International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

MINIMIZE SECURITY AND PRIVACY RISKS OF CLOUD STORAGE IN BIG DATA ERA USING A DATA SHARING PROTOCOL

T.MOUNIKA[1], D.V PADMAVATHI [2]
[1] PG SCHOLAR, DEPT OF CSE, ST.MARY'S GROUP OF INSTITUTION, GUNTUR, AP, INDIA.
[2]ASST. PROFESSOR [M.TECH], DEPARTMENT OF CSE, ST.MARY'S GROUP OF INSTITUTION, GUNTUR, AP, INDIA.

ABSTRACT: A cloud-based big data sharing system utilizes a storage facility from a cloud service provider to share data with legitimate users. In contrast to traditional solutions, cloud provider stores the shared data in the large data centers outside the trust domain of the data owner, which may trigger the problem of data condentiality. This paper proposes a secret sharing group key management protocol (SSGK) to protect the communication process and shared data from unauthorized access. Different from the prior works, a group key is used to encrypt the shared data and a secret sharing scheme is used to distribute the group key in SSGK. The extensive security and performance analyses indicate that our protocol highly minimizes the security and privacy risks of sharing data in cloud storage and saves about 12% of storage space.

1.INTRODUCTION

The emerging technologies about big data such as Cloud Computing [1], Business Intelligence [2], Data Mining [3], Industrial Information Integration Engineering(IIIE) [4] and Internet-of-Things [5] have opened a newera for future Enterprise Systems(ES) [6]. Cloud computing is a new computing model, in which all resource on Internet form a cloud resource pool and can be allocated to different applications and services dynamically. Compared with traditional distribute system, a considerable amount of investment saved and it brings exceptional elasticity, scalability and efficiency for task execution. By utilizing Cloud Computing services, the numerous enterprise investments in building and maintaining a supercomputing or grid computing environment for smart applications can be effectively reduced. Despite these advantages, security requirements dramatically rise when storing personal identifiable on cloud environment [7], [8]. This raise regulatory compliance issues since migrate the sensitive data from federate domain to distribute domain. To take the benefit enabled by big data technologies, security and privacy issues [9], [10] must be addressed firstly.

Building security mechanism for cloud storage is not an easy task. Because shared data on the cloud is outside the control domain of legitimate participants, making the shared data usable upon the demand of the legitimate users should be solved. Additionally, increasing number of parties, devices and applications involved in the cloud leads to the explosive growth of numbers of access points, which makes it more difficult to take proper access control. Lastly, shared data on the cloud are vulnerable to lost or incorrectly modified by the cloud provider or network attackers. Protecting shared data from unauthorized

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

deletion, modification and fabrication is a difficult task.

Conventionally, there are two separate methods to promote the security of sharing system. One is access control [11], in which only authorized user recorded in the access control table has the access privilege of the shared data. The other method is group key management [12]_[16] in which a group key is used to protect the shared data. Although access control makes the data only be accessed by legitimate participants, it cannot protect the attack from cloud providers. In the existing group key sharing systems, the group key is generally managed by an independent third party. Such methods assume that the third party is always honest. However, the assumption is not always real especially in the environment of cloud storage.

2.LITERATUREREVIEW

On minimizing energy cost in Internet-scale systems with dynamic data by P. Zhao, W. Yu, S. Yang, X. Yang, and J. Lin

With the tremendous growth of cloud computing and Internet-scale online services, massive geographically distributed infrastructures have been deployed to meet the increasing demand, resulting in significant monetary expenditure and environmental pollution caused by energy consumption. In this paper, we investigate how to minimize the long-term energy cost of dynamic Internet-scale systems by fully exploiting the energy efficiency in geographic diversity and variation over time. To this end, we formulate a stochastic optimization problem by considering the fundamental uncertainties of Internet-scale systems, such as the dynamic data. We develop a dynamic request mapping algorithm to solve the formulated problem, which balances the tradeoff between energy cost and delay performance. Our designed algorithm makes real-time decisions based on current queue backlogs and system states, and does not require any knowledge of stochastic job arrivals and service rates caused by dynamic data queries. We formally prove the optimality of our approach. Extensive trace-driven simulations verify our theoretical analysis and demonstrate that our algorithm outperforms the baseline strategies with respect to system cost, queue backlogs, and delay.

