3rd International Conference on Recent Innovations in Science, Technology, Management and Environment
Indian Federation of United Nations Associations, New Delhi, India (ICRISTME-16)
18th December 2016 , www.conferenceworld.in ISBN: 978-93-86171-13-9

DATA SHARING IN CLOUD STORAGE BY USING EFFECTIVE KEY CRYPTOSYSTEM

Mandapalli Sindhu Devi[1], Dr.P.Amaravathi[2]

[1]M.Tech Student, [2]M.Tech, Ph.D Dept of CSE,

V.S.Lakshmi Engg. College for Womens, Matlapalem, Kakinada, (India)

ABSTRACT

Data sharing is an important functionality in cloud storage. 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 text such that efficient delegation of decryption rights for any set of cipher text 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. The secret key holder can release the constant-size aggregate key for the flexible choices of cipher text set in cloud storage, but 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.

Key words: Cloud storage, data sharing, key-aggregate encryption, Public Key Encryption.

I. INTRODUCTION

New computing paradigms keep rising. Are placement economic computing model created attainable by the advances in networking technology, wherever a consumer will leverage a service provider's computing ,storage or networking infrastructure. With the unprecedented exponential rate of information, there is an Associate in nursing increasing demand for out sourcing information storage to cloud services like a Microsoft's Azure. Storing information remotely to the cloud in an exceedingly versatile on demand manner brings appealing benefits: relief of the burden for storage management, universal information access with the freelance geographical locations, and avoidance of value on hardware and software, and personnel maintenances etc.al though the infrastructures at a lower place the cloud unit of measurement far more powerful and reliable than personal computing devices, they're still facing the broad vary of every internal and external threats for information integrity. Samples of outages and security breaches of noteworthy cloud services appear from time to time. Secondly, there do exist various motivations for CSP(cloud service provider) to behave unfaithfully towards the cloud users regarding the standing of their outsourced information. As examples, CSP may reclaim storage for monetary reasons by discarding information that has not been or isn't accessed, or even hide information. Considering information privacy, As a result of its shared atmosphere, things become worst. As information is access from any virtual machines (VMS) but it resides on one physical machine. Information in an exceedingly target VM is also taken by instantiating another VM co-resident with the target one by traditional means that it completely depends upon the server to produce the access management alone once authentication .it recommends that any shocking increase can expose all information. Commonly in study schemes, TPA will check the supply of information on behalf of owner but cloud server doesn't trust TPA. So we've an inclination to follow vary hypothetical approach for good security .users is required to cipher their own information by using their own key before uploading. Information sharing is Associate in nursing crucial usefulness in cloud storage. Sharing encrypted information effectively is form of tough task. Clearly user will transfer encrypted information and decode them, and share with others; however approach violates worth of cloud storage. Finding Associate in nursing economical and secure thanks to share partial information in cloud

storage isn't trivial. Consider Associate in nursing example of 2 military camps. Assume that military camp A is willing to share space maps with military camp B. however because of varied information run chance they can't expose maps to everybody. That the camp A encrypts all the map victimization her own keys before uploading. And send key firmly to the camp B however this might cause draw back that they share all the photos.

II. RELATED WORK

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public audit ability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design. Wireless Sensors have seen a lot of applications in our daily lives in the recent years. The market has been flooded with high end consumer electronics using wireless sensor technology. However, most of the current technologies require the sensor to be in the vicinity of the end-user application. There has been some study in the techniques for sensor provisioning and sharing for the large number of existing Wireless Sensor Networks. Virtualization of Wireless Sensor Networks (WSNs) is a step forward in exposing these WSNs to large user base from remote locations. However, there is still a huge gap in bringing together information available from heterogeneous, distributed resources of Wireless Sensor Networks to a non-localized user. In this work, we utilize IaaS paradigm of Cloud Computing in virtualization of sensor networks which gives the flexibility of handling heterogeneous systems. The system also enables a smart device user to access information generated by Wireless Sensors through the cloud via SaaS based design. This allows the system to take common computational tasks to be hosted as a service through the cloud. It frees the smart device user from running heavy applications for data processing and storing. Thus, system provides the smart device user a Cloud Enabled Wireless Sensor Network infrastructure. The system architecture provides the necessary features for it to be scalable and flexible, ensuring reliable sensor data transfer and processing through cloud infrastructure. We also present a small test bed implementation of the system. Many group communications require a security infrastructure that ensures multiple levels-of access privilege fix group members. Access control in hierarchy is prevalent in multimedia applications, which consist of users that subscribe to different quality levels or different sets of data streams. In .this paper, we present a multi-group key management scheme that achieves such a hierarchical access control by employing an integrated key graph and by managing group kegs for all wars with various access privileges Compared with applying existing tree-based group keg management schemes directly to the hierarchical access control problem, the proposed scheme significantly reduces the communication, computation and storage overhead associated with key management and achieves better scalability when the number of access levels increases. In addition, the proposed key graph is suitable for both centralized and contributory environments.

