Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 04, pp.68465-68467, April, 2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

SENSITIVE DATA PROTECTION ON BIG DATA USING ENCRYPTION ALGORITHM

***[1]Vimala Roselin, J. and [2]Dr. G. M. Nasira**

[1]Research scholar, Bharathiyar University,Coimbatore-641046
[2]Assistant Professor, Dept. of Computer Application, Chikkanna Government Arts College, Tirupur – 641602

ARTICLE INFO

Article History:
Received 19th January, 2018
Received in revised form
07th February, 2018
Accepted 29th March, 2018
Published online 30th April, 2018

Key words:
Sensitive data,
Secure sharing,
Big data,
Identity-based conditional
Proxy re-encryption.

ABSTRACT

Big data concern extremely large volume and complex data both structured and unstructured to reveal patterns and trends. The organisation procure large data storage, data delivery on semi-trusted big data sharing platform. An enterprise can obtain huge amount of sensitive data by storing, analysing, processing these data. In digital world, keeping sensitive data secure from theft and vulnerability is very difficult .This abstract proposes a framework for secure sensitive data sharing on a big data platform using effective encryption algorithm. We present an identity based conditional proxy encryption based on heterogeneous cipher text transformation. It protects security of user's sensitive data on big data platform.

Citation: Vimala Roselin, J. and Dr. G. M. Nasira, 2018. "Secure sensitive data sharing on big data platform", *International Journal of Current Research*, 10, (04), 68465-68467.

INTRODUCTION

Big data is colossal sets are voluminous complex that it is difficult to process using on-hand database system tools or traditional data processing application. User's stores huge amount of sensitive data on a platform. Sharing sensitive data is used to reduce the cost providing users with personalized services and non-core services. However, the secure sensitive data sharing is complicated. We use identity-based conditional proxy encryption (IBCPRE) to re-encrypt a cipher text but ciper text will be correctively for decryption, if a condition applied and re-encryption is satisfied. It provides fine-grained proxy re-encryption and useful for secure sharing on big data platform.

Literature study

IBCPRE algorithm (identity-based conditional proxy encryption)

- AES algorithm (Advanced Encrypt Standard)
- AES is more secure (it is less susceptible to cryptanalysis than 3DES).
- AES is faster in both hardware and software.

Corresponding author:* **Vimala Roselin, J.,
Research scholar, Bharathiyar University,Coimbatore-641046.

Cloud storage provides services to keep the data available and accessible, and the physical environment has to be preserving and running .Cloud storage keeps encrypted data .This types of data are not recommended for calculation. So, a big data platform provides services to transfer of sensitive data. It provides huge data storage, value added and computational services. These services can be provided high-level computational intelligence based on emerging analytical techniques.

Primary Safety aspects in secure sensitive data sharing

The Secure sensitive data sharing contains well-being factors. There are insecure Web Interface can be allowed an attacker to utilize an administration web interface. Insufficient Authentication can allow an attacker to use a bad password policy. Insecure Network Services leads to exploit unnecessary or weak services running on the device, There are issues involves in Poor Physical Security which can use USB ports, SD cards or other storage access the device OS and potentially any data stored on the device. Traditional security services are inadequate to share the secured sensitive data. Some security problem while transmitting sensitive data from a data owner's local server to a big data platform. Computational Storage security problems on the big data platform and secure data destruction. Existing technologies are not providing the adequate solution for secure sensitive data sharing.

To protect the sensitive data on the big data platform using Identity Based conditional Proxy Re-Encryption (IBCPRE) technology, and to secure the sensitive data sharing using Virtual Machine Monitor (VMM).

Efficient Framework for Secure Sensitive Data Sharing on a Big Data Platform

A systematic framework for secure sensitive data sharing on a big data platform is shown in Fig. 1

For multiple friends to share the encrypted messages with, Alice simply needs to generate identity based conditional proxy re-encryption key for each of her friends and sends all the re-encryption keys to the server for carrying out the re-encryption. The number of re-encryption keys that Alice needs to generate depends on the number of friends that Alice wants to share the encrypted messages with. It does not depend on the number of encrypted messages. One re-encryption key will allow the Server to convert all the encrypted messages provided the tag of the encrypted messages and the tag of the re-encryption key matches.

