ISSN 2395-1621

A Secure Sensitive Data Sharing On Big-Data Platform

[#1]Ajay Bhosale, [#2]Vinod shinde, [#3]Mayur Wanjale, [#4]Shubham Tharkar, [#5]R.M.Samant

[1]ajaygb1846@gmail.com
[3]vinodshinde500v@gmail.com
[4]mayur7050@gmail.com
[2] tharkar.shubham1994@gmail.com
[5]rahul.samant@sinhgad.edu

[#1234]Department of Information Technology,NBN Sinhgad School Of Engineering,Pune,India-411041

[#5]Professor,Department of Information Technology,NBN Sinhgad School Of Engineering, Pune,India 411041

ABSTRACT

With the massive development of information digitization, massive amounts of data are generated quickly. By collecting, sorting, analyzing, and mining this data. Anyone can obtain large amounts of individual users' sensitive data. The major problem of user is security of data warehouse on cloud. For fraudulent purpose Consumers cannot always just depend on the cloud provider's security infrastructure. We have developed a web-based application for secure sensitive data sharing on a big data environment, including secure data delivery, storage, usage, and demolition on a semi-trusted big data sharing platform. The application protects the security of users' sensitive data effectively and shares the data safely. The major security challenge with clouds is that of the data may not have control of where data is placed. This is because if one wants to exploits the benefits of using cloud, one must also utilize the resource allocation and scheduling provided by clouds. Secure sensitive data as a Service cloud platform provides security of the infrastructure level for a public cloud by providing security to cloud that is highly elastic, portable and fully Controlled by the cloud consumer.

ARTICLE INFO

Article History

Received :15th April 2016

Received in revised form :

17th April 2016

Accepted : 19th April 2016

Published online :

23rd April 2016

***Keyword*:** secure sharing; sensitive data; big data; proxy re-encryption; private space.

I. INTRODUCTION

Users store huge amounts of sensitive data on a big data platform. Sharing sensitive data will help enterprises minimal the cost of providing users with individual services and gives value-added data services. However, secure data sharing is difficult. This paper proposes a framework for secure sensitive data sharing on a big data environment, including secure data delivery, storage, utilization, and destruction on a semi-trusted big data sharing environment.

We present a proxy re-encryption algorithm based on diverse cipher text transformation and a user process protection method based on a virtual machine monitor, which provides help for the realization of system functions. The framework protects the security of users' sensitive data implicitly and shares these data safely. At the same time, data owners retain complete control of their own data in a sound territory for modern Internet information security

Materials and Method

- ➢ Technologies Used:

During the solution development, following hard-wares were used:

- 250 GB HD
- 4GB RAM
- Cloud Environment

- ▪ Software Requirement:
  - JAVA
  - Hadoop Framework
  - MySql
  - HTML5

- Bootstrap
- Ajax

Stepwise flow of Methodology:

in these system, we are taking different data as input(structured ,semi0structured, unstructured data). We are using algorithm for security for cloud environment RSA algorithm (SHA-1 algorithm, MD-5 algorithm), H-PRE algorithm to make data secure.
We are using RSA algorithm (SHA-1 algorithm, MD-5 algorithm), H-PRE algorithm because they provide simple and fast performance on server side. These algorithms widely used for secure data transmission.

Our system has following advantages:
1. It improves efficiency of encryption.
2. Reducing the overhead of the interaction among involved parties.
3. Upload the encrypted data to a big data platform.
4. Use for secure data transmission.
5. It has Fast performance.

- The interaction as well as the communication of the user with the application can be shown with the help of following diagram :

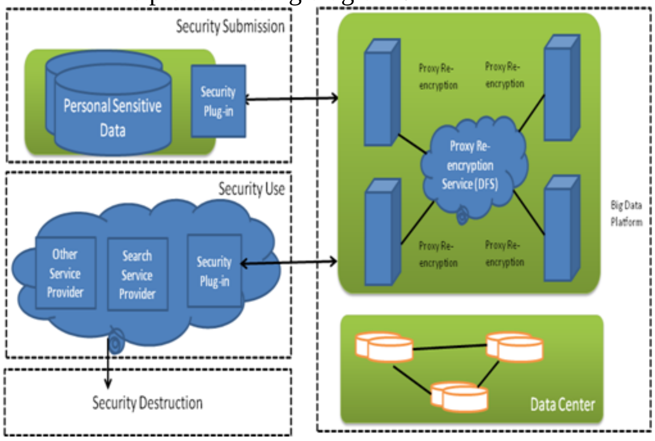

Fig.1 Systematic framework for secure sensitive data sharing on a big data platform

II. MATHEMATICAL MODEL

Set theory analysis:
(a)Let ‘S’ be the | question paper set as the final set

S = {…………
(b) Identify the inputs as D , Q, I, P
S = {d, q, i, p, …
D = {d1, d2, d3,d4, … | ‘d’ given cloud storage}
Q= {Q1,Q2, Q3, … | ‘Q’ gives the request by user to secure the data}
I = {I1, I2, … |’I’ gives user ID for login}
P= {P1, P2, … |’P’ gives the respective password for login ID}

Set theory analysis:
(a)Let ‘S’ be the | question paper set as the final set

S = {…………
(b) Identify the inputs as D , Q, I, P
S = {d, q, i, p, …
D = {d1, d2, d3,d4, … | ‘d’ given cloud storage}
Q= {Q1,Q2, Q3, … | ‘Q’ gives the request by user to secure the data}
I = {I1, I2, … |’I’ gives user ID for login}
P= {P1, P2, … |’P’ gives the respective password for login ID}

