Volume No:2, Issue No:2 (July-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Group Data Sharing by Encryption key words are Searchable by Cloud Storages

Annaram Shiva Shankar
PG Scholar,
Dept of CSE,
Jawaharlal Nehru Institute of Technology,
Hyderabad.

K.Shalini
Associate Professor,
Dept of CSE,
Jawaharlal Nehru Institute of Technology,
Hyderabad.

Abstract:

Data sharing is an important functionality in cloud storage. In this paper, we show how to securely, efficiently, and flexibly share data with others in cloud storage. We describe new public-key cryptosystems that produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts is 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: broadcast, encryption, signature.

INTRODUCTION:

Cloud Computing has been envisioned as the next-generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One Fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud.

From users' perspective, including both individuals and enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc . While these advantages of using clouds are unarguable, due to the opaqueness of the Cloud—as separate administrative entities, the internal operation details of cloud service providers (CSP) may not be known by cloud users—data outsourcing is also relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time . Secondly, for the benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully. towards the cloud users regarding the status of their outsourced data. Examples include cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed, or even hiding data loss incidents so as to maintain a reputation. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture.

EXISTING SYSTEM:

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.

Volume No:2, Issue No:2 (July-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In a shared-tenancy cloud computing environment, things become even worse.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, or without compromising the data owners anonymity. 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, 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.

DISADVANTAGE:

» correctness of the data in the cloud is being put at risk
» data integrity
» The costs and complexities involved generally increase with the number of the decryption keys to be shared.
» The encryption key and decryption key are different in public key encryption.

PROPOSED SYSTEM:

In this paper, we study how to make a decryption key more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size. Specifically, our problem statement is "To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the cipher texts (produced by the encryption scheme) is decry p table by a constant-size decryption key (generated by the owner of the master-secret key)." We solve this problem by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of cipher text called class. That means the cipher texts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of cipher text classes.

ADVANTAGES:

» The extracted key have can be an aggregate key which is as compact as a secret key for a single class.
» The delegation of decryption can be efficiently implemented with the aggregate key.
» Storage correctness

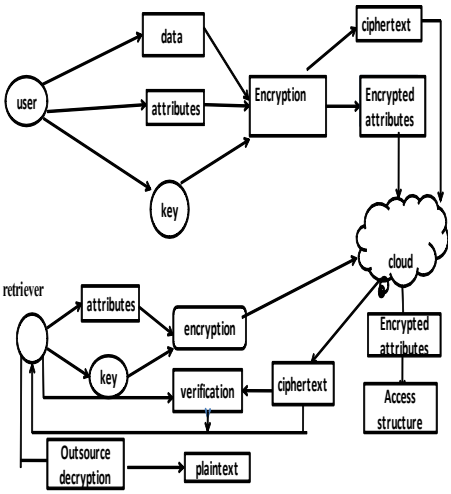

Fig: 1 Architecture Diagram

LITRETURE SURVEY:

1.PERFORMANCE EVALUATION OF PUBLIC-KEY:

WTLS (Wireless Transport Layer Security) is an important standard protocol for secure wireless access to Internet services. WTLS employs public-key cryptosystems during the hand shake between mobile client and WAP gateway (server).Several cryptosystems at different key strengths can be used in WTLS. The trade-off is security versus processing and transmission time. In this paper, an analytical performance model for public-key cryptosystem operations in WTLS protocol is developed. Different handshake protocols ,different cryptosystems and key sizes are considered. Public-key crypto systems are implemented using state-of-the–art performance improvement techniques, yielding actual performance figures for individual cryptosystems. These figures and the analytical model are used to calculate the cost of using public-key cryptosystems in WTLS. Results for different cryptosystems and handshake protocols are comparatively depicted and interpreted. It has been observed that ECC(Elliptic Curve Cryptography) performs better than its rival RSA cryptosystem in WTLS. Performance of some stronger

Volume No:2, Issue No:2 (July-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

ECC curves, which are not considered in WTLS standard, is also analysed. Results showed that some of those curves could be used in WTLS for high security applications with an acceptable degradation in performance

2) PRIVACY-PRESERVING PUBLIC AUDITING FOR DATA STORAGE SECURITY IN CLOUD COMPUTING:

Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formable task, especially for users with constrained computing resources and capabilities. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homo morphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

3) AN IMPROVED DYNAMIC PROVABLE DATA POSSESSION MODEL:

Cloud computing is becoming increasingly popular. Many companies, organizations and individuals choose to outsource their computing demands and storage demands. In order to ensure the integrity of the data in the Cloud, especially the dynamic files which can be updated online, we propose an improved dynamic provable data possession model: It divides file into blocks, generates a tag for each block, computes a hash value for each tag, use stags to ensure the integrity of the file blocks, and uses hash values to ensure the integrity of the tags. Compared with previous works, it reduces the computational and communication complexity from to constant. Although client needs to store some secret values which may create some additional storage expense, it only takes up about0.02% of the original file size. Hence it is acceptable in most cases.