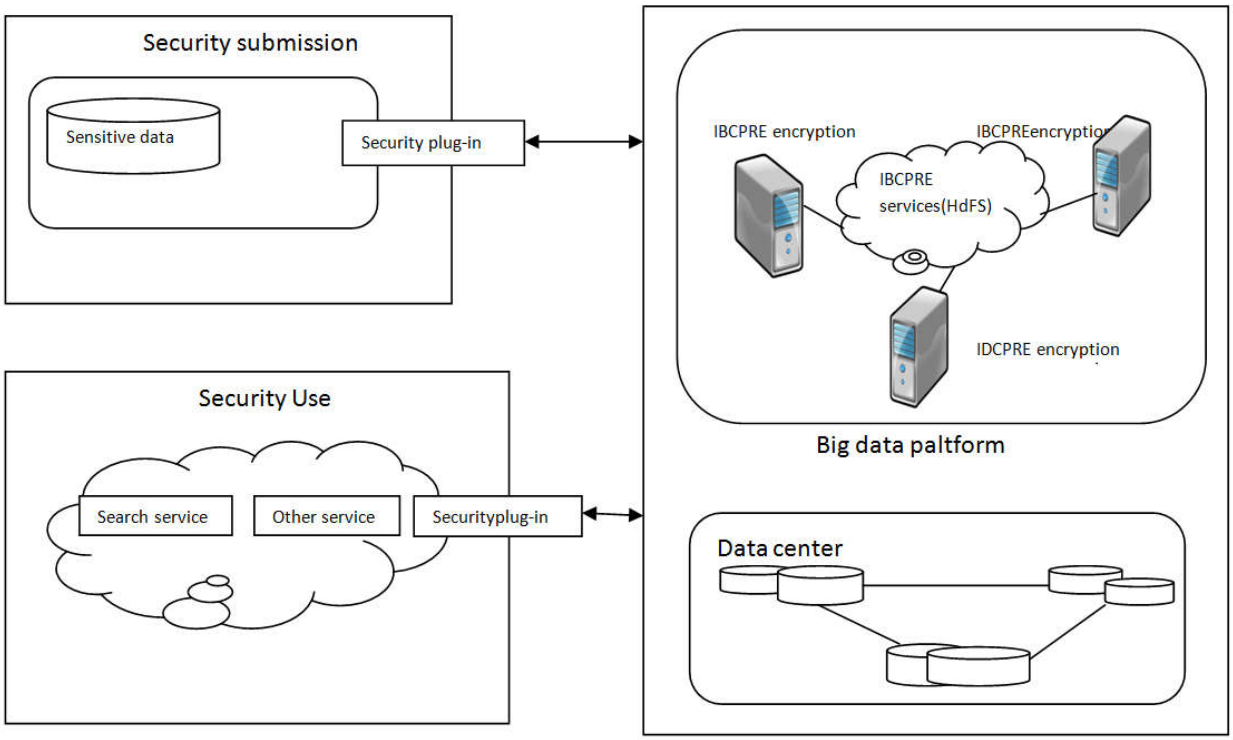

Fig.1. Efficient Framework for Secure Sensitive Data Sharing on a Big Data Platform

We have designed Identity-based conditional proxy encryption (IBCPRE) for secure sensitive. An IBCPRE scheme is an extension of proxy re-encryption on two aspects. The first aspect is to extend the proxy re-encryption to the identity-based public key cryptographic setting. The second aspect is to extend the feature set of proxy re-encryption to support conditional proxy re-encryption. Using conditional proxy re-encryption, a proxy can use an IBCPRE scheme to re-encrypt a cipher text but the cipher text would be well-formed for decryption if a condition applied onto the cipher text together with the re-encryption key is satisfied. This allows proxy fine-grained encryption and can be useful for applications such as secure sharing over encrypted cloud data storage. IBCPRE is very useful in encrypted email forwarding. One of the key features of IBCPRE is that when Alice as a data owner encrypts messages, the encryption is done for her and only Alice herself can decrypt the encrypted messages using her secret key. There is no need for Alice to know in advance about who that she would like to share the encrypted messages with. In other words, picking the friends to share with by Alice can be done after she encrypts the messages and uploads to the Server. Another feature of IBCPRE is that it supports end-to-end encryption. The server which stores the encrypted messages cannot decrypt the messages both before and after the re-encryption. IBCPRE supports one-to-many encryption. The data owner Alice can choose multiple friends to share her data with.

