International Journal of Engineering & Technology, 7 (2.8) (2018) 358-360

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A comprehensive survey of pre-authentication approach towards proxy re-encryption in cloud data context

Amish Singh[1], Saurabh Shukla[2], Sowmiya. B[3]

[1,2]SRM Institute of Science & Technology,
[3]Assistant Professor, SRMIST – Dept. of CSE
**Email: amish_singh@srmuniv.edu.in*

Abstract

This survey paper categorizes, compares, and summarizes the algorithms, data sets and performance measurement in the published articles related to proxy re-encryption and medical systems. Most of the systems either deploy a pre-authentication approach or a proxy re-encryption approach, they are seldom seen together. Most of the systems either take a patient -centric or a doctor-centric approach whereas the demand is for a common system that can be accessible to all access groups. Multi-data sharing is another concept that is necessary to be implemented in the newer systems and is lacking in many of them .The proposed system overcomes all these problems . It uses RSA for the pre authentication and AES algorithm to to perform pre authentication.

Keywords: *Pre-Authentication, Proxy Re-encryption, Identity-based encryption(IBE), Ciphertext.*

1. Introduction

Cloud storage is a tool that the users get from the cloud to be able to host their data over the cloud. Data security is provided in an organized manner over the cloud by a service called data access control. But the existing public key encryption (PKE) is not anon. , i.e., when the parties receive the ciphertexts, they can very easily differentiate between the sender and receiver of the ciphertext. The public key encryption cannot help to keep anonymity of the users in addition to send and acquire the ciphertext. To achieve the anonymity and data confidentiality, the proposed system combines the public-key algorithm as proxy re-encryption and attribute-based pre-authentication technique which ensure the security of the attributes as well as the data. A proxy re-encryption method is applied which ensures the multiple sharing of secured data. It also ensures that the information I.D and original message of both the cipher text parties is not leaked and it also ensures it is not exposed to cipher text attacks. The privacy of encrypted data depends on the secrecy of the key needed to decrypt it. So the proposed system works at reducing the vulnerability of sharing the secret key. For providing higher levels of security, the symmetric keys are shared using public key cryptography.

2. Literature Review

[1]This literature discusses a fine-grained data access control framework for accessing personal health record data over the cloud, in a multiple owner environment. To make sure that each user has absolute oversight of their healthcare data, the encryption standard used in this system is attribute based encryption, where every user creates their own set of ABE keys. In this fashion, public health record data can be selectively shared by the patient to a set of users by encrypting the file based on a number of attributes, and this encryption and user management complexity is directly proportional to the quantity of attributes used instead of the amount of data proprietors in the framework. The advantage that the system provides are the low complexity in encryption as well a key management due the large number of users. The security at the receiver end is lacking though.

[2]In EHR systems, hospitals, devices, and patients can upload health records and obtain and view them at any given instance. To preserve the patient's privacy these types of systems, Patient Controlled Encryption (PCE) is used as a means to secure and privately store the patient's medical records. This means that the patient can selectively share records with healthcare providers and doctors. A hierarchical encryption system defines the soul of the soul of the system design. The PHR is organized in a hierarchical structure, where a key is assigned to every level in the hierarchy. The patient stores a root secret key, from which a tree of subkeys is obtained. The user passes out subkeys selectively for decryption restricting access to only certain portions of his record. For selective search of portions of the records, the patient is given the power to create and allot trapdoors. Patient Controlled Encryption system stops the unauthorized users from accessing the patient's data by healthcare providers and data storage providers. Sometimes, a patient can unknowingly allow access to a corresponding class without the knowledge of the the type of file. The complexity in key management is high due to all the low-level categories involved, that requires different decryption keys for each category.

[3]Accomplishing effective trust management in DTN's is the primary objective of this system, therefore a probabilistic misbehavior detection scheme is deployed. It varies from pre-existing systems which consider only one of the two out of incentive schemes or misbehavior detection, this work combines the incentive scheme and misbehavior detection in a single framework. Inspection game is what inspires the system in

question here, a figurehead called the inspector inspects a party called the inspectee who has to adhere to a certain set of legal rules. This is a model derived from the modern game theory. Here, the inspector provides a restricted check on the inspectee but it is a restricted one due to the limited amount of resources available too him, here the inspectee may be interested in violating the rule set. To discourage this behavior the inspector can perform a partial check and give a punishment to the inspectee. Moreover, the inspectee can be put through a check by the inspector to check the probability against the Nash equilibrium points and a higher probability means that the probability of offenses is lower, as rationality forces strict following of the rules on the part of the inspectee. It has a low cost and detection overhead. Although there is a big disadvantage, the data is leaked due to transmission of data from provider to another cloud center.

[4]To translate an encryption under X's identity into another system under Y's identity, an identity based proxy-re encryption system is deployed. The translation has to be performed without knowing the plaintext, to achieve this proxy keys or encryption keys are used. Furthermore, the proxy keys should give out no information about the secret key's of X and Y. A simple extension to an identity based encryption scheme gave birth to the PRE rendition of it. It is a two prong system, an algorithm for the generation of encryption keys for assignment to the proxy is the first part. The second prong is for re-encryption and here the ciphertexts are given re-encryption keys by the proxy and their identity is re-made into another one. The re-encryption keys are generated by the delegator with the aid of his IBE secret key, this is the trademark of a non interactive system. The IBE master secret key isn't a requirement. It prevents ciphertext attacks a well but a detailed Pre-Authentication mechanism has not been investigated.

