Analysis of Cloud Storage & Emergence on Expressive words Searchable Encryption

Ms. CH. Hyma
Associate Professor
Dept. Of Computer Science And Engieering
Swami Vivekananda Institute Of Technology,Sec-Bad,Telangana,India.

Ms. M. Supriya
Associate Professor
Dept. Of Information Technology
Swami Vivekananda Institute Of Technology,Sec-Bad,Telangana,India.

Ms. M. Umadevi
Associate Professor
Dept. Of Information Technology
Swami Vivekananda Institute Of Technology,Sec-Bad,Telangana,India.

Abstract – *The term search encryption allows conducting keyword search over encrypted data on behalf of the data users without learning the underlying plaintexts in cloud environment. The most existing searchable encryption schemes only support single or conjunctive keyword search, while a few other schemes that are able to perform expressive keyword search are computationally inefficient since they are built from bilinear pairings over the composite-order groups. Our analysis shows the public-key searchable encryption scheme in the prime-order groups, which allows keyword search policies predicates, access structures to be expressed in conjunctive, disjunctive or any monotonic Boolean formulas and achieves significant performance improvement over existing schemes. One of the most important is Keyword researching, valuable, and high return activities in the search marketing field keywords can make or break your website.*

Keywords – Encryption, Cryptography, Cloud computing, Security, Expressive Keywords

Introduction I

Cloud computing is data processing service in the IT field offer cloud services to a range of customers from organizations of all sizes to individuals. Cloud computing serves to a range of customer from organizations of all sizes to individuals best cloud computing providers include Amazon with EC2 Microsoft with Azure and Google Apps, cloud computing described in simple terms as offering particular IT services that are hosted on the internet the most common ones being platform as a service, infrastructure as service and software as a service. As security and privacy issues are most important addressed before cloud computing establishes an important market issues are important should be addressed before cloud computing establishes an important market share. Two issues can lead to a number of legal and security concerns to infrastructure identity management access control risk management regulatory and legislative compliance auditing and logging integrity control as well as cloud computing provider dependent risks. Most customers are aware of the danger of letting data control and storing data with an outside cloud computing provider, data could be compromised by the cloud computing provider itself or other competitive enterprises which are customers with the same cloud computing provider. Transparency for customers on how why and where the data is processed is in opposition to the data protection requirement that customer know what happens with their data. Many cloud computing providers are technically able to perform data mining techniques to analyse user data very sensitive function and even more users are often storing and processing sensitive data when using cloud computing services, especially true for social media applications that encourage users to share much of their private. The effective use of smart technologies every business goal is to accomplish the targets of high financial gains at lower

operational costs this requires the optimal utilization of available resources. With the IT industry recognize and acknowledge that at the core of it all business remain focused on processes and projects, successful delivery of cloud projects depend on the project managers with project management frameworks and proven methodologies combined with experience acts as catalyst in building the robust service delivery engine to deliver faster and cheaper services in the cloud areas like public and private.

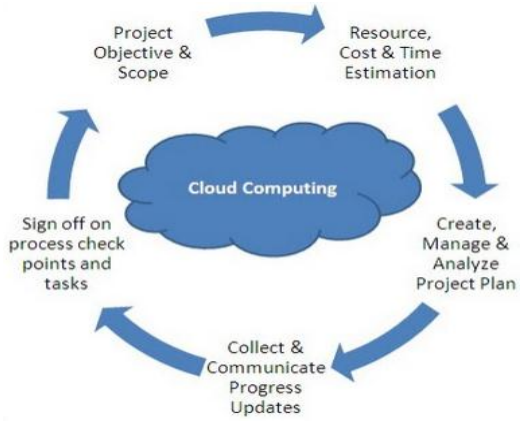

Figure 1 Cloud Management

Cloud computing introduces more than technical changes in IT processes and alters the way that the business interacts with its customers to improve the process in an easy and manageable way.

The key to successful project management in the cloud is to create and manage a project framework that embeds best practices of standard project management and cloud computing methodology into how one manages projects inside and outside the cloud. Impact of cloud on project management will include a higher emphasis on security parallel processing scalability and ability to utilize infinite resources.

Section II

2. Related Work: The survey of major cloud service providers to investigate the security mechanisms to overcome the security issues discussed in this paper. We consider ten major cloud service providers. These providers provide their services in all major areas of cloud computing, including SaaS, PaaS and IaaS. List shows the list of service providers that we studied in this survey. In order to analyze the complete state of art of security in cloud computing, the survey needs to be more exhaustive. However, due to the fact that the scope of our work is not just to explore the state of art but to look at the major factors that affect security in cloud computing. Therefore we have intentionally not considered other cloud service providers in this survey. In list 2, we present the results of the survey that depicts the current state of security mechanisms. Information given in table 2 is based on the information available online at the official websites of these providers.

1. IaaS Service Provides is a Amazon EC2 Amazon S3 Go Grid
2. PaaS Service Provides Google Application Engine Microsoft Azure Services, Elastic Map Reduce
3. SaaS service provides Sales force Google Docs

Password Recovery 90% are using standard methods like other common services while 10% are using sophisticated techniques.

Encryption 40% are using standard SSL encryption while 20% are using encryption mechanism but at an extra cost 40% are using advance methods like HTTPS access

Data Location 70% have their data centers located in more than one country while 10% are located at a single location 20% are not open about this issue.

Cloud computing is a model for information and services using exiting methods, it uses the internet infrastructure to allow communication between client side and server side applications. Cloud clients service providers provides exist between that offers cloud platforms for their customers to use and create their own web services. When making decisions to adopt cloud services privacy or security has always been a major deal with these issues the cloud provider must build up sufficient controls to provide such level of security than the organization would have if the cloud were not used.

The major security challenge is that the owner of the data has no control on their data processing. Due to involvement of many technologies including networks, databases, operating systems, resource scheduling, transaction management, concurrency control and memory management [3],various security issues arises in cloud computing.

Top seven security threats to cloud computing discovered by “Cloud Security Alliance” (CSA) are [4]:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders.
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking.
- Unknown Risk Profile

Formal "proof of retrievability" (POR) model for ensuring the remote data integrity. Their scheme combines spot-checking and error correcting code to ensure both possession and retrievability of files on archive service systems. Shacham et al. built on this model and constructed a random linear function based homomorphism authenticator which enables unlimited number of challenges and requires less communication overhead due to its usage of relatively small size of BLS signature. Bowers *et al.* [7] proposed an improved framework for POR protocols that generalizes both Juels and Shacham's work. Later in their subsequent work, Bowers et al. extended POR model to distributed systems. However, all these schemes are focusing on static data. The effectiveness of their schemes rests primarily on the pre-processing steps that the user conducts before outsourcing the data file **F**. Any change to the contents of **F**, even few bits, must propagate through the error-correcting code and the corresponding random shuffling process, thus introducing significant computation and communication complexity. Recently, Dodis *et al.* gave theoretical studies on generalized framework for different variants of existing POR work. Ateniese *et al.* defined the "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key based homomorphism tags for auditing the data file. However, the pre-computation of the tags imposes heavy computation overhead that can be expensive for an entire file. In their subsequent work, Ateniese *et al.* described a PDP scheme that uses only symmetric key based cryptography. This method has lower-overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work. However, their scheme focuses on single server scenario and does not provide data availability guarantee against server failures, leaving both the distributed scenario and data error recovery issue unexplored. The incremental cryptography work done by Bellare *etal.* Also provides a set of cryptographic building blocks such as hash, MAC, and signature functions that may be employed for storage integrity verification while supporting dynamic operations on data. However, this branch of work falls into the traditional data integrity protection mechanism, where local copy of data has to be maintained for the verification. It is not yet clear how the work can be adapted to cloud storage scenario where users no longer have the data at local sites but still need to ensure the storage correctness efficiently in the cloud.

SECTION III

3. Problem Definition: Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services) which can be rapidly provisioned and released with minimal management effort. Cloud-based healthcare information system that hosts outsourced personal health records (PHRs) from various healthcare providers. The PHRs are encrypted in order to comply with privacy regulations like HIPAA. In order to facilitate data use and sharing, it is highly desirable to have a searchable encryption (SE) scheme which allows the cloud service provider to search over encrypted PHRs on behalf of the authorized users (such as medical researchers or doctors) without learning information about the underlying plaintext. Note that the context we are considering supports private data sharing among multiple data providers and multiple data users.

Cloud computing classified into three segments application storage and connectivity each one is used for different purpose and offers different products for business and individuals around the world, which uses remote server to maintain data and various applications provides significant cost effective IT resources as cost on demand IT based on the actual usage of the customer. Cloud computing provides clients with a virtual computing infrastructure on top of which they can store data and run applications, to transfer data from one device to other device we design cryptographic primitives and protocols to the setting of cloud computing attempting to strike a balance between security efficiency and functionality. Cloud computing infrastructure do not provide any security against untrusted cloud operators making them unsuitable for storing sensitive information such as medical records financial records for high impact business data.

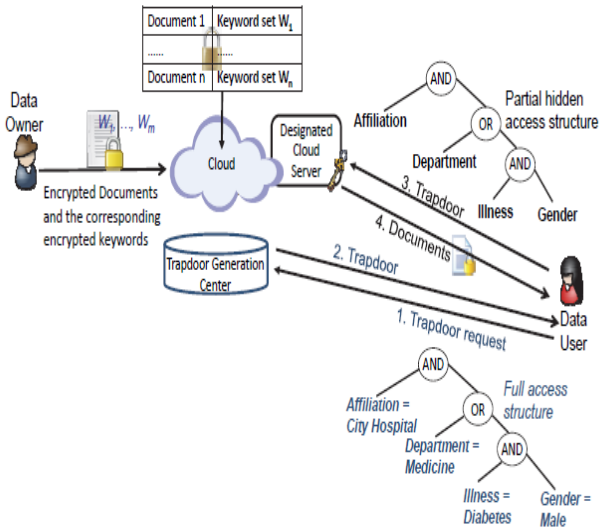

Figure 2 Encryption process in Cloud Management

3.1. Data Attribute Based Search: Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). The basic idea of our scheme is to modify a key-policy attributed-based encryption (KP-ABE) scheme constructed from bilinear pairing over prime-order groups. Without loss of generality, we will use the large universe KP-ABE scheme selectively secure in the standard model proposed by Rouselakis and Waters.

3.2. Expressiveness Keywords: scheme should support keyword access structures expressed in any Boolean formula with AND OR gates efficiency. The proposed scheme should be adequately efficient in terms of computation, communication and storage

TABLE I

Comparisons of expressive keyword search schemes.

	Keyword Privacy	Expressiveness	Bilinear Group	Security	Unbounded keywords
BCOP04 [7]	keyword guessing attacks on trapdoors	AND	prime	full random oracle	yes
KSW13 [16]	keyword guessing attacks on trapdoors	AND, OR	composite	full standard model	no
LZDLC13 [8]	keyword guessing attacks on trapdoors	AND, OR	composite	full standard model	no
LHZP14 [14]	no keyword guessing attacks on trapdoors	AND, OR, NOT	composite	full standard model	no
Our scheme	keyword guessing attacks on trapdoors by designated server only	AND, OR	prime	selective standard model	yes

Table 1 show for the practical applications.

A ciphertext without its corresponding trapdoors should not disclose any information about the keyword values it contains to the cloud server and outsiders. Second, a trapdoor should not leak information on keyword values to any outside attackers without the private key of the designated cloud server.

We capture this notion of security for the SE scheme in terms of semantic security to ensure that encrypted data does not reveal any information about the keyword values, which we call "selective in distinguishability against chosen keyword-set.

3.3. Searchable Encryption: Searchable encryption is a cryptographic technique that allows search of specific information encrypted by Dan Boyen. Assume that John want to redirect the mail to Jordan containing the term official as he is away in a holiday so how would the service provider know which mail to send to Jordan if it is not able to read the data and again it is a security concern to transmit the data without end of encryption. Here the John chose to encrypt the message and create a collection of tags or search keywords that can uniquely identify the message for a specific search that are appended to the encrypted message the service provided can perform the task of forwarding the mail without knowing the details of the mail.

SECTION IV

4. Comparative Study : The solution in as well as other existing PEKS schemes which improve on only support equality queries As such, our scheme is not only capable of expressive multi-keyword search, but also significantly more efficient than existing schemes built in composite-order groups. Using a randomness splitting technique, our scheme achieves security against offline keyword dictionary guessing attacks to the ciphertexts. Moreover, to preserve the privacy of keywords against offline keyword dictionary guessing attacks to trapdoors, we divide each keyword into keyword name and keyword value and assign a designated cloud server to conduct search operations in our construction. We formalize the security definition of expressive SE, and formally prove that our proposed expressive SE scheme is selectively secure in the standard model.

set intersection leaks extra information to the cloud server beyond the results of the conjunctive query, whilst the approach using meta keywords require 2m meta keywords to accommodate all the possible conjunctive queries for m keywords. It is straightforward to see that compared to the existing ones, our construction make a good balance in that it allows unbounded keywords, supports expressive access structures, and is built in the prime-order groups compare to earlier work our proposed work shows best analysis an expressive public-key searchable encryption scheme in the prime-order groups, which allows keyword search policies (i.e., predicates, access structures) to be expressed in conjunctive, disjunctive or any monotonic Boolean formulas and achieves significant performance improvement over existing schemes. We formally define its security, and prove that it is selectively secure in the standard model. In order to tackle the keyword search problem in the cloud-based healthcare information system scenario, we resort to public-key encryption with keyword search (PEKS) schemes, which is firstly proposed in . In a PEKS scheme, a ciphertext of the keywords called "PEKS ciphertext" is appended to an encrypted PHR. To retrieve all the encrypted PHRs containing a keyword, say "Diabetes", a user sends a "trapdoor" associated with a search query on the keyword "Diabetes" to the cloud service provider, which selects all the encrypted PHRs containing the keyword "Diabetes" and returns them to the user while without learning the underlying PHRs more efficient benefits that expressive SE scheme inherits

the advantages of the Rouselakis-Waters scheme. Thus, it is straightforward to see that in our SE scheme, the size of the public parameter is immutable with the number of keywords, and the number of the keywords allowed for the system is unlimited and can be freely set. According to the analysis in terms of the pairing-friendly elliptic curves, prime order groups have a clear advantage in the parameter sizes over composite order groups. The advantage for a polynomial time adversary that can distinguish between the games Game0 and Game1 is negligible.

CONCLUSION V

To allow a cloud server to search on encrypted data without learning the underlying plaintexts in the PublicKey setting, cryptographic primitive called public-key encryption with keyword search. Since then, considering different requirements in practice, e.g., communication overhead, searching criteria and security enhancement, various kinds of searchable encryption systems have been put forth. However, there exist only a few public-key searchable encryption systems that support expressive keyword search policies, and they are all built from the inefficient composite-order groups. This analysis presents on the design and analysis of public-key searching formulas on a large universe key-policy attribute-based encryption scheme that presented an expressive searchable encryption system in the prime order group which supports expressive access structures expressed in any monotonic Boolean formulas.

Reference

[1] Atallah, M.J., Frikken, K.B.: Securely outsourcing linear algebra computations. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 48–59. ACM (2010)

[2] Atallah, M.J., Li, J.: Secure outsourcing of sequence comparisons. International Journal of Information Security **4**(4), 277–287 (2005) 4.

[3] Attrapadung, N., Libert, B.: Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In: Public Key Cryptography–PKC 2010, pp. 384–402. Springer (2010)

[4] Azab, A.M., Ning, P., Zhang, X.: Sice: a hardware-level strongly isolated computing environment for x86 multi-core platforms. In: Proceedings of the 18th ACM conference on Computer and communications security, pp. 375–388. ACM (2011)

[5] Bao, F., Deng, R.H., Ding, X., Yang, Y.: Private query on encrypted data in multi-user settings. In: Information Security Practice and Experience, pp. 71–85. Springer (2008)

[6] Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Advances in Cryptology-Eurocrypt 2004, pp. 506–522. Springer (2004)

[7] Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Advances in Cryptology – CRYPTO 2001, pp. 213–229. Springer (2001)

[8]Boneh, D., Waters, B.: Conjunctive, subset, and range queries on encrypted data. In: Proceedings of the 4th conference on Theory of cryptography, pp. 535–554. Springer-Verlag (2007)

[9] Cao, N., Wang, C., Li, M., Ren, K., Lou, W.: Privacy-preserving multi-keyword ranked search over encrypted cloud data. In: Proceedings of IEEE INFOCOM, pp. 829–837 (2011)

[10]. Chang, Y.C., Mitzenmacher, M.: Privacy preserving keyword searches on remote encrypted data. In: Applied Cryptography and Network Security, pp. 442–455. Springer (2005)