(c)Identify the outputs as O
S = {d, q, i, p, n, r, …
N = {n1, n2, n3, n4, … | ‘n’ data is secure in cloud environment}
R= {R1, R2 … | ‘R’ is the response for secure data}
(d)Identify the functions as ‘F’
S = {d, q, i, p, n, r, f…
F = {f1(), f2(), f3(), f4(), f5()}
F1(v) :: access the cloud storage
F2 (V) :: process requests
F3 (V) :: secure the data
F4 (T) :: response to data
F5(D) :: login

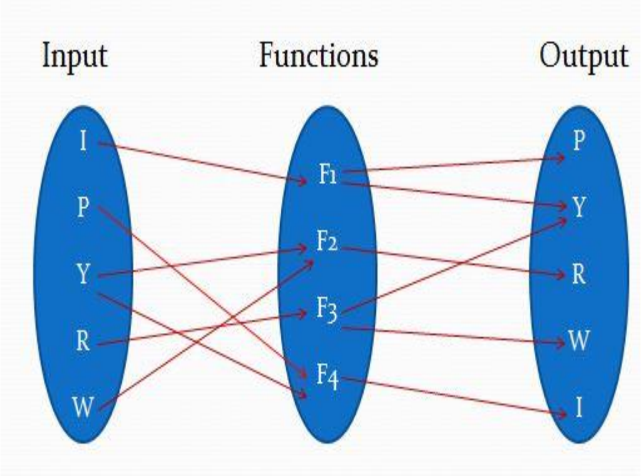

Fig.2: Function Representation in set

III.RESULT/DISCUSSION

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

IV.CONCLUSION

The proposed project well protects the security of users’ sensitive data. At the same time the data owners have the entire control of their own data, which is a feasible solution to balance the benefits of involved parties under the semi-trusted conditions.

REFERENCES

1)S. Yu, C. Wang, K. Ren, and W. Lou, Attribute based data sharing with assigned attribute revocation, in Proc. 5th ACM Symposium on Information, Computer andCommunications Security, Beijing, China, 2010, pp. 261– 270

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

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

4) L. Dong, Y. Zhuang, Y. Gao, and Y. Bu, Research on realtime trigger system for sensitive data safe destruction, (in Chinese), Journal of Chinese Computer System, vol. 31, no. 7, pp. 1323–1327, 2010.

5) S. Razick, R. Mocnik, L. F. Thomas, E. Ryeng, F. Drabløs,and P. Sætrom, The eGenVar data management system —Cataloguing and sharing sensitive data and metadata for thelife sciences, Database, vol. 2014, p. bau027, 2014.

6) A. M. Azab, P. Ning, E. C. Sezer, and X. Zhang,HIMA: A hypervisor-based integrity measurement agent, in Proc. 25th Annual Computer Security Applications Conf., Hawaii, USA, 2009, pp. 461–470.

7) Z. Lv, C. Hong, M. Zhang, and D. Feng, A secureand 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, 2012, pp. 545–550.

8) J. Yang and K. G. Shin, Using hypervisor to providedata secrecy for user applications on a per-page basis, in Proc. 4th Int. Conf. on Virtual Execution Environments, Seattle, USA, 2008, pp. 71–80.

9) H. Chen, F. Zhang, C. Chen, Z. Yang, R. Chen, B. Zang, W. Mao, H. Chen, F. Zhang, C. Chen, et al., Tamperresistant execution in an untrusted operating system using a virtual machine monitor, Technical Report, Parallel Processing Institute, Fudan University, FDUPPITR-2007-0801, 2007.

10) P. Dewan, D. Durham, H. Khosravi, M. Long, and G. Nagabhushan, A hypervisor-based system for protecting software runtime memory and persistent storage, in Proc. the 2008 Spring Simulation Multiconference, Ottawa, Canada, 2008, pp. 828–835.

11) G. Wang, F. Yue, and Q. Liu, A secure self-destructing scheme for electronic data, Journal of Computer and System Sciences, vol. 79, no. 2, pp. 279–290, 2013.

12) L. Zeng, Z. Shi, S. Xu, and D. Feng, Safevanish: An improved data self-destruction for protecting data privacy, in Proc. 2nd Cloud Computing International Conf., Indianapolis, USA, 2010, pp. 521–528.

13) L. Dong, Y. Zhuang, Y. Gao, and Y. Bu, Research on realtime trigger system for sensitive data safe destruction, (in Chinese), Journal of Chinese Computer System, vol. 31, no. 7, pp. 1323–1327, 2010.

14) J. Qin, Q. Deng, and J. Zhang, Design of multi-grade safety data destruction mechanism of HDFS, (in Chinese), Computer Technology and Development, vol. 23, no. 3, pp. 129–133, 2013.

15) F. Zhang, J. Chen, H. Chen, and B. Zang, Lifetime privacy and self-destruction of data in the cloud, (in Chinese), Journal of Computer Research and Development, vol. 48, no. 7, pp. 1155–1167, 2011.

16) S. Razick, R. Mocnik, L. F. Thomas, E. Ryeng, F. Drabløs, and P. Sætrom, The eGenVar data management system — Cataloguing and sharing sensitive data and metadata for the life sciences, Database, vol. 2014, p. bau027, 2014.