Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.516 – 520

RESEARCH ARTICLE

Security Issues Related to Data Storage in Cloud

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

[1]Computer Science, Bishop Heber College, Tiruchirappalli

[2]Computer Science, Bishop Heber College, Tiruchirappalli

[1] hariganesh17@gmail.com; [2] geetha.c2290@gmail.com

Abstract— Cloud computing represents today's most exciting computing archetype. It gives computing via internet. Cloud systems can be used to enable data sharing capabilities and this can provide abundant of benefits to the user. It is the most important trend in cloud technology for allows users to access data expediently. Privacy and security is the big challenge for stored data in cloud. Most existing algorithms are low in level of security comparing with mCL-PKE (mediated Certificate Less – Public Key Encryption) scheme. This scheme gives protection via encryption and decryption to share sensitive data in public cloud without combining operation. The scheme has been introduced as efficient certificate less cryptography technique. It can solve key escrow and revocation problem in public key cryptography. The purpose of this paper is to review all the existing algorithms related to public key encryption and point out the best in efficiency and needed implementations.

Keywords— Cloud computing, public cloud, public key cryptography, mcl-pke scheme.

I. INTRODUCTION

Cloud computing is a compilation of existing techniques and technologies wrapped within a new infrastructure paradigm that offers improved, scalability, elasticity, and business agility, faster start up time, reduced management costs and just in time availability of resources. Cloud computing infrastructure security is greatly affected by whether the cloud employed is a private cloud or a public cloud. The public cloud infrastructure, however, requires that an organization rethink security architecture and processes how its network fits with the network. A secure cloud implementation must reduce risk to managing confidential data, integrity, and availability, as well as protect data storage and ensure proper access control. Information that requires a higher level of classification than public data. This information is protected from a loss of confidentiality as well as from a loss of integrity due to an unauthorized alteration. This classification applies to information that requires special precautions to ensure the integrity of the information by protecting it from unauthorized action with modify or delete the data. It is information that requires a higher than normal assurance of accuracy and completeness. Today cloud computing communications replaces traditional outsourcing techniques and provides flexible services to clients at different locations via Internet. This leads to the constraint for data classification to be performed by potentially less security servers in the cloud and lot of problems like key escrow problem (Hacking problem), revocation problem in public key cryptography.

II. PUBLIC KEY CRYPTOGRAPHY

Any cryptographic primitive should meet security and a consistent condition ensures that the original fulfils its function [1]. Today the main difficulty in developing secure systems based on public key cryptography and it is not the problem of choosing properly secure algorithms or implementing those algorithms. Slightly, it is the

deployment and management of infrastructures to support the authenticity of cryptographic keys: there is a need to provide an assurance to the user about the relationship between a public key and the identity or authority of the holder of the corresponding private key. In a traditional Public Key Infrastructure (PKI), this assurance is delivered in the form of certificate, signature by a Certification Authority (CA) on a public key [2]. A first requirement is the support for varying protection granularity levels. In some cases, the same access control policy may apply to a set of documents. In other cases, different access control policies may apply to different components within the same document. Many other transitional situations may also arise. The access control mechanism must be flexible to support a spectrum of protection granularity levels [4]. Most existing public key encryption methods allow a party to encrypt data to a particular user, but they are unable to competently handle more expressive types of encrypted access control and privacy assurance [5]. There is an increasing need to provide privacy to users accessing sensitive medical and financial information.

III. MCL-PKE

Without combining operations the mCL-PKE scheme giving solution for sharing sensitive information in public clouds. The cloud is employed as a safe storage as well as a key generation center. In this system, the data owner encrypts the Secret (sensitive) data using the cloud generated users' public keys based on its access control policies and uploads the encrypted data to the cloud. Upon booming approval, the cloud incompletely decrypts the encrypted data for the users. The users accordingly fully decrypt the incompletely decrypted data using their private keys. The privacy of the satisfied and the keys is preserved with respect to the cloud, because the cloud owner cannot fully decrypt the information. The following diagram shows the public key encryption process in data storage.