The basic flow of the framework is as follows. First, sensitive information to be pre-set those service providers that need to share this sensitive information store the corresponding encrypted data on a big data platform. Second, we should perform the required operation with the submitted data using IBCPRE on the big data platform. Then, cloud platform service providers who want to share the sensitive information download and decrypt the corresponding data in the private.

Conclusion

We are using RSA algorithm (SHA-2 algorithm, MD-5 algorithm) and IBCPRE algorithm because they provide the elimination of public key certificates to enhance the usability of the target security application. It provides fast performance on server side. These algorithms widely used for secure data transmission.

Our system has following advantages:

- It improves efficiency of encryption.
- Reducing the overhead of the interaction among involved parties.
- Upload the encrypted data to a big data platform.
- Use for secure data transmission.
- It has Fast performance.

REFERENCES

Ananthi, S., Sendil, M.S. and Karthik, S. 2011. Privacy preserving keyword search over encrypted cloud data, in Proc. 1st Advances in Computing and Communications, Kochi, India, pp. 480–487.

Azab, A. M., Ning, P., Wang, Z., Jiang, X., Zhang, X. and Skalsky, N. C. 2010. Hyper Sentry: Enabling stealthy in-context measurement of hypervisor integrity, in Proc. 17th *ACM Conference on Computer and Communications Security,* Chicago, USA, pp. 38–49.

Hanaoka, G., Kawai, Y., Kunihiro, N., Matsuda, T., Weng, J. Zhang, R., Zhao, Y. 2012. Generic construction of chosen cipher text secure proxy re-encryption. CT- RSA. LNCS, vol. 7178: Springer. pp. 349–364.

Hanaoka, G., Y. Kawai, N. Kunihiro, T. Matsuda, J. Weng, R. Zhang, Y. Zhao, 2012. Generic construction of chosen cipher text secure proxy re-encryption. CT- RSA. LNCS, vol. 7178: Springer. pp. 349–364.

Liang, K. Liu, Z. Tan, X. Wong, D. S., Tang, C. 2012. A CCA-secure identity-based conditional proxy re-encryption without random oracles. The 15th International Conference on Information Security and Cryptology (ICISC 2012), LNCS 7839: Springer. pp. 231–246.

Libert, B., D. Vergnaud, 2011. Unidirectional chosen-cipher text secures proxy re-encryption. IEEE Transactions on Information Theory 57(3): IEEE. pp. 1786–1802.

Lv, Z., Hong, C., Zhang, M. and Feng, D. 2012. A secure and efficient revocation scheme for fine-grained access control in cloud storage, in Proc. 4th IEEE Int. Conf. on Cloud Computing Technology and Science, Taipei, Taiwan, China, pp. 545–550.

Shao, J., Wei, G., Ling, Y., Xie, M. June 2011. Identity-Based Conditional Proxy Re-Encryption. Proceedings of IEEE International Conference on Communications, ICC 2011: IEEE.

Wang, L., Wang, L., Mambo, M. and Okamoto, New identity-based proxy re-encryption schemes to prevent collusion attacks, in Proc. 4th Int. Conf. Pairing-Based Crypto

Wing, J., Deng, R. H., Ding, X. Chu, C. K. Lai, J. 2009. Conditional proxy re-encryption secure against chosen-cipher text attack. ASIACCS: ACM. pp. 322–332.

Xinhua Dong ,Ruixuan Li, Heng He ,Secure sensitive data sharing on big data platform, Huazhong University of Science and Technology, Wuhan 430074,China,2015,PP 72-80.

****