IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Efficient Security Framework for Sensitive Data sharing On Big Data Platform in Cloud Computing

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

[1] Research Scholar (Computer Science), Bharthiar University, Coimbatore
[2]Department of Computer Applications, Chikkanna Government Arts College, Tirupur

[*]*Corresponding Author: nasiragm99@yahoo.com , Tel.: 8838745870*

DOI: https://doi.org/10.26438/ijcse/v7i5.277280 | Available online at: www.ijcseonline.org

Accepted: 13/May/2019, Published: 31/May/2019

Abstract— Big data contains enormous number of semi structured and unstructured data. It is hard to process these data utilizing traditional databases and programming technologies. The association acquire substantial data storage data delivery on big data sharing platform. It expands the use. An organisation and enterprise can acquire huge amount of sensitive data by putting away, breaking down, handling these information. They utilized logging, vulnerability and encryption to keep sensitive data secure in advanced world. It offers some benefit included data administrations. Clients are looking at encryption, tokenization advancements to secure the information. The major objective of the work is to examine security issues comprising the entire sensitive data sharing and clarify a security mode created to guarantee secure sensitive data sharing on a big data platform. It also assures secure capacity on the big data platform. This abstract presents a framework to share the secure sensitive data on a big data platform using Identity based ConditionaI Proxy Re-encryption (IBCPRE) algorithm. It is based on heterogeneous cipher text transformation technique to gives the end-to-end security of big data in the cloud It provides the security when sharing the sensitive data.

Keywords— Secure Data, Sensitive, and Identity Based Conditional Proxy Re-Encryption (IBCPRE), Encryption.

I. INTRODUCTION

Massive amounts of structured, semi-structured, and unstructured data are generated quickly in the fast development. An enterprise can get the huge amount of individual user's sensitive data by storing and collecting data from different types of data. These data provide services to their enterprises and other businesses on a big data platform. Traditional cloud storage stores plain text or encrypted data. These types of data are considered as "dead", because they are not active and also they are not involving in calculation. However, a big data platform allows data transmission a including sensitive data. It provides huge number of data storage and computational services in the organisation [1]. However, data sharing increases enterprise assets, insecurity and sensitive data leakage also produce the security issues for sharing the sensitive data.

In this work, a proposed productive structure for secure sharing of sensitive data is possible [3]. This work guarantees safe submission and limits sensitive data dependent based on the proxy re-encryption algorithm. It also guarantees secure utilization of evident data in the cloud organized by the private space of customer process which is subject to the Virtual Machine Monitor (VMM) besides identity-based conditional proxy encryption (IBCPRE).

Data sharing can be done in a secured way over huge data frameworks including functionalities, information security, data access, and secure data destruction using various cloud services also. This work is implemented using Java, Hadoop, and Html5.

II. PRELIMINARY SAFETY ASPECTS IN SECURE SENSITIVE DATA SHARING

Secure sensitive data sharing contains four primary safety issues. First, issues will occur when sensitive data are transmitted from a local server to a big data platform. Second, there can be sensitive data computational problem and storage problems on the big data platform[5]. Third, there are the big secure sensitive data issues on the cloud. Fourth, secure data destruction issue. Research institutions and scholars have contributed to exploration and research aimed at solving these type security problems.

III. ENCRYPTION AND ACCESS CONTROL

According to the encryption technology, the Attribute-Based Encryption (ABE) algorithm contains Key-Policy ABE (KP-ABE) and Cipher text-Policy ABE (CPABE). ABE decryption is used to avoid the costs of frequent key distribution in cipher text access control[7]. When the access control strategy changed a data owner is required to re-encrypt the data. A data agent with a proxy key can re-encrypt cipher text; the agent cannot get the corresponding plaintext or compute the decryption key. A Fully Homomorphic Encryption (FHE) mechanism is proposed and provides a specific algebraic operation based on cipher text that is not given the l encrypted result. The encrypted data provides the correct results, but the data are not decrypted throughout the entire system. The FHE scheme requires additional computation.