HYBRID PROVABLE DATA POSSESSION AT UNTRUSTED STORES IN CLOUD COMPUTING:

In recent years, cloud computing has gradually become the mainstream of Internet services. When cloud computing environments become more perfect, the business and user will be an enormous amount of data stored in the remote cloud storage devices, hoping to achieve random access, data collection, reduce costs, and facilitate the sharing of other services. However, when the data is stored in the cloud storage device, a long time, enterprises and users inevitably will have security concerns, fearing that the information is actually stored in the cloud is still in the storage device or too long without access to, has long been the cloud server removed or destroyed, resulting in businesses and users in the future can't access or restore the data files. Therefore, this scheme goal to research and design for data storage cloud computing environments that are proved. Stored in the cloud for data storage, research and develop a security and efficient storage of proof protocol, also can delegate or authorize others to public verifiability whether the data actually stored in the cloud storage devices.

ROBUST DYNAMIC PROVABLE DATA POSSESSION:

Remote Data Checking (RDC) allows clients to efficiently check the integrity of data stored at un trusted servers. This allows data owners to assess the risk of outsourcing data in the cloud, making RDC a valuable tool for data auditing. Robust RDC scheme incorporates mechanisms to mitigate arbitrary amounts of data corruption.

Volume No:2, Issue No:2 (July-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In particular, protection against small corruptions (i.e., bytes or even bits) ensures that attacks that modify a few bits do not destroy an encrypted file or invalidate authentication information. Early RDC schemes have focused on static data, whereas later schemes such as DPDP support the full range of dynamic operations on the outsourced data, including insertions, modifications, and deletions. Robustness is required for both static and dynamic RDC schemes that rely on spot checking for efficiency. However, under an adversarial setting there is a fundamental tension between efficient dynamic updates and the encoding required to achieve robustness, because updating even a small portion of the file may require retrieving the entire file. We identify the challenges that need to be overcome when trying to add robustness to a DPDP scheme. We propose the first RDC schemes that provide robustness and, at the same time, support dynamic updates, while requiring small, constant, client storage. Our first construction is efficient in encoding, but has high communication cost for updates. Our second construction overcomes this drawback through a combination of techniques that includes RS codes based on Cauchy matrices, decoupling the encoding for robustness from the position of symbols in the file, and reducing insert/delete operations to append/modify operations when updating the RS-encoded parity data.

A SECURITY ANALYSIS OF AMAZON'S ELASTIC COMPUTE CLOUD SERVICE:

Cloud services such as Amazon's Elastic Compute Cloud and IBM's Smart Cloud are quickly changing the way organizations are dealing with IT infrastructures and are providing online services. Today, if an organization needs computing power, it can simply buy it online by instantiating a virtual server image on the cloud. Servers can be quickly launched and shut down via application programming interfaces (API), offering the user a greater flexibility compared to traditional server rooms. In this talk, I will explore the general security risks associated with using virtual server images from the public catalogues of cloud service providers. In particular, we investigate in detail the security problems of public images that are available on the Amazon EC2 service. I will describe the design and implementation of an automated system that we used to instantiate and analyze the security of public AMIs (Amazon Machine Images) on the Amazon EC2 platform, and provide detailed descriptions of the security tests that we performed on each image. Our findings demonstrate that both the users and the providers of public AMIs may be vulnerable to security risks such as unauthorized access, malware infections, and loss of sensitive information. The Amazon Web Services Security Team has acknowledged our findings, and has already taken steps to properly address all the security risks we present in this talk.

APPROACHES:

Advanced Encryption Standard

A complicated secret writing normal may be a 128 bit cruciform key secret writing algorithmic rule having sixteen bit key size. It's a secret writing and decoding with same key. The AES cipher is given as variety of repetitions of transformation rounds that convert the input plaintext into the ultimate output of a cipher text. every spherical consists of many process steps, that including one that depends on the secret writing key Here we square measure mistreatment 128 bit key therefore it's ten rounds of operation. Those are

1) Sub bytes
2) Shift rows
3) Combine columns
4) Add spherical Key

Therein except tenth spherical every spherical ought to perform total nine spherical however tenth round perform solely three operations i.e. sub bytes, shift rows, add spherical keys. The AES cipher is given as variety of repetitions of transformation rounds that convert the input plaintext into the ultimate output of a cipher text. every spherical consists of many process steps, that together with one that depends on the secret writing key a group of reverse rounds square measure applied to rework cipher text which will into the initial plaintext mistreatment an equivalent secret writing key. Encryption converts knowledge to AN unintelligible kind known as cipher text, decrypting the cipher text converts the info into its original kind, known as plaintext. The AES algorithmic rule is capable of mistreatment crypto logic keys of 128, 192, and 256 bits to write and rewrite knowledge in blocks of 128 bits.The Advanced secret writing normal (AES) is a secret writing algorithmic rule for securing sensitive (Encryption for the United States military and alternative classified communications square measure handled by separate, secret algorithms approaches.