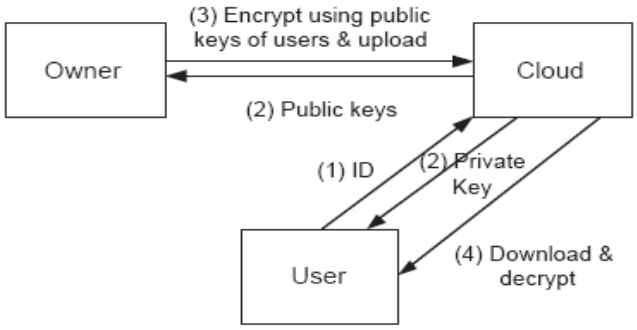

Fig. 1 Process of public key encryption

The diagram explains the process of key encryption that the user can access the private key from cloud for downloading the files and decryption purpose. In which the data files stored in cloud have already been encrypted and uploaded by the cloud owner using public keys. By implementing MCL-PKE scheme the overall cloud systems can provide more secure file storage without key hacking problem.

IV. LITERATURE SURVEY

The distinguishing authors have been analysed as follows regarding public key encryption using certificate less scheme. The following papers explain the algorithms which are related to public key encryption and its merits and demerits.

M. ABDALLA and M. BELLARE., focused about consistency properties in public key encryption and used searchable encryption method to encrypt and decrypt the user's file. With the implemented randomized key generation algorithm key generation is easy enough.

S. AI.RIYAMI and K. PATERSON., produced an approach to reduce the escrow problem using certificate less public key encryption. This is the best approach to provide identity based encryption for finding out key accuracy in public key infrastructure.

E. BERTINO and E.FERRARI., proposed online key distribution method by using marking algorithm. This method is an efficient approach for secure document distribution to the user by using key distribution.

J. BETHANCOURT et al., examined key policy attribute based encryption for maintaining confidential data storage. The cyber text policy attribute based method is best in validating the user while accessing the files.

S. COULL et al., found out signature scheme to detect the hackers and invalid users. To provide more security at all levels in file storage, RSA encryption has been introduced with signature scheme.

V. GOYAL et al., created an approach to provide private keys for users. This method is best in securely managing the data because the main advantage is invalid user cannot audit the file which is in encrypted format. Only particular users can access the file by decrypting who had private keys.

J. KATZ et al., created a generic model for providing security. The method used for this generic model is hidden vector encryption which is best in providing high level security to the files.

A. SAHAI and B. WATERS., produced a key generation method which will encrypt the file by using users attributes. Keys encryption is the main advantage.

N. SHANG et al., developed symmetric key encryption in which oblivious commitment based envelope is proposed. This method provides rekey process and it is not transparent. Merit of this method is the user no needs to distribute the actual keys during the registration phase.

V. RESULT AND DISCUSSION

The use of mediated certificate less public key encryption is asymmetric key generation. The data owner and user can encrypt and decrypt the files using different keys. The cloud owner does not know the actual keys. They just transmit the files only. The following table consists of merits and demerits of the existing algorithms which are related to public key encryption during data storage into cloud.

TABLE I
COMPARISON OF PUBLIC KEY ENCRYPTION RELATED ALGORITHMS

SALGORITHM	**MERITS**	**DEMERITS**
Randomized Key Generation Algorithm	1. Using Public Key Encryption (encrypt and Decrypt the files)	1. Inconsistency of data. 2. Searchable Encryption
Secure Algorithm	**1.** Reduced the escrow using certificate less public key encryption. 2. Using Identity based encryption for key accuracy.	**1**. Problem of accuracy of keys. 2. Computational Problem
The Marking Algorithm	1. Efficient approach for secure Document Distribution using key Distribution.	1. More Complexity for providing security for documents.
Cipher text-Policy Attribute-Based Encryption	1. More confidential for data storage server. 2. Only valid user decrypts the files.	1. More Collusion attack. 2. Problem of Multi authority process and also unable to encrypt the data by particular user while using public key encryption
RSA Encryption	1.Using the RSA encryption providing more security	1. Problem during file transferring
Attribute Based Encryption	**1.** Can't able to audit because of file content is in encrypted format. 2. Only particular valid users can login and decrypt the files using keys.	**1.** Serious problem is audit logs 2. Less Security

