ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2278-2566
Vol.02, Issue.03
October -2018
Pages: -143-147

SECURE DATA SHARING IN CLOUDS VIA DENIABLE ATTRIBUTE-BASED ENCRYPTION

Venkata Sai Rama Krishna T[1], B.Suryanarayana murthy[2]
[1] *M. Tech., Dept of CSE, Sri Sunflower College of Engineering and Technology. AP, India,* krishna.224488@gmail.com @gmail.com
[2] *M. Tech. Assoc Proff, Dept of CSE. Sri Sunflower College of Engineering and Technology. AP, India,* suryanarayanamurthy.b@gmail.com

ABSTRACT
Distributed storage is a use of mists that frees associations from setting up in-house information stockpiling frameworks. Be that as it may, distributed storage offers ascend to security concerns. In instance of gathering shared information, the information confront both cloud-particular and ordinary insider dangers. Secure information sharing among a gathering that counters insider dangers of real yet vindictive clients is an imperative research issue. In this paper, we propose the Secure Information Sharing in Clouds (SeDaSC) procedure that gives: 1) information privacy and trustworthiness; 2) get to control; 3) information sharing (sending) without utilizing figure concentrated re encryption; 4) insider risk security; and 5) forward and in reverse access control. The SeDaSC system scrambles a record with a solitary encryption key. Two diverse key offers for every one of the clients are created, with the client just getting one offer. The ownership of a solitary offer of a key enables the SeDaSC strategy to counter the insider dangers. The other key offer is put away by a trusted outsider, which is known as the cryptographic server. The SeDaSC technique is material to ordinary and versatile distributed computing situations. We execute a working model of the SeDaSC technique and assess its execution dependent on the time developed different activities. In this paper, we present our structure for another distributed storage encryption conspire that empowers distributed storage suppliers to make persuading counterfeit client privileged insights to ensure client security. Since coercers can't confess whenever gotten insider facts are valid or not, the distributed storage suppliers guarantee that client security is still safely ensured.

Key-Words:-Access Control, Cloud-Computing , Deniable Encryption, Attribute-Based Encryption, Cloud Storage

***----------*

I.INTRODUCTION:-

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are numerous ABE schemes that have been proposed ,including [1], [2], [3], [4], [5], [6], [7].Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant [8]. In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies [9], [10]. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness. Though we hope cloud storage providers can fight against such entities to maintain user privacy through legal avenues, it is seemingly more and more difficult. As one example, Lava bit was an email service company that protected all user emails from outside coercion; unfortunately, it failed and decided to shut down its email service [11].Since it is difficult to fight against outside coercion, we aimed to build an encryption scheme that could help cloud storage providers avoid this predicament. In our approach, we offer cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only obtained forged data

from a user's stored ciphertext. Once coercers think the received secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets. Therefore, user privacy is still protected. This concept comes from a special kind of encryption scheme called **deniable encryption**, first proposed in [12]. Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in ciphertexts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence. This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data1.In this work, we describe a deniable ABE scheme for cloud storage services. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. Our scheme is based on Waters cipher text policy-attribute based encryption (CP-ABE) scheme [4]. We enhance the Waters scheme from prime order bilinear groups to composite order bilinear groups. By the subgroup decision problem assumption, our scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers.

II. Literature Survey:-

#1 Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems

Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. Ciphertext-policy attribute-based encryption is a promising cryptographic solution to these issues for enforcing access control policies defined by a data owner on outsourced data. However, the problem of applying the attribute-based encryption in an outsourced architecture introduces several challenges with regard to the attribute and user revocation. In this paper, we propose an access control mechanism using ciphertext-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. We demonstrate how to apply the proposed mechanism to securely manage the outsourced data. The analysis results indicate that the proposed scheme is efficient and secure in the data outsourcing systems.

#2 Role-Based Access Controls

While Mandatory Access Controls (MAC) is appropriate for multilevel secure military applications, Discretionary Access Controls (DAC) is often perceived as meeting the security processing needs of industry and civilian government. This paper argues that reliance on DAC as the principal method of access control is unfounded and inappropriate for many commercial and civilian government organizations. The paper describes a type of non- discretionary access control - role-based access control (RBAC) - that is more central to the secure processing needs of non-military systems then DAC.

