2019 International Conference on Math and Engineering (ICME 2019)

Review of Research on Proxy Re-encryption Based on Identity

Pingshu Wang

School of Mathematics, Qinghai University for Nationalities, Xining, China,810007

Keywords: Re-encryption; Secret key; Identity; Research

Abstract: The development of cryptography and informatics has laid the foundation for the development of modern network technology. Up to now, the field of information security has been the focus of current research. Among them, the proxy re-encryption system has always been a hot spot of research in related fields. It transforms ciphertext through a kind of semi-trusted agent as the intermediary, and in the process of ciphertext transformation, the agent needs to re-encrypt the secret key and does not obtain the relevant plaintext information. At present, due to the increasing attacks on secret keys, strengthening the security of secret keys isolation has become the focus of researchers. Therefore, this paper studies the identity-based proxy heavy encryption and related applications and has obtained some research results.

The field of information security has increasingly become the focus of current research, among which the agent heavy encryption system is one of the research hot spots. In the traditional proxy re-encryption, the agent can apply the secret key to transform the ciphertext information, which also increases the possibility of information disclosure. How to deal with this challenge has become the focus of current research. Therefore, research on identity-based proxy re-encryption has become a new direction of research. The identity-based proxy re-encryption scheme is an important extension of the traditional PRE scheme, which reduces the management of public key certificates and is more suitable for practical applications. However, the IB - PRE scheme cannot take into account multiple advantages, since the security and multiple functions cannot be realized perfectly.

1. Research Background

1.1 Overseas and Domestic Research

Cloud computing services based on the Internet platform have multiple advantages such as simple operation, convenient use, low cost and so on, thus presenting a huge development trend at present. At the same time, cloud computing service is a new and efficient computing method. By transferring the responsibilities of data analysis, storage and calculation on the user's local device to the cloud server, as shown in figure 1, it greatly reduces the computing burden on the local device. This way is very close to the user's own needs and thus widely welcomed by the market.

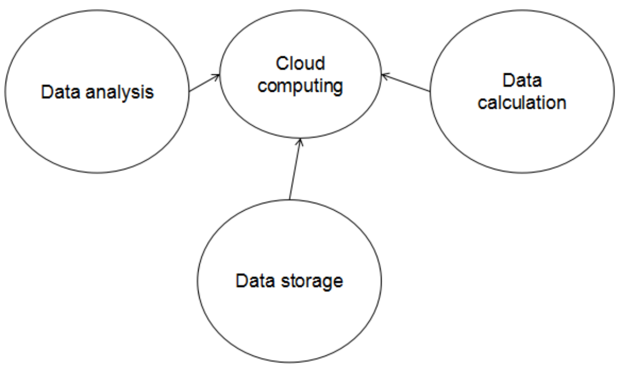

Figure 1 Cloud computing

  DOI: 10.25236/icme.2019.113

However, cloud computing services also have some security risks. On the one hand, most cloud service providers are not completely trustworthy and they are likely to leak users' privacy and important documents due to interests. Such incidents have become commonplace in recent years. Fundamentally, such events are unlikely to go away thoroughly. The direct solution to this problem is data encryption, but the traditional data encryption has been unable to meet the needs of Internet users. Therefore, how to solve this kind of problems has become the current research focus.

The proxy re-encryption scheme was proposed in 1997 and developed into a formal definition in 1998. However, the development of proxy re-encryption technology fell into a state of stagnation. Until 2007, Green and others proposed an IB -- PRE scheme, which was also the focus of this paper. From 2011 to 2019, the IB - PRE scheme has been continuously expanded. From the single secure IB - PRE scheme to the revocable identity based on broadcast re-encryption scheme, the IB - PRE scheme has been greatly expanded, making it more practical. The development of these schemes is mainly used in cloud computing to promote the improvement of security performance of cloud computing.

1.2 Concept of identity-based proxy re-encryption and associated properties

The proxy re-encryption scheme mainly transforms ciphertext through a semi-trusted agent as the intermediary, and in the process of ciphertext transformation, the agent needs to re-encrypt the secret key and does not obtain the relevant plaintext information. Identity-based agent re-encryption is mainly based on the conversion of ciphertext between user A and user B whose key is based on different identities.