A fuzzy preference tree-based recommender system for personalized business-to-business E-services by D.Wu, G. Zhang, and J. Lu

The Web creates excellent opportunities for businesses to provide personalized online services to their customers. Recommender systems aim to automatically generate personalized suggestions of products/services to customers (businesses or individuals). Although recommender systems have been well studied, there are still two challenges in the development of a recommender system, particularly in real-world B2B e-services: (1) items or user profiles often present complicated tree structures in business applications, which cannot be handled by normal item similarity measures and (2) online users' preferences are often vague and fuzzy, and cannot be dealt with by existing recommendation methods. To handle both these challenges, this study first proposes a method for modeling fuzzy tree-structured user preferences, in which fuzzy set techniques are used to express user preferences. A

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

recommendation approach to recommending tree-structured items is then developed. The key technique in this study is a comprehensive tree matching method, which can match two tree-structured data and identify their corresponding parts by considering all the information on tree structures, node attributes, and weights. Importantly, the proposed fuzzy preference tree-based recommendation approach is tested and validated using an Australian business dataset and the MovieLens dataset. Experimental results show that the proposed fuzzy tree-structured user preference profile reflects user preferences effectively and the recommendation approach demonstrates excellent performance for tree-structured items, especially in e-business applications. This study also applies the proposed recommendation approach to the development of a Web-based business partner recommender system.

3.EXISTING SYSTEM

Rao [19] proposed a secure sharing schemes of personal health records in cloud computing based on ciphertextpolicy attributed-based(CP-ABE) signcryption [20]. It focus on restricting unauthorized users on access to the confidential data. Liu *et al.* [21] proposed an access control policy based on CP-ABE for personal records in cloud computing as well. In [19] and [21],only one fully trusted central authority in the system is responsible for key management and key generation. Huang *et al.* [22] introduced a novel public key encryption with authorized equality warrants on all of its ciphertext or a specified ciphertext. To strengthen the securing requirement, Wu *et al.* [23] proposed an efficient and secure identity-based encryption scheme with equality test in cloud computing. Xu *et al.* [24] proposed a CP-ABE using bilinear pairing to provide users with searching capability on ciphertext and fine-grained access control. He *et al.* [25] proposed a scheme named ACPC aimed at providing secure, efficient and fine grained data access control in P2P storage cloud. Recently, Xue *et al.* [26] proposed a new framework, named RAAC, to eliminate the single-point performance bottleneck of the exiting CP-ABE based access control schemes for public cloud storage. While these schemes use identity privacy by using attribute-based techniques which fail to protect user attribute privacy. The most recent work addressing the privacy issues in a cloud-based storage is carried out by Pervez *et al.* [27], who proposed a privacy aware data sharing scheme SAPDS. It combines the attribute based encryption along with proxy re-encryption and secret key updating capability without relying on any trusted third party. But the storage and communication overhead of SAPDS is decided by attribute encryption scheme.

In the existing work, there is no group based access control system.

The system's security is very less due to lack of strong cryptography techniques.

4.PROPOSED SYSTEM

In SSGK, an efficient solution is proposed to solve the secure problems of data sharing on the cloud storage without relying on any trust third party. Beyond using symmetric encryption algorithm [11] to encrypt the shared data, asymmetric algorithm [12] and secret sharing scheme [28], [29] is used to prevent the key used to decrypt the shared

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

data from getting by unauthorized users. Secret sharing schemes were introduced by both Blakley [30] and Shamir [31] independently in 1979 as solution for safe guarding cryptography keys. In a secret sharing scheme, a secret is divided into n shares by a dealer and shared among n shareholders. Any t shares can reconstruct this secret. Chor et al. [32] extended the notion of the original secret sharing and presented a notion of verifiable secret sharing (VSS). The property of verifiability means that shareholders are able to verify whether their shares are consistent.

The data owner is totally trusted and will never be corrupted by any adversaries.

The system is more secured due to the group key is distributed by running the secret sharing scheme. Parts of the group members can gather their sub secret shares to reconstruct the group key.

5.SYSTEM ARCHITECTURE:

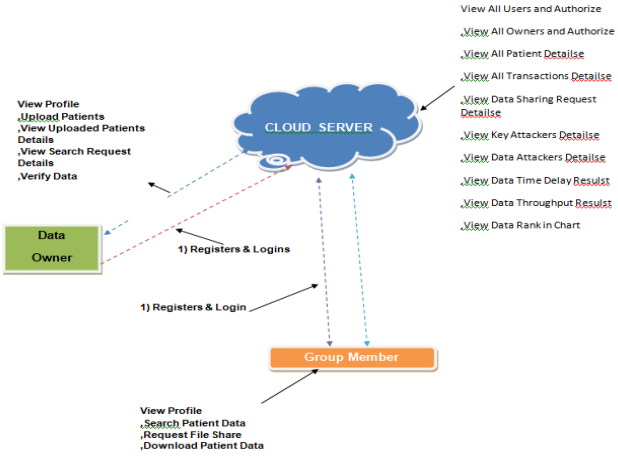


Fig 4.1 architecture Diagram

6. IMPLEMENTATION

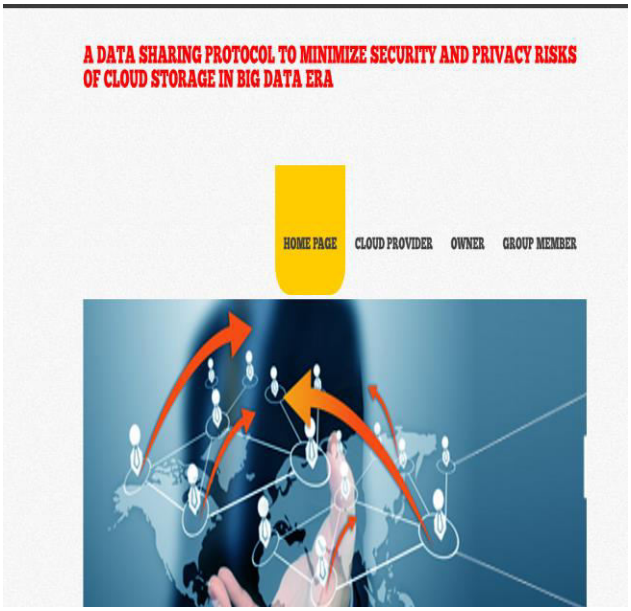
The cloud provider: provides a public platform for data owners to store and share their encrypted data. The cloud provider doesn't conduct data access control for owners. The encrypted data can be download freely by any users.

Data owner: defines the access policy and encrypts its data with a symmetric encryption algorithm using a group key. The group members who satisfied the access policy constitute a sharing group. Then secret sharing scheme is used by the owner to distribute the encryption key to the sharing group. Group members: every group member including the data owner is assigned with an unique and a pair of keys.

The group members can freely get any interested encrypted data from the public cloud. However the user can decrypt the data if and only if it get the data decryption key from the data owner.

7. SCREEN SHOTS

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



8.CONCLUSION

In this paper, we propose a novel group key management protocol for the data sharing in the cloud storage. In SSGK, we uses RSA and verified secret sharing to make the data owner achieve fine-grained control over the outsourced data without relying on any third party. In addition, we give detailed analysis of possible attacks and corresponding defenses, which demonstrates that GKMP is secure under weaker assumptions. Moreover we demonstrate that our protocol exhibits less storage and computing complexity. Security mechanism in our scheme guarantees the privacy of grids data in cloud storage. Encryption secures the transmission on the public channel; verified security scheme make the grids data only accessed by authorized parties. The better performance in terms of storage and computation make our scheme more practical.

The problem of forward and backward security in group key management may require some additions to our protocol. An efficient dynamic mechanism of group members remains as future work.

9.BIBILOGRAPHY

[1] P. Zhao, W. Yu, S. Yang, X. Yang, and J. Lin, ``On minimizing energy cost in Internet-scale systems with dynamic data," IEEE Access, vol. 5, pp. 20068_20082, 2017.

[2] D.Wu, G. Zhang, and J. Lu, ``A fuzzy preference tree-based recommender system for personalized business-to-business E-services," IEEE Trans. Fuzzy Syst., vol. 23, no. 1, pp. 29_43, Feb. 2015.

[3] X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, ``Data mining with big data," IEEE Trans. Knowl. Data Eng., vol. 26, no. 1, pp. 97_107, Jan. 2014.

[4] X. Shi, L. X. Li, L. Yang, Z. Li, and J. Y. Choi, ``Information _ow in reverse logistics: An industrial information integration study," Inf. Technol. Manage., vol. 13, no. 4, pp. 217_232, Dec. 2012.

[5] N. Bizanis and F. A. Kuipers, ``SDN and virtualization solutions for the Internet of Things: A survey," IEEE Access, vol. 4, pp. 5591_5606, May 2016.

[6] S. Li, L. Xu, X. Wang, and J. Wang, ``Integration of hybrid wireless networks in cloud services oriented enterprise information systems," Enterprise Inf. Syst., vol. 6, no. 2, pp. 165_187, Nov. 2012.

[7] K.-Y. Teng, S. A. Thekdi, and J. H. Lambert, ``Risk and safety program performance evaluation and business process modeling," IEEE Trans. Syst., Man, Cybern. A, Syst. Humans, vol. 42, no. 6, pp. 1504_1513, Nov. 2012.

[8] Z. Fu, X. Sun, S. Ji, and G. Xie, ``Towards ef_cient content-aware search over encrypted outsourced data in cloud," in Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM), Apr. 2016, pp. 1_9.
[9] J. Han, W. Susio, Y. Mu, and J. Hou, ``Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 665_678, Mar. 2015.
[10] D. Zou, Y. Xiang, and G. Min, ``Privacy preserving in cloud computing environment," Secur. Commun. Netw., vol. 9, no. 15, pp. 2752_2753 Oct. 2016.
[11] Y. Tang, P. P. C. Lee, John C. S. Lui, and R. Perlman, ``Secure overlay cloud storage with access control and assured deletion," IEEE Trans. Dependable Secure Comput., vol. 9, no. 6, pp. 903_916, Nov./Dec. 2012.
[12] J. Shao, R. Lu, and X. Lin, ``Fine-grained data sharing in cloud computing for mobile devices," in Proc. IEEE Conf. Comput. Commun. (INFOCOM), Apr./May 2015, pp. 2677_2685.
[13] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ``Privacypreserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362_375, Feb. 2013.
[14] S. Tanada, H. Suzuki, K. Naito, and A. Watanable, ``Proposal for secure group communication using encryption technology," in Proc. 9th Int. Conf. Mobile Comput. Ubiquitous Netw., Oct. 2016, pp. 1_6.
[15] J. Zhou et al., ``Securing outsourced data in the multi-authority cloud with _ne-grained access control and ef_cient attribute revocation," Comput. J., vol. 60, no. 8, pp. 1210_1222, Aug. 2017.
[16] R. Ahuja, S. K. Mohanty, and K. Sakurai, ``A scalable attribute-set-based access control with both sharing and full-_edged delegation of access privileges in cloud computing," Comput. Elect. Eng., vol. 57, pp. 241_256, Jan. 2017
[17] J. Thakur and N. Kumar, ``AES and blow_sh: Symmetric key cryptography algorithms simulation based performance analysis," Int. J. Emerg. Technol. Adv. Eng., vol. 1, no. 2, pp. 6_12, Dec. 2011.