#3 Secure Provenances: The Essential of Bread and Butter of Data Forensics in Cloud Computing

Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it is still a challenging issue today. In this paper, to tackle this unexplored area in cloud computing, we proposed a new secure provenance scheme based on the bilinear pairing techniques. As the essential bread and butter of data forensics and post investigation in cloud computing, the Proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

#4 Trust Cloud: A Framework for Accountability and Trust in Cloud Computing

The key barrier to widespread uptake of cloud computing is the lack of trust in clouds by potential customers. While preventive controls for security and privacy measures are actively being researched, there is still little focus on detective controls related to cloud accountability and audit ability. The complexity resulting from the sheer amount of virtualization and data distribution carried out in current clouds has also

Revealed an urgent need for research in cloud accountability, as has the shift in focus of customer concerns from server health and utilization to the integrity and safety of end-users' data. This paper discusses key challenges in achieving a trusted cloud through the use of detective controls, and presents the Trust Cloud framework, which addresses accountability in cloud computing via technical and policy-based approaches.

III. Related Work:-

Xu *et al.* [9] proposed a certificate less proxy re encryption (CL-PRE) scheme for securely sharing the data within a group in the public cloud. In the CL-PRE scheme, the data owner encrypts the data with the symmetric key. Subsequently, the

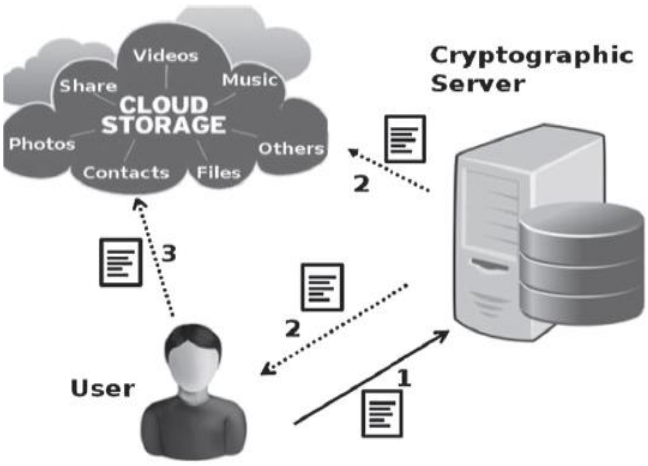
symmetric key is encrypted with the public key of the data owner. Both the encrypted data and the key are uploaded to the cloud. The encrypted key is re encrypted by the cloud (that acts as a proxy re encryption agent) that becomes de cryptable by the user's private key. The public–private keys generated in the proposed scheme are not based on the certificates. The user's identity is used to generate the public–private key pair. The proxy re encryption is based on bilinear pairing and the BDH that makes the CL-PRE scheme computationally intensive. The computational cost of the bilinear pairing is high as compared with the standard operations in finite fields.To reduce the computational overhead of bilinear pairing,

Seo *et al.* [11] introduced a mediated certificate less encryption approach for data sharing in the public cloud that avoids bilinear pairing. In the proposed scheme, the cloud generates the public–private key pairs for all of the users and transmits the public keys to all of the participating users. Partial decryption is performed at the cloud. Due to the fact that key management and partial decryption are handled by the cloud, user revocation is easier to handle. However, the proposed scheme treats the public cloud both as a trusted and un trusted entity at the same time. From a security perspective, it is not recommended to shift the key generation process to the shared multitenant public cloud environment. Moreover, the decryption is performed twice in the system that reduces the advantage of not pairing to some extent.

Algorithm 1 Key Generation and Encryption

Input:
F, the ACL, the SKA, the 256-bit hash function H_f
Compute:
$R = \{0, 1\}^{256}$
$K = H_f(R)$
$C = \text{SKA}(F, K)$
for each user i **in the ACL, do**
$K_i = \{0, 1\}^{256}$
$K_i = K \oplus K_i$
Add K_i' for user i in the ACL
Send K_i' for user i
end for
delete (K)
delete (K_i')
return C to the owner or upload to the cloud.

System-Architecture:-



Basic idea for the SeDaSC methodology.

- **DenSetup**$(1^\lambda) \rightarrow (PP, MSK, PK)$: This algorithm runs **Setup**(1^λ) and obtains PP. System public key PK is $\{g_2g_3, (g_2g_3)^\alpha, e(g_3, g_3)^\alpha, e(g_2g_3, g_2g_3)^\alpha\}$ and system secret key MSK is $\{(g_1g_3)^\alpha, g_1g_2g_3, (g_1g_2g_3)^\alpha\}$.
- **DenKeyGen**$(MSK, S) \rightarrow (SK, FK)$: This algorithm runs **KeyGen** and obtains SK for S. Next, this algorithm picks $t' \in \mathbb{Z}_N$ and generates FK as follows:

$$FK = \{(g_1g_2g_3)^{\alpha+at'}, (g_1g_2g_3)^{t'}, \{H_1(x)^{t'}\}_{\forall x \in S}\} = \{K', L', \{K_x'\}_{\forall x \in S}\}.$$