Existing methods have partly resolved information sharing and privacy protection issues from several perspectives; however they have not measured the complete method in the complete information security life cycle. On the other hand, a big data platform is a complete system by means of multi-stakeholder involvement, and consequently shouldn't accept any safety violation resulting in sensitive information loss.

Usual securities services are not enough towards distribute the secured sensitive data. A number of the security issue occurs by means of transmitting the sensitive information from a data owner's local server to a big data technology. A computational Storage security issue on the big data technology and secure information destruction develop into one of the most significant problems.

The existing algorithm is not always easy to implement .so we provides Identity-based conditional proxy re-encryption (IBCPRE) to solve the issues.

IV. IDBCPRE (Identity Based Conditional Proxy Re-Encryption)

IDBCPRE includes three sorts of algorithm, traditional based encryption (counting SetupIBE, KeyGenIBE, EncIBE, and DecIBE), re-encryption (counting KeyGenRE, ReEnc, and ReDec capacities); what's more, the last one is the tradition public key cryptosystems (counting KeyGenPKE, EncPKE, and DecPKE). The data owner encrypts sensitive data utilizing a nearby security module and after that transfers the encrypted data to a big data platform. The data are changed into the ciphertext that can be decrypted by a predetermined user after PRE administrations. In the event that a SESP is the predefined client, at that point the SESP can unscramble the information utilizing its own private key to acquire the comparing clear content. We complete the following steps to execute the H-PRE calculation.

(1) SetupIBE.k/: Input security parameters k, create haphazardly an essential security parameter Mk, and compute the framework parameter set params utilizing a bilinear guide and hash work.

(2) KeyGenIBE.mk, params, id/: When the client demands the private key from the key age focus, the key age focus gets the legitimate personality (id) of the client and produces the general population and private keys (pkid, slip) for the client utilizing params and mk.

(3) KeyGenPKE.params/: When a client presents a demand, the key administration focus not just creates the personality based open and private keys, yet in addition creates general society and private keys of the conventional open key framework (pk' id, sk' id).

(4) EncIBE.pkid; skid; params; m/: When the client encodes information, the information proprietor scrambles the reasonable content (m) into the ciphertext (c D .c1; c2/) utilizing the client's own (pkid, slip) and an irregular number (r 2 RZ p).

(5) KeyGenRE.skidi ;sk'idi ; pk'idj ; params/: When the information proprietor (client I) stipends client j authorizations, utilizing skidi , sk0 idi , and pk'idj , client I figures the PRE key (rkidiidj), finishing the change from client I to client j . (6) ReEnc.ci; rkidiidj; params/: is procedure is executed straightforwardly on the enormous information stage. The work re-scrambles the ciphertext that client I encoded into cipher text that client j can unscramble. It inputs ci.ci D .ci1; ci2//, the PRE key (rkidiidj), and related framework parameters, and afterward the huge information stage figures furthermore, yields the PRE cipher text (cj D .cj1; cj 2/). (7) DecPKE.cj; sk' idj; params/: This is a capacity for decoding the PRE ciphertext. In the wake of getting the PRE cipher text (cj D .cj1; cj 2/) from the intermediary server of the huge information stage, client j decides the reasonable content (m'D m) of the information utilizing his or her very own SK' idj.

V. RESULTS AND DISCUSSION ON SECURE SENSITIVE DATA ON VMM

To ensure secure running of an application in the cloud, we use the private space of a customer method in perspective on a VMM. We acknowledge that some undertaking (for instance, a SESP) rents Infrastructure as a Service (IaaS) to complete some business. The business strategy necessities to remove tricky individual data on the colossal data organize. We consider the guaranteed program that isolates delicate information from the enormous information stage a touchy procedure. A danger model of a delicate model on a cloud organize is showed up in Fig. 3. A sensitive technique must keep risks from an organization VMM and a dishonest working structure layer underneath it. Lease base equipment uses the TPM mode, ensuring that the VMM is trusted. For this circumstance, the key organization segment of the

occupant, (for instance, a SESP) must shape this relationship subject to trusting in a VMM, ensuring safe errand under the dangerous working system.