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
Symmetric-key encryption algorithm	**1.** Rekey process is not transparent. 2. Users by not distributing actual keys during the registration Phase.	**1.** Major source of data theft and privacy breaches. **2.** Disseminated contents 3. Bandwidth overhead

The result demonstrates the effectiveness of the mcl-pke scheme. The accuracy of secure encryption is compared and shown in following graph. It shows the performance of the existing encryption algorithm. As can be seen from the below graph the mcl-pke scheme is best in providing security for the files using algorithms.

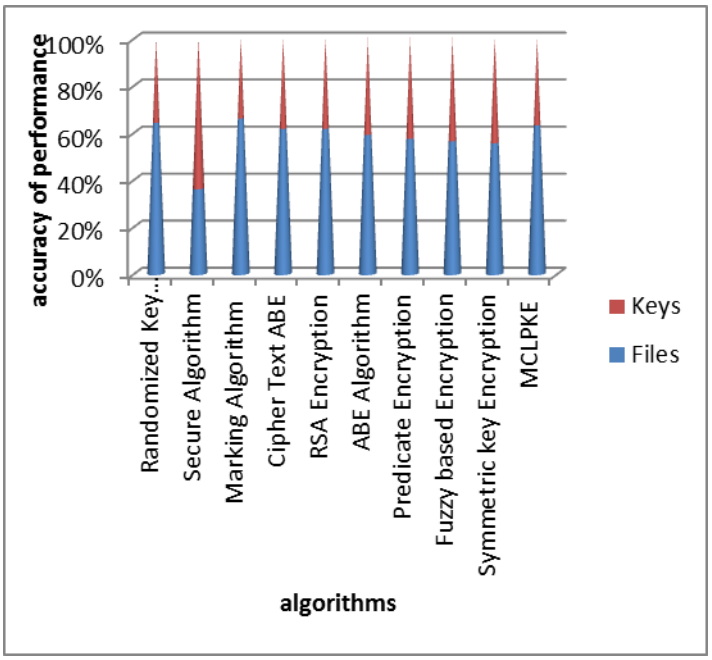

Fig. 2 Comparison of algorithms

VI. LIMITATIONS

Although the mediated certificate less public key encryption is best than existing algorithms to provide better secure encryption and decryption, this approach still needs to be improved in terms of avoiding decryption failure. This improvement will give the assurance to avoid the delay while storing the data in cloud. The following table consists of merits and demerits of mcl-pke scheme.

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.

VII. CONCLUSION

Since we have visited hundred papers which is absolutely related to public key encryption the proposed system can be assessed. And also categorized and compared all the existing algorithms which have been used for developing public key encryption to find the best. We conclude this paper as the improved approach performs single encryption of each stored data item in cloud safely by avoiding encryption failure. With this few further implementation of mcl-pke scheme can satisfy multiple users of cloud. An improved approach will provide more confidentiality for the data stored in untrusted public cloud.

REFERENCES

[1] M. Abdalla et al., "Searchable encryption revisited: Consistency properties, relation to anonymousibe, and extensions", vol 21, no 3, Springer, pages 350– 391, 2008.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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 on Advances in cryptology, EUROCRYPT'08, pages 146–162, Berlin, Heidelberg, Springer-Verlag, 2008.
[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption", In LNCS 3494, Proc. EUROCRYPT, pages 457–473, Springer - Verlag, 2005.
[9] 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.