IV. Conclusion:-

We proposed the SeDaSC approach, which is a cloud capacity security conspire for gathering information. The proposed philosophy gives information classification, secure information sharing without re encryption, get to control for pernicious insiders, and forward and in reverse access control. In addition, the SeDaSC procedure gives guaranteed cancellation by erasing the parameters required to decode a document. The encryption and decoding functionalities are performed at the CS that is a confided in third party in the SeDaSC procedure. The proposed strategy can be likewise utilized to portable distributed computing due to the certainty that register concentrated assignments are performed at the CS. The working of SeDaSC was formally investigated utilizing HLPNs, the SMT-Lib, and a Z3 solver. The execution of the SeDaSC procedure was assessed dependent on the time utilization amid the key age, record transfer, and document download tasks. The outcomes uncovered that the SeDaSC approach can be for all intents and purposes utilized in the cloud for secure information sharing among the gathering. Later on, the proposed philosophy can be stretched out by constraining the trust level in the CS. This will additionally upgrade the framework to adapt to insider dangers. Additionally, the reaction of the strategy with fluctuating key sizes can be assessed.

V.Feature Enhancement & conclusion:-

In this work, we proposed a deniable CP-ABE plan to assemble a review free distributed storage benefit. The deniability include makes compulsion invalid, and the ABE property guarantees secure cloud information offering to a fine-grained get to control instrument. Our proposed plan gives a conceivable method to battle against unethical impedance with the privilege of security. We trust more plans can be made to secure cloud client protection.

VI.References:-

[1] A. Abbas and S. U. Khan, "A review on the State-of-the-art privacy preserving approaches in e-health clouds," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 1, pp. 1431–1441, Jul. 2014.
[2] K. Alhamazani *et al.*, "An overview of the commercial cloud monitoring tools: Research dimensions, design issues, state-of-the-art," *Computing*, DOI: 10.1007/s00607-014-0398-5, 2014, to be published.
[3] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future Gen. Comput. Syst.*, vol. 29, no. 5, pp. 1278–1299, Jul. 2013.
[4] L. Wei, H. Zhu, Z. Cao, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," *Inf. Sci.*, vol. 258, pp. 371–386, Feb. 2014.
[5] Cloud security Alliance, "Security guidelines for critical areas of focus in cloud computing v3.0," 2011.
[6] D. Chen *et al.*, "Fast and scalable multi-way analysis of massive neural data," *IEEE Trans. Comput.*, DOI: 10.1109/TC.2013.2295806, 2014, to be published.
[7] A. N. Khan, M. M. Kiah, S. A. Madani, M. Ali, and S. Shamshir-band, "Incremental proxy re-encryption scheme for mobile cloud computing environment," *J. Supercomput.*, vol. 68, no. 2, pp. 624–651, May 2014.
[8] Y. Chen and W. Tzeng, "Efficient and provably-secure group key management scheme using key derivation," in *Proc. IEEE 11th Int. Conf. TrustCom*, 2012, pp. 295–302.
[9] L. Xu, X. Wu, and X. Zhang, "CL-PRE: A certificate less proxy re encryption scheme for secure data sharing with public cloud," in *Proc. 7th ACM Symp. Inf. , Comput. Commun. Security*, 2012, pp. 87–88.
[10] P. Gutmann, "Secure deletion of data from magnetic and solid-state memory," in *Proc. 6th USENIX Security Symp. Focusing Appl. Cryptography*, 1996, p. 8.
[11] S. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificate less Encryption for Secure Data Sharing in Public Clouds," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2107–2119, Sep. 2013.
[12] Y. Chen, J. D. Tygar, andW. Tzeng, "Secure group key management using uni-directional proxy re-encryption schemes," in *Proc. IEEE INFOCOM*, pp. 1952–1960.
[13] T. Murata, "Petri Nets: Properties, analysis and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.
[14] L. Moura and N. Bjrner, "Satisfiability modulo theories: An appetizer," in *Proc. Formal Methods, Found. Appl.*, vol. 5902, *Lecture Notes in Computer Science*, 2009, pp. 23–36.
[15] S. U. R. Malik, S. K. Srinivasan, S. U. Khan, and L. Wang, "A methodology for OSPF routing protocol verification," in *Proc. 12th Int. Conf. Scal Com*, Changzhou, China, Dec. 2012, pp. 1–5.

VENKATA SAI RAMA KRISHNA .T is a student of sri sunflower college of Engineering and Techonology, Lankapalli Present he is Pursuing his M.tech[Computer Science & Engineering] from this college and he received B.tech Degree(Bachelor of techonology) from the University of JNTUK,Kakinada.

B.Suryanarayana murthy
Associate Professor in sunflower college of Engineering and Techonology Lankapalli and Also Received Master Degree from JNTUK University.Having 12 years of Experience in Faculty.