The introduction of virtualization and believed figuring advancement ensures that master association applications and a protected module continue running at thesame time private space[13]. This mode can guarantee the security of delicate information and avoid impedance from outside programs, even the working structure.

With PRE cipher text decided on a major information stage separated onto a cloud arrange, private memory space of systems on the cloud stage can guarantee data security in memory and on the Hard Disk Drive (HDD). To begin with, the VMM gives private memory space for demonstrating a VM system[9]. The strategy Continues running in private memory space whose memory can't be gotten to by the working structure or distinctive applications. The strategy of memory detachment ensures data insurance and security in the memory. In addition, the data used and set away on circle is cipher text. The VMM decodes or encodes when perusing or composing independently. Thusly, a mix of these two measures can be guaranteed using the VMM, paying little mind to whether the customer program continues running in memory or is secured on circle.

To assure secure running of an application in the cloud computing, we use the private space of a user process based on a cloud simulator[11]. The results of the proposed proxy re-encryption and IBCPRE algorithm are measured in terms of security, data encryption time and computation time. The results of the proposed methods and existing methods (self-destructing, and Conditional proxy re-encryption) is shown as follows.

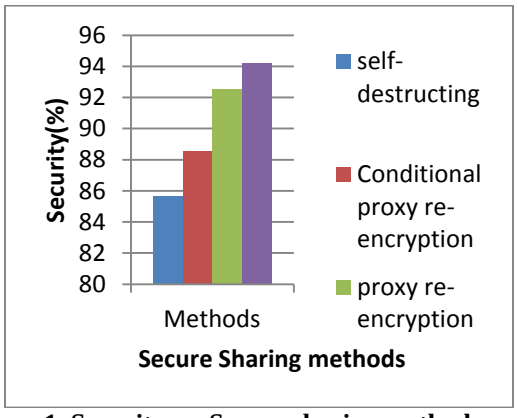

Figure 1. Security vs. Secure sharing methods

Figure 1 shows the performance comparison results of the security level for four different methods such as self-destructing, Conditional proxy re-encryption, proxy re-encryption and IBCPRE methods. From the results it concludes that the proposed IBCPRE produces higher security value of 94.18%, whereas other methods such as self-destructing, Conditional proxy re-encryption, proxy re-encryption produces only 85.63%, 88.52% and 92.52% respectively.

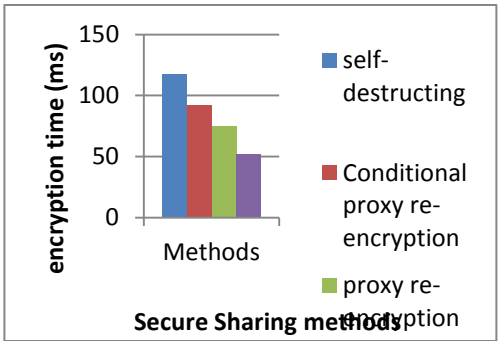

Figure 2. Encryption time vs. secure sharing methods

Figure 2 shows the performance comparison results of the encryption time for four different methods such as self-destructing, Conditional proxy re-encryption, proxy re-encryption and IBCPRE methods. From the results it concludes that the proposed IBCPRE has takes lesser encryption time of 52 ms, whereas other methods such as self-destructing, Conditional proxy re-encryption, proxy re-encryption produces only 118 ms, 92 ms and 75 ms respectively.

VI.CONCLUSION

We proposed an efficient structure of secure sharing of touchy information huge information stage organize, which ensures secure accommodation and limit of sensitive data on the Identity Based Conditional proxy re-encryption algorithm, and guarantees secure usