Efficient cryptosystem for scalable data sharing in cloud storage

Dhivya P
Dept of computer science&Engg
Maha barathi Engineering College
China salem 606201,Tamil nadu,India
Dhivyaab.e@gmail.com

Amudhapandiyan D
Dept of computer science&Engg
Maha Barathi Engineering College
China salem 606201,Tamil nadu,India

Abstract— Data sharing is an important functionality in cloud storage. In this article, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In particular, our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known..

Keywords—Deniable Encryption, Decryption,Advanced Encryption Standards, Cloud Storage.

I INTRODUCTION

Cloud storage is gaining popularity recently. In enterprise settings, we see the rise in demand for data outsourcing, which assists in the strategic management of corporate data. It is also used as a core technology behind many online services for personal applications. Nowadays, it is easy to apply for free accounts for email, photo album, file sharing and/or remote access, with storage size more than 25GB (or a few dollars for more than 1TB). Together with the current wireless technology, users can access almost all of their files and emails by a mobile phone in any corner of the world. Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication), which means any unexpected privilege escalation will expose all data. In shared-tenancy cloud computing environment, things become even worse. Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine.

Data in a target VM could be stolen by instantiating another VM co-resident with the target one. Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor

To check the availability of files on behalf of the data owner without leaking anything about the data [3].without compromising the data owner's anonymity [4]. Likewise,

cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality. A cryptographic solution, e.g., [5], with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the VM or the honesty of the technical staff. These users are motivated to encrypt their data with their own keys before uploading them to the server.

Data sharing is an important functionality in cloud storage. For example, bloggers can let their friends view subset of their private pictures; an enterprise may grant her employees access to a portion of sensitive data. The challenging problem is how to effectively share encrypted data. Of course users can download the encrypted data from the storage, decrypt them, then send them to others for sharing, but it loses the value of cloud storage. Users should be able to delegate the access rights of the sharing data to others

So that they can access these data from the server directly. However, finding ancient and secure way to share partial data in cloud storage is not trivial. Below we will take Drop box as an example for illustration. Assume that Alice puts all her private photos on Dropbox, and she does not want to expose her photos to everyone.

Due to various data leakage possibility Alice cannot feel relieved.by just relying on the privacy protection mechanisms provided by Drop box, so she encrypts all the photos using her own keys before uploading. One day, Alice's friend, Bob, asks her to share the photos taken over all these years which Bob appeared in. Alice can then use the share function of Drop box, but the problem now is how to delegate the decryption rights for these photos to Bob. A possible option Alice can choose is to securely send Bob the secret keys involved. have system-wide secrets and must be able to decrypt all encrypted data[1] High-dimensional similarity search is a fundamental problem in many content-based search systems and also widely exists in many related application areas, such as machine learning, computer vision, information retrieval and data mining. One classical kind of methods to address this problem is the tree-based index, such as KD-Tree. These
methods usually partition the data space recursively, and perform exact similarity search in the low-dimension feature space. However, these methods cannot work well for high- dimensional data since their performances degrade significantly to linear scan as the dimensionality increases. Therefore, tree based indexes are not preferable in high- dimensional search problems. Another kind of ANN search algorithm is based on vector quantization, such as k means LSH and Product Quantization (PQ). The key of these methods is the compositionality. In PQ, by dividing each data into several subspaces and expressing data in terms of recurring parts, the representational capacity of PQ grows exponentially in the number of subspaces. In these methods, each data point is represented by a reconstructed cluster center and the search process is performed in the original data space. As a result, the search process is time- consuming even with an inverted file indexing. Recently, hashing based method has been widely used for similarity search .

Related applications as it allows constant-time search. A lot of hashing methods have been proposed, and in general, these methods can be roughly divided into two main categories: data-independent methods and data- dependent methods.

Recently, many data-dependent methods, which focus on earning hash functions from dataset, have been developed to earn more compact codes. In PCA-Hashing (PCAH), he eigenvectors corresponding to the largest Eigen values of the dataset covariance matrix are used to form the projection matrix for hashing. An extension of PCAH, Iterative Quantization (ITQ) is proposed to learn an orthogonal otation matrix to refine the initial PCA-projection matrix to minimize the quantization error of mapping the data from original data space to Hamming space. Isotropic Hashing (IsoH) n learns the projection functions which can produce projected dimensions with isotropic variances. The spectral graph partitioning strategy is employed to develop new kinds of hashing schemes, such as Spectral hashing (SPH). SPH uses the simple analytical eigen function solution of Laplacians as the hash function. Anchor Graph Hashing (AGH) applies the similar formulation of SPH for hash codes generation, while its neighborhood graph is constructed in a novel way such that it can be applied to large scale In manifold learning area, it is true that a manifold can be entirely characterized by giving the relative or comparative proximities, e.g. a first region is close to a second one but far from a third one. Comparative information between distances, like inequalities or rankings, suffices to characterize a manifold for any embeddings. Moreover, for many similarity search problems, the relative rankings of results are more important than their actual similarities to a query. Hamming embeddings can be learned by incorporating.

Dataset topology with the learning process. Furthermore, if the local topology is well preserved in Hamming space, the ambiguity caused by ranking with Hamming distance can be better alleviated..