[5] The most important concern for any system providing means for data storage is Security. The cloud plays an important role in accessing and storage of big data because of it's efficient data processing capability. The confidentiality and integrity of the data must be maintained by assuring that the data is accessed only by the authorised users after their credentials get approved and at the same time the anonymity of service providers should be taken care of. We need to make sure that only the encrypted data is provided to the authorised individuals by the data owners in accordance to a set of restrictions and high quality encrypted data sharing should be provided by such systems. In the system being discussed only the cipher-text is shared multiple times maintaining it's integrity and after a process of several authentication steps while ensuring that the non-encrypted data along with the identity of it's users is secured and made invulnerable to cipher text attacks. In this system, detailed Pre-Authentication mechanism has not been investigated.

[6]A cipher-text encrypted under one key can be converted into an encryption done under a different key using a proxy and the technique is known as Proxy Re-Encryption(PRE). The proxy performs all it's translations keeping a track that all the information is encapsulated and only the information that is needed to allow the translations is revealed. The most trivial requirement is that the proxy stays unaware of the keys that are used to encrypt the data by the users. However, a problem exists where almost all the PRE schemes can easily identify the encryption keys of the participants. For reference, in a secure distributed file system, the users use a proxy to encrypt confidential information without giving the identity of the recipient, therefore sometimes an anonymous private-key re-encryption is used in order to solve the prior issue. Therefore a private key PRE system is is built to test the CPA security using a simple extension of a decision bi-linear Diffie Hellman system and to prove the key privacy of the standard model, a decision linear assumption of the aforementioned algorithm is built . The advantages of this system are that it prevents cipher text attacks (CCA), provides the facility for multiple receiver update and reduces workload. The only disadvantage is that the computation overhead is heavy.

[7]This paper examines a straightforward and resourceful approach towards a CPA-secure identity-based encryption (IBE) scheme from which a CCA-secure public key encryption scheme can be dervied. A CCA-secure encryption scheme depends upon only an IBE scheme which fulfilling the weaker conception of security [1]. A CCA secure PKE is obtained from an identity based encryption scheme is the following way: the new secret key of the system is the master secret key of the identity based encryption scheme and correspondingly, the new public key is the old master public key .For the encryption process a key-pair (vk, sk) is generated by the user for a one-time strong signature scheme. The "identity" vk is then used as a reference to encrypt the message [4] Then sk is obtained by signing the ciphertext C which was obtained a consequence of the encryption. The identity based encryption ciphertext C, the signature σ and vk or the verification key make up the final ciphertext. The reciever obtains a signature on c w.r.t. to vk and outputs O, this is done to decrypt C. The receiver derives the secret key Skvk with respect to the "identity" vk on successful authentication, the main IBE scheme[1]with the help of SkVk decrypts the ciphertext. This framework works more efficiently along with security features. Although, secure Multi-data sharing requirement has not been investigated in this system.

3. Conclusion

The proposed system provides means of highly secure data sharing in a cloud environment . The confidentiality and anonymity of data is maintained by encrypting it during the sharing process . The security of data and other attributes is ensured by combining the algorithms of proxy re-encryption with a multi sharing mechanism and throwing into the mix, an attribute based authentication technique. The multi - dimensional privacy of user data, user identities along with other attributes by using a pre-authentication mechanism and various cipher attacks are prevented by the use of proxy re-encryption technique. The use of above techniques gives the proposed system an upper hand over the pre-existing systems and being a doctor as well as patient centric system the user can use it according to their needs.

References

[1] K. R. M. Li, S. Yu and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings", Security and Privacy in Communication Networks, International ICST Conference, SECURECOMM, pp. 89–106, 2010.

[2] E. H. J. Benaloh, M. Chase and K. Lauter, "Patient controlled encryption: Ensuring privacy of electronic medical records" ACM Cloud Computing Security Workshop, pp. 103–114, 2009.

[3] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks" IEEE Transaction on Parallel and Distributed Systems, vol. 25, no. 1, pp. 22–32, Jan 2014.

[4] M.Green and G.Ateniese, "Identity-based proxy re-encryption" Applied Cryptography and Network Security, vol. 4521, pp. 288–306, 2007.

[5] W. S. K. Liang and J. Liu, "Privacy-preserving ciphertext multi-sharing control for big data storage" IEEE Transaction on Information Forensics and Security, vol. 10, no. 8, Aug 2015.

[6] K. B. G. Ateniese and S. Hohenberger, "Key-private proxy re-encryption"Topics in Cryptology- CT- RSA (Lecture Notes in Computer Science), vol. 5473, pp. 279–294, 2009.

[7] S.H.R. Canetti and J.Katz, "Chosen-ciphertext security from identity-based encryption" Advances in Cryptology-EUROCRYPT, pp. 207–222, 2004.

[8] S.V.Manikanthan and T.Padmapriya "Recent Trends In M2m Communications In 4g Networks And Evolution Towards 5g",

International Journal of Pure and Applied Mathematics, ISSN NO:1314-3395, Vol-115, Issue -8, Sep 2017.

[9] T. Padmapriya and V. Saminadan, "Priority based fair resource allocation and Admission Control Technique for Multi-user Multi-class downlink Traffic in LTE-Advanced Networks", International Journal of Advanced Research, vol.5, no.1, pp.1633-1641, January 2017.