both access policies and attributes.The access privileges of a user dynamically varies. For example when user is leaving the system, it loses the access privileges of all data in the cloud, is called user revocation. When the user is degraded in the system, it loses some part of access privileges as some the attributes should be removed from it, which is called attribute revocation.

Requirement of attribute Revocation Method:

1. With the help of previous secret key the revoked user should not decrypt the newly generated ciphertext. This is called as Backward secrecy.
2. The newly joined user with sufficient attributes can still decrypt the older ciphertexts which were published before he joined the system. This is called Forward secrecy.

The attribute revocation scheme includes three phases:

i) Key generation Update by authority.
ii) Secret key Update for non revoked Users.
iii) Ciphertext Update by cloud server

Access Control Policy

Access control refers to managing identities, defining access policies, and controlling access to resources in secure manner. The Access control model is the key aspect of security which includes set of abstractions capable of expressing access policy statements for a wide range of information resources. There are three Access control schemes widely recognized. They are i) User Based Access control ii) Role Based Access control ii) Attribute Based Access control. Among the variety of access control methods, Attribute base access control mechanism is more suitable as we use predicates of attribute for encryption. This sceheme prevents replay attacks.

IV SURVEY ON PREDICATE ENCRYPTION TECHNIQUE

There are two class in predicate encryption:

i) secret-key predicate encryption schemes and
ii) public-key predicate encryption schemes.

However, everyone can encrypt using the public-key in public-key encryption. But in secret-key encryption, both encryption and decryption are performed using the secret-key. Hence, only the key owner can encrypt. But decryption is performed only

the secret-key owner in both the cases. secret-key predicate encryption scheme is suitable for single user environment whereas public-key predicate encryption scheme are for multi user environment.

1. ‘**Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products' by Jonathan Katz, Amit Sahai and Brent Waters I in 2008**
In their proposal predicates corresponding to the evaluation of inner products over ZN (for some large integer N) This, in turn, enables constructions in which predicates correspond to the evaluation of disjunctions, polynomials, CNF/DNF formulae, or threshold predicates (among others). These scheme provides attribute hiding and payload hiding. But they fail to address range queries in their inner product.

2. ‘Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds’ By Sushmita Ruj,, Milos Stojmenovic,, and Amiya Nayak in 2014.
In this paper they apply Attribute Based Encryption to provide security of the outsourced data. Bilinear pairing on elliptic curves groups is used. Two users cannot collude and create an access policy consisting of attributes shared between them. Their scheme uses decentralized access control technique with anonymous authentication. It also address user revocation and prevents replay attacks. One limitation is that the cloud knows the access policy for each record stored in the cloud.

3. Patient–Centric Secure Data Sharing Frame Work for Cloud-Based PHR Systems By Shaik.Musthafa, Dora Babu.Sudars in 2013.
They proposed fine-grained and scalable data access control for PHRs with the help of Ciphertext-Policy - Attribute-Based Encryption (ABE) techniques to encrypt each patient’s PHR file. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority ABE. It also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios systems. They fail to address attribute revocation problem and operations supported by search queries.

V CONCLUSION

Cloud computing have several benefits like higher resource utilization, elasticity, reducing IT cost or capital expenditure. The major barrier for cloud computing to enlarge its market is security and privacy of data stored at cloud. In our paper we address some of the techniques to break the barrier. A new cryptographic primitive called Predicate Encryption is well studied for use it in the cloud which supports anonymous authentication and key revocation problem. In our future work we fine-tune predicate encryption algorithm to speed up search process and to support access to range queries which are still hot points in research.

References

1. Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, 2014, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds " IEEE Transactions on Parallel and Distributed systems, vol. 25, PP 384-394.
2. Liang Hu, Yuanmo Zhang, Hongtu Li, Yicheng Yu, Fangming Wu, and Jianfeng Chu, 2014, "Challenges and Trends on Predicate Encryption—A Better Searchable Encryption in Cloud ", Journal of Communications Vol. 9, PP 908-915.
3. Chase and S.S.M. Chow, 2009 "Improving Privacy and Security in Multi-Authority Attribute- Based Encryption, " Proc. ACM Conf.Computer and Comm. Security, pp. 121-130.
4. M. Chase, 2007, "Multi-Authority Attribute Based Encryption, " Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.
5. D. Boneh and M. Franklin, 2001, "Identity-based encryption from the weil pairing, " in *Proc. 21st Annual International Cryptology Conference*, Santa Barbara, pp. 213-229
6. D. Boneh, A. Sahai, and B. Waters, 2011, "Functional encryption: Definitions and challenges, " in *Proc. 8th Conference on Theory of Cryptography*, Providence, pp. 253-273.
7. R. Wei and D. Ye, 2009, "Delegate predicate encryption and its application to anonymous authentication, " in Proc. 4th International Symposium on ACM Symposium on Information, Computer and Communications Security, Sydney, pp. 372-375.
8. Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance" O'Reilly Publications.
9. M. Li, S. Yu, K. Ren, and W. Lou, 2010, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings, " Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106.
10. J. Hur and D. Kun Noh, 2011, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems, " IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221.
11. V. Goyal, O. Pandey, A. Sahai, and B. Waters, 2006, "Attribute-based encryption for fine-grained access control of encrypted data, " in ACM CCS.
12. Jonathan Katz, Amit Sahai and Brent Waters, 2008, "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products", In: Advances in Cryptology EUROCRYPT, pp. 146-162.
13. Shaik.Musthafa, Dora Babu.Sudarsa, 2013, "Patient–Centric Secure Data Sharing Frame Work for Cloud-Based PHR Systems", International Journal of Engineering Science Invention. PP.17-26