The paradigm of hashing generally consists of two steps dimension reduction and 0/1 quantization. To capture meaningful neighbors, the neighborhood structure of a give dataset should be preserved. Therefore, the dimension reduction step is a key factor and significant research

II.RELATED WORK

In [2] authors used average cloud storage to the member of relationship i) average residual security of the nodes on the path.ii) In this article, we show how to securely, efficiently, and flexibly share data with others in cloud storage. [3]Attribute based encryption of the cryptosystem. thus altogether circumventing storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected [4] This paper describes the integration of the Personal Software Process (PSP) into an introductory database course in an MIS curriculum. PSP is a highly disciplined, process-based approach that serves to guide an individual programmer's activities during the development of a software system. Developed at the Software Engineering Institute (SEI) at Carnegie Mellon University, PSP defines how to use process principles to plan, track, and analyze personal programming work . In [5] authors improved key generate protocol by implementing a balanced energy consumption idea into route discovery process. Security message will be forwarded when the nodes have sufficient amount of energy to transmit the message otherwise message will be dropped. This condition will be checked with threshold value which is dynamically changing. It allows a node with over used battery to refuse to route the traffic in order to prolong the network life. In [6] Authors had modified the route table of AES changing attribute based encryption algorithm adding power factor field. Only active nodes can take part in rout selection and. In [7] Cryptosystem of the module and sharing the data. In additional to this introductory section, we introduce preliminaries used, we formally define deniable CP-ABE and its properties. we show how to set up a basic deniable CPABE scheme and prove security, deniability and other features of our scheme.

III PROPOSED

ALGORITHM PROPOSED

SYSTEM:

The parent key implicitly grants all the keys of its descendant nodes.

Proposed a method to generate a tree hierarchy of symmetric keys by using repeated evaluations of pseudo random function/block-cipher on a fixed secret. More advanced cryptographic key assignment schemes support access policy that can be modelled by an acyclic graph or cyclic graph.Most of these schemes produce keys for symmetric-key cryptosystems, even though the key derivations may require modular arithmetic as used in public-key cryptosystems, which are generally more expensive than -symmetric-key operations| such as pseudorandom function.

PROPOSED ALGORITHM:

AES algorithm

It should provide a strong crypto algorithm for government and commercial use.

It should be significantly more efficient than DES It should have a variable key size so that security could be increased when needed

It should be selected in a fair and open manner It should be evaluable by (sufficiently expert) members of the public.

AES shall be a symmetric block cipher.

AES shall be implementable in both hardware and software

KEY GEN PHASE

The key generation algorithm takes as input the master key MK and a set of attributes.

The key Support for both sender and receiver on cloud server.

The key have support for securely sharing the data on cloud.

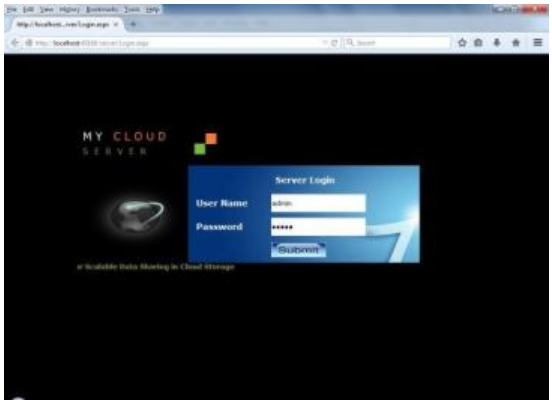
One time using this key then limited validity of key.

IV. SIMULATION RESULT

The basics of ASP.NET Web API. We will try to understand what a Web API is, what is the basic structure of a Web API project. We will also create a simple application to demonstrate the CRUD operation on a simple entity using Web API. .NET provides a new, object-oriented API as a set of classes that will be accessible from any programming language. This book describes this framework of classes and provides a reference to what is available and how you

can use this framework to write Windows applications in the brave new world of .NET.

In addition to the bitranslucent set, there are other proposed approaches to building deniable encryption schemes. ONeill et al. proposed a new deniable method through a simulatable public key system [5]. The simulatable public key system provides an oblivious key generation function and an oblivious ciphertext function. When sending an encrypted bit, the sender will send a set of encrypted data which may be normally encrypted or oblivious. The sender can send a true message encrypted by one key with a fake message encrypted by the other key. The sender decides which key is released according to the coercer's identity. Gasti et al. also applied this idea to cloud storage services. One representative data- independent method is Locality Sensitive Hashing (LSH), the hash functions are just simple random projections, which are independent of dataset. Anti-Sparse Coding (ASC) improves LSH based on the spread representations of a dataset, but it requires the bit number larger than the data dimensionality. Super-bit LSH (SBLSH) orthogonalizes the random projections and guarantees that an unbiased estimate



V. CONCLUSION.

The advanced feature support for unlimited data sharing in cloud storage have highly support for Advanced Encryption System (AES).With more mathematical tools, this are support with cryptographic schemes are getting more versatile and often involve multiple keys for a m u l t i p l e applications. In this article, we consider how to -compress‖ secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. Refusal issue which one among the power set of classes, the delegate can always get an aggregate key of constant size. Our approach is more flexible than hybrid key task which be able to only save spaces if all key-holders share a similar set of privileges

References.

[1] R. S. Sandhu, -Cryptographic Implementation of a Tree Hierarchy for Access Control,‖ Information Processing Letters, vol. 27, no. 2,pp. 95–98, 1988.

[2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, -Privacy Preserving Public Auditing for Secure Cloud Storage,‖ IEEE Trans. Computers, vol. 62, no. 2, pp. 362– 375, 2013.

[3] B. Wang, S. S. M. Chow, M. Li, and H. Li, -Storing Shared Data on the Cloud via Security-Mediator,‖ in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013

[4] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, -Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,‖ Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.

[5] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, -Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,‖ in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.