III.EXISTING SYSTEM

There exist several expressive ABE schemes where the decryption algorithm only requires a constant number of pairing computations. Recently, Green et al. proposed a remedy to this problem by introducing the notion of ABE with outsourced decryption, which largely eliminates the decryption overhead for users. Based on the existing ABE schemes, Green et al. also presented concrete ABE schemes with outsourced decryption.In these

existing schemes, a user provides an untrusted server, say a proxy operated by a cloud service provider, with a transformation key TK that allows the latter to translate any ABE cipher-text CT satisfied by that user's attributes or access policy into a simple cipher-text CT', and it only incurs a small overhead for the user to recover the plaintext from the transformed cipher-text CT'. The security property of the ABE scheme with outsourced decryption guarantees that an adversary (including the malicious cloud server) be not able to learn anything about the encrypted message; however, the scheme provides no guarantee on the correctness of the transformation done by the cloud server. In the cloud computing setting, cloud service providers may have strong financial incentives to return incorrect answers, if such answers require less work and are unlikely to be detected by users.

IV.PROPOSED SYSTEM

We considered the verifiability of the cloud's transformation and provided a method to check the correctness of the transformation. However, the we did not formally define verifiability. But it is not feasible to construct ABE schemes with verifiable outsourced decryption following the model defined in the existing. Moreover, the method proposed in existing relies on random oracles (RO). Unfortunately, the RO model is heuristic, and a proof of security in the RO model does not directly imply anything about the security of an ABE scheme in the real world. It is well known that there exist cryptographic schemes which are secure in the RO model but are inherently insecure when the RO is instantiated with any real hash function.In this thesis work, firstly modify the original model of ABE with outsourced decryption in the existing to allow for verifiability of the transformations. After describing the formal definition of verifiability, we propose a new ABE model and based on this new model construct a concrete ABE scheme with verifiable outsourced decryption. Our scheme does not rely on random oracles.In this paper we only focus on CP-ABE with verifiable outsourced decryption. The same approach applies to KP-ABE with verifiable outsourced decryption.To assess the performance of our ABE scheme with verifiable outsourced decryption, we implement the CP-ABE scheme with verifiable outsourced decryption and conduct experiments on both an ARM-based mobile device and an Intel-core personal computer to model a mobile user and a proxy, respectively.

The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen. Messages can be encrypted via Encrypt by anyone who also decides what ciphertext class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of ciphertext classes via Extract. The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally; any user with an aggregate key can decrypt any ciphertext provided that the ciphertex's class is contained in the aggregate key via Decrypt.

4.1 User Behavior Profiling

By monitoring data access in the cloud and detect abnormal data access patterns User profiling is a well-known Technique that can be applied here to model how, when, and how much a user entrances their information in the Cloud. Where behavior is continuously checked to determine whether abnormal access to a user's information is occurring. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would materially include sizable information, how many documents are typically read and how often. I monitor for abnormal search behaviors that exhibit deviations from the user baseline the correlation of search behavior anomaly detection with trap based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's cleanness.

4.2 Decoy Technology

Decoy technology is the technology which is providing the decoy information to the unauthorized user or the attacker. Decoy technologies for example honey pot, or the generating The useless data files on the demand of the system to do attack against the attacker. Using this technique the original information gets changed in unexpected format so that the ex-filtering of the document or information is becomes impossible. Decoy means the relative disinformation, Fake information about the respective data documents. This technology is mainly stores some of the decoy data files in the database of the customer as the part of his database. As the decoy files are in same database of the user so that the attacker is gets failed to verify between the actual documents and

decoy documents. As the attacker is going to continuing the attack on user's data documents so there is direct linking fog computing sites. So the Fake documents getting receive to the attacker in the much more amount. As the Fake data is gets downloaded by the attacker he gets confused among which data is the actual targeted data. But all the documents are of the Fake types so the original data is gets secured from the malicious insider attack.