Volume No:2, Issue No:2 (July-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

RELATED WORK:

1.User Registration:

For the registration of a user with establish the ID the cluster managers arbitrarily selects with variety. Then the cluster managers add into the cluster user to list that is employed within the traceability state. Once complete the registration of a user, user obtains a key through mail which can be used for cluster signature generation and file decoding.

2. User Revocation:

User revocation is performed by the cluster manager via a public keys square measure on the market. Revocation list supported that cluster members will write the info files and make sure the confidentiality against the revoked users. Cluster trough update the revocation list every day even no user has being revoked within the day. In alternative words, the others will verify the info of the revocation list from the contained current date.

3. File Generation and Deletions:

To store and share file within the cloud, a bunch member performs to obtaining the revocation list from the cloud. During this method, the member sends the cluster identity ID to cluster as asking to the cloud. validatory the validity of the received revocation list. File hold on within the cloud will be deleted by either the cluster manager or the info owner.

4. File Access and Traceability:

To access the cloud, a user has to work out a bunch signature for his/her authentication. The used cluster signature theme will be considered a variant of the short cluster signature that inherits the inherent un-forge ability property, anonymous authentication, and following capability. Once a knowledge dispute happens, the tracing operation is performed by the cluster manager to spot the $64000 identity of the info owner.

CONCLUSION:

In this paper, we tend to tend to vogue a secure data sharing theme, Mona, for dynamic groups in associate untrusted cloud.

In Mona, a user is prepared to share data with others inside the cluster whereas not revealing identity privacy to the cloud. To boot, island supports economical user revocation and new user amendment of integrity. lots of specially, economical user revocation square measure usually achieved through a public revocation list whereas not amendment the private keys of the remaining users, and new users can directly rewrite files keep inside the cloud before their participation. Moreover, the storage overhead and so the cryptography computation worth unit of measurement constant. Intensive analyses show that our planned theme satisfies the specified security desires and guarantees efficiency equally. Planned a crypto graphical storage system that allows secure file sharing on un-trusted servers, named Plutus. By dividing files into file teams and encrypting each file cluster with a completely unique file-block key, the information owner can share the file teams with others through delivering the corresponding safe-deposit key, where the safe-deposit secret is accustomed write the file-block keys. However, it brings some of great key distribution overhead for large-scale file sharing. to boot, the file-block key must be updated and distributed all over again for a user revocation.

REFERENCES:

1.Key-Aggregate Cryptosystem for ScalableData Sharing in Cloud StorageCheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, andRobert H. Deng, Senior Member, IEEE

2.U.S. Department of Health and Human Services. (2011, Sep.). HIPAA—General Information [Online]. Available: https://www.cms.gov/ hipaageninfo

3.PCI Security Standards Council. (2006, Sep.) Payment Card Industry (PCI) Data Security Standard—Security Audit Procedures Version 1.1 [Online]. Available:https://www.pcisecuritystandards.org/pdfs/pci−audit−procedures−v1-1.pdf

4.Sarbanes-Oxley Act 2002. (2002, Sep.). A Guide to the Sarbanes-Oxley Act [Online]. Available: http://www.soxlaw.com/

5.C. Lonvick, the BSD Syslog Protocol, Request for Comment RFC 3164, Internet Engineering Task Force, Network Working Group, Aug. 2001.

Volume No:2, Issue No:2 (July-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

6.6. K. Kent and M. Souppaya. (1992). Guide to Computer Security Log Management, NIST Special Publication 800-92 [Online]. Available:http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

7.D. New and M. Rose, Reliable Delivery for Syslog, Request for Comment RFC 3195, Internet Engineering Task Force, Network Working Group, Nov. 2001.

8. 8.G. Ateniese, K. Fu, M. Green, and S.ohenberger, "ImprovedProxy Re-Encryption Schemes with Applications to SecureDistributed Storage," ACM Trans. Information and System Security,vol. 9, no. 1, pp. 1-30, 2006.

9.D. Boneh, C. Gentry, and B. Waters, "Collusion Resistant BroadcastEncryption with Short Ciphertexts and Private Keys," Proc.Advances in Cryptology Conf. (CRYPTO '05), vol. 3621, pp. 258-275,2005.

10.. L.B. Oliveira, D. Aranha, E. Morais, F. Daguano, J. Lopez, and R.Dahab, "Tiny Tate: Computing the Tate Pairing in Resource-Constrained Sensor Nodes," Proc. IEEE Sixth Int'l Symp. NetworkComputing and Applications (NCA '07), pp. 318-323, 2007.

Author Profile:

Annaram Shiva Shankar,
M.Tech (CSE), Jawaharlal Nehru Institute of Technology (JNIT), He is Interested in Digital Image Processing.