An Analysis of secure user data in cloud computing using encryption techniques

Dr. S. Hari Ganesh[1], C.Geetha[2],

1Assistant Professor, Computer Science, Bishop Heber College, Trichy, India[1]

2Mphil.Scholor, Computer Science, Bishop Heber College, Trichy, India[2]

Abstract

Cloud computing is a model for enabling suitable, on-demand network access to a shared pool of configurable and reliable computing resources. It provides the capabilities of computing and storage resources. Cloud storage is a model of data storage where the digital data is stored in logical pools. The cloud storage providers are responsible for keeping the data available and accessible.To keep the data safe encryption is the best technique for converting data into another form which cannot be easily understood by anyone except authorized parties. Cloud encryption is a service offered by cloud storage providers whereby data or text transformed using encryption algorithms and then placed on a storage cloud. In this paper we have discussed about safe data storage in cloud, possible issues, and comparison of security algorithms.

Keywords

Cloud computing, Cloud storage**,** Data security, Encryption algorithms.

Introduction

Cloud computing means storing and accessing data and programs over the internet. The important aspect of cloud computing is secure data which has been stored and cannot be hacked. Even though there are some security issues for the sensitive data many possible solutions also therefor a trust worthy cloud environment [1]. Cloud storage is a service model in which data is maintained, managed and back up remotely and made available to user over a network. The three main cloud storage models are public cloud, private cloud, hybrid cloud [2]. Private cloud storage services provide a dedicated environment protected behind an organization's firewall. These clouds are appropriate for users who need customization and more control over their data. Public cloud storage services provide multi-tenant storage environment that is more suitable. Hybrid cloud storage is a combination of the other two models that includes at least one private cloud and public cloud infrastructure.

The concept of secure storage includes certain techniques which keeps all data safe. Cloud storage providers can offer a service called cloud encryption whereby data or text is transformed using encryption algorithms and then placed on a storage cloud. This would be useful for the users to protect confidentiality of data stored [3]. The advantage of cloud computing storage is includes augment or back up existing storage systems, migrating clouds. Some services of cloud storage come in hybrid implementations that link to remote service provider's storage. These arrangements can make cloud data storage for feasible alternative and promising option for remote site storage.

Methodology

A systematic review presented in [6] is followed in this research work to present the comparison

ISSN: 2278 – 1323

for different approaches related which are absolutely related to encryption techniques used for data confidentiality. The focus of this review is to find out the solution for encryption failure during cloud storage process. Some researchers contribute their efforts in data correctness as well as efficiency in [3]. In [8] review process was adopted partially for comparing encryption techniques in cloud computing.

Issues and challenges of data security

Cloud computing technologies include the control based one for data security to protect data. User access control is one of the best concern for prevent from malicious activity. There are data security challenges in the cloud, the need to protect confidential data, auditing, compliance concern, and loss of visibility. Following table differentiates the defect of each encryption algorithms.

TABLE 1: COMPARISON OF PUBLIC KEY ENCRYPTION RELATED ALGORITHMS

TECHNIQUES	**MERITS**	**DEMERITS**
RSA Encryption	1.Using the RSA encryption providing more security	1. Problem during file transferring
Predicate Encryption	**1.** Creating Generic Model for providing Security.	**1.** Problem of Uploading Files
Fuzzy Identity-Based Encryption	**1**. Using User Attribute Encrypt the File. 2. Keys Encryption	**1.** Hamming Distance Problem. 2. Error Tolerant

Review of literature

The author has been analyzed as follows regarding secure data storage in cloud and encryption algorithms. The following paper explains the techniques which are related to secure storage and its merits and demerits.

CONG WANG AND KUI REN, focused about auditing data storage for correctness guarantee. The scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers. But the public key encryption scheme needs to be developed to overcome the problem of encryption failure.

Result and discussion

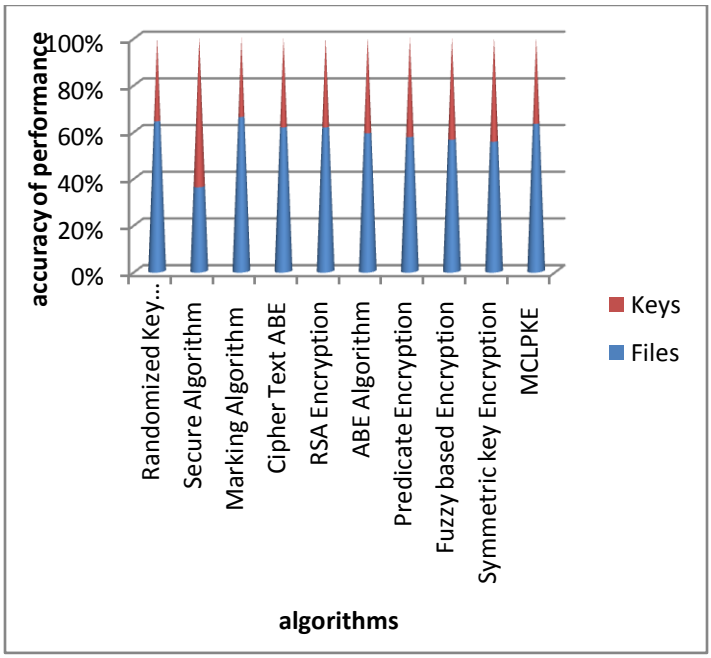
During review the concepts of security issues in cloud computing and different encryption techniques for data storage were compared. The reason for encryption failure has been identified and the possible solutions are provided. The following table describes merits and demerits of MCL-PKE scheme. And the graph denoting accurate performance of various algorithms.