V. RESULT AND DISCUSSION

Our approaches change the compression issue F (F =n inour schemes) to be a tunable parameter, at the cost of O(n)-sized system parameter. Cryptography is tired constant time, whereas coding is tired O(|S|) cluster multiplications (or purpose addition on elliptic curves) with2 pairing operations, where S is that the set of ciphertext classes decryptable by the granted mixture key and $|S| \leq n$.of course, key extraction wants O(|S|) cluster multiplications additionally, that a replacement advance on the stratified key assignment (a ancient approach) that preserves areas providing the entireties of the key-holders share similar edges is our approach of "compressing" secret keys in public key cryptosystems. These public key cryptosystems manufacture cipher texts of constant size nominal economical delegation of secret writing rights forany set of cipher texts is possible. This not exclusively enhances user privacy and confidentiality of data in cloud storage, but it'll this by supporting the distribution or appointing of secret keys varied for diverse} cipher text classes and generating keys by numerous derivation of cipher text class properties of the information and its associated keys. This sums up the scope of our paper. As there is a limit attack selection the quantity the quantity}of cipher text classes beforehand & in addition to the exponential growth inside the quantity of cipher texts in cloud storage, there is a demand for reservation of ciphertext classes for future use. As for potential modifications and enhancements to our current cause, in future, the parameter size area unit usually altered nominal it's freelance of the utmost style of cipher text classes. to boot,a specially designed cryptosystem, with the employment of an accurate security formula, as associate degree example, the Diffie-Hellman Key-Exchange methodology, which can then be imperviable, or at the foremost proof against outpouring at the aspect of economical key appointing, will confirm that one can transport same keys on mobile devices without fear of outpouring.

VI.CONCLUSION

A new advance on the class-conscious key assignment (a ancient approach) that preserves areas providing the entireties of the key-holders share similar edges is our approach of "compressing" secret keys publicly key cryptosystems. These public key crypto systems manufacture cipher texts of the constant size of specified economical delegation of secret writing rights for any set of cipher texts is feasible. This not solely enhances user privacy and confidentiality of knowledge in cloud storage, however it will this by supporting the distribution or appointing of secret keys numerous for diverse} cipher text categories and generating keys by various derivation of cipher text category properties of the info and its associated keys. Of cipher text categories beforehand & let alone the exponential growth within the number of cipher texts in cloud storage, there's a requirement for reservation of cipher text categories for future use. As for potential modifications and enhancements to our current cause, in future, the parameter size are often altered specified it's freelance of the utmost variety of cipher text categories. To boot, a specially designed cryptosystem, with the utilization of a correct security algorithmic rule, as an example, the Diffie-Hellman Key-Exchange methodology, which may then be ladder proof, or at the most proof against outpouring at the side of economical key appointing, can make sure that one will transport same keys on mobile devices without worrying of outpouring.

REFERENCES

[1] key –Aggregate Cryptosystem for Scalable Data Sharing in CloudStorage Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng,Jianying Zhou, and Robert H. Deng, Senior Member, IEEE

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

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted data,"inProceedings of the 13th ACM Conference on Computer andCommunications Security (CCS '06). ACM, 2006, pp. 89–98.

[4] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic andEfficient Key Management for Access Hierarchies,"ACMTransactions on Information and System Security (TISSEC), vol.12,no. 3, 2009.

[5] S. S. M. Chow, C.-K.Chu, X. Huang, J. Zhou, and R. H. Deng,"Dynamic Secure Cloud Storage with Provenance," inCryptography and Security: From Theory to Applications – EssaysDedicated to Jean-Jacques Quisquater on the Occasion of His 65thBirthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.

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

[7] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M.Yiu, "SPICE -Simple Privacy-Preserving Identity-Management for CloudEnvironment," in Applied Cryptography and Network Security –ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.

[8] L. Hardesty, "Secure computers aren't so secure," MIT press,2009,http://www.physorg.com/news176107396.html [9] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data onthe Cloud via Security-Mediator," inInternational Conference onDistributed Computing Systems - ICDCS 2013. IEEE, 2013.

[10] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient ControlledEncryption: Ensuring Privacy of Electronic Medical Records," inProceedings of ACM Workshop on Cloud Computing Security (CCSW'09). ACM, 2009, pp. 103–114.

[11] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-KeyDecryption without Random Oracles," in Proceedings of InformationSecurity and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990.Springer, 2007, pp. 384–398.

[12] G. C. Chick and S. E. Tavares, "Flexible Access Control with MasterKeys," in Proceedings of Advances in Cryptology - CRYPTO'89, ser.LNCS, vol. 435. Springer, 1989, pp. 316–322

[13] W.-G. Tzeng, "A Time-Bound Cryptographic Key AssignmentScheme for Access Control in a Hierarchy," IEEE Transactions onKnowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188,2002.

[14] G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," J.Cryptology, vol. 25, no. 2, pp. 243–270, 2012Cho,

[15] J., Garcia-Molina, H., Page, L., Efficient Crawling: Through URLOrdering, Computer Science Department, Stanford University,Stanford, CA, USA, 1997.

AUTHORS PROFILE:

	**MANDAPALLI SINDHU DEVI** is a student of V.S.LAKSHMI ENGINEERING COLLEGE FOR WOMENS. Presently he is pursuing M.Tech [Computer Science and Engineering] from this college and he also completed his B.Tech .
	Mrs.P.AMARAVATHI, working as a Professor in the Dept.of Computer Science and Engineering from V.S.Lakshmi Engineering College, Matlapalem, Kakinada.