Moreover, the important attributes of identity-based agent heavy encryption are unidirectivity, anti-complicity aggression, multi-hop and secret agent. Due to the limitation of space, this paper only analyzes these important attributes. Unidirectivity is one of the most critical attributes in the IB -- PRE scheme. In short, it means that the secret keys held by the agent can only be converted into ciphertext in one direction, that is, they can only be converted from user A to user B. In terms of its scheme design, it is more difficult to realize than the two-way secret keys design scheme, as shown in figure 2.

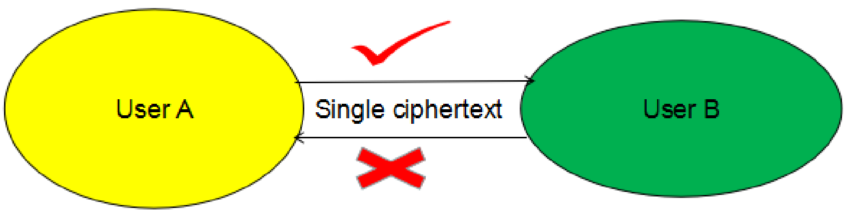

Figure 2 Unidirectivity of ciphertext

Anti-conspiracy aggression mainly means that the authorized person and the agent cannot conspire to get the key, reducing the possibility of information disclosure. Multihop mainly means that the ciphertext in the case of different transformation key transformation of the plaintext remains unchanged. The secret agent attribute mainly refers to the fact that the enemy cannot obtain the information of the conversion key from the agent during ciphertext conversion to reduce the possibility of information disclosure.

2. Application of proxy re-encryption scheme based on identity

2.1 Applications in the Internet of things

The third wave of development of the information industry mainly refers to the Internet of things, which can realize information exchange between devices. Without the help of human participation, thus more convenience is provided for human daily life. In the Internet of things, due to a large number of information exchanges between devices, part of the relevant information is relatively large, so the encryption of transmission information is particularly important. Therefore, IB -- PRE scheme is also applied in the Internet of things, which ensures information security and reduces the technology application scenarios caused by the risk of information leakage. For example, in handling business requests, IB - PRE reduces the risk of information leakage and controls the flow of information in one system.

2.2 Applications in cloud storage

The application of identity-based proxy re-encryption scheme has another kind of important application scenarios that are mainly used in the field of cloud storage. The application of identity-based proxy re-encryption scheme in the field of cloud storage has been mentioned above, and this paper will elaborate on it. As the servers of cloud services are often managed by untrusted third parties, they are faced with a high risk of information leakage, which is also a major problem that troubles the development of cloud storage field. The IB - PRE scheme is to reduce the possibility of information leakage risk in the overall application of cloud storage. For example, in the uploading of sensitive data, since the information has been encrypted by this scheme, the data conversion of encrypted data is unidirectional, leading to the less and less information leakage.

Conclusion

At the present stage, traditional PRE schemes have developed a variety of different schemes due to their own defects, among which IB -- PRE scheme is one of the most important ones. According to studies by scholars in related fields, IB -- PRE scheme is more suitable for the current development. Since the IB - PRE scheme cannot give consideration to the realization of efficiency and multiple functions, the research on this content has also become a research hot spot. Re-encryption based on the identity of the proxy is paid great attention by researchers due to its key attribute. In particular, the unidirectional feature conforms more to the development of modern cloud storage while the feature of conspiracy achieved by reducing the communication between the agent and the authorizer to avoid getting the key can effectively reduce the related information.

Acknowledgement

Project: Uncertainty method for decision analysis, item number:2028-ZJ-911.

References

[1] Huang Xiao. Research and application of group agent heavy encryption in cloud storage environment [D].

[2] Zhao Xuexia, Zhao Jingjing. Reencryption scheme based on certificate agent [J]. Information Technology, 2015(04):156-160.

[3] Lan Caihui, Wang Caifen, Qu Yili. Identity - based one - way multi - purpose proxy heavy encryption scheme [J]. Application Research Of Computers, 2014(08):243-246+250.

[4] Lou Shengming, Cao Fuzhen. An identity-based proxy re-encryption scheme for threshold multi-agents [J]. Journal of natural science of Heilongjiang University, 2010(02):15-20.

[5] Jiang Mingming, Guo Yuyan, et al. Effective reencryption of identity-based agents on the standard model grid [J]. Journal of Electronics Information Technology, 2019, 41(01):66-71.