ISSN: 2278 – 1323

TABLE 2: MERITS AND DEMERITS OF MCL-PKE SCHEME

SCHEME	MERITS	DEMERITS
MCL-PKE SCHEME	1. Asymmetric key generation 2. Solves key escrow problem 3. Solves revocation problem	1. No assurance for storage correctness guarantee. 2. Encryption failure.

FIGURE 1: COMPARISON OF ALGORITHMS



Conclusion and Future enhancement

In this paper encryption scheme has been proposed to make storage of data in cloud successfully without encryption failure. Security issues and challenges and also comparisons have been made between RSA encryption, predicate encryption and fuzzy identity based encryption to find which is best and it has to be used in cloud data storage. An encryption technique plays an important role for safe storage of data in cloud. In future several approaches can be compared to produce security results and effective framework can be provided.

References

[1]Cong wang and kuiRen, "Toward Publicly Auditable secure cloud data storageservices", IEEE , 2010.

[2] Qian wang et al, "Privacy preserving public auditing for secure cloud storage", vol 62, IEEE, 2013.

ISSN: 2278 – 1323

[3] Ayman kayssi et al, "Privacy as a sevice: Privacy aware data storage & processing in cloud computing architecture", IEEE, 2009.

[4] Carlo curino et al, " Relational Cloud : A Database as a service for the cloud", 5th Biennial conference on innovative Data system Research, CIDR, 2011.

[5] Kui Ren," Security Challenges for the public cloud", IEEE, 2012.

[6] Mohammed A. Alzain et al, "Cloud computing security: From single to multi clouds", 45th Hawai International Conference on system sciences, 2012.

[7]Sushmita Ruj et al" DACC: Distributed Access Control in Clouds", International joint conference of IEEE, ICESS, 2011.

[8]Rachna Arora et al," secure user data in cloud computing using encryption algorithms", IJERA, ISSN:2248-9622, vol 3, issue 4, 2013.

[9]Cong wang et al," Towards secure & Dependable storage services in Cloud computing", IEEE, vol5, issue2,2012.

[10] Mandeep kaur and Manish Mahajan," Using encryption algorithms to enhance data security in cloud computing",

[11] Gurudatt Anil Kulkarni et al," A Security aspect in cloud computing", ICSESS, vol 10, 2012.

[12] Aized amin soofi et al, " Encryption Technique for cloud data confidentiality", vol 7, IJGDC, 2013.

[13] M. Abdalla et al., "Searchable encryption revisited: Consistency properties, relation to anonymousibe, and extensions", vol 21, no 3, Springer, pages 350– 391, 2008.

[14] S. Al-Riyami and K. Paterson, "Certificate less public key cryptography", In Proceedings of Advances in Cryptology - ASIACRYPT, volume 2894 of Lecture Notes in Computer Science, pages 452–473, Springer Berlin / Heidelberg, 2003.

[15]. E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents", ACM Transactions on Information and System Security, vol 5, no 3 pages 290–331, 2002.

[16]. A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption", In SP '07: Proceedings of the IEEE Symposium on Security and Privacy, pages 321–334, Washington, DC, USA, 2007.

[17]. S. Coull, M. Green, and S. Hohenberger, "Controlling access to an oblivious database using stateful anonymous credentials", In Irvine: Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography, Springer, pages 501–520, Berlin, Heidelberg, 2009.

[18]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", In CCS '06: Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98, ACM New York, USA, 2006.

[19]. J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products", In Proceedings of the theory and applications of cryptographic techniques 27th annual international conference

ISSN: 2278 – 1323

on Advances in cryptology, EUROCRYPT'08, pages 146–162, Berlin, Heidelberg, Springer-Verlag, 2008.

[20]. A. Sahai and B. Waters, "Fuzzy identity-based encryption", In LNCS 3494, Proc. EUROCRYPT, pages 457–473, Springer - Verlag, 2005.

[21]. N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A privacy preserving approach to policy-based content dissemination", In ICDE 10, Proceedings of the IEEE 26th International Conference on Data Engineering, 2010.

ISSN: 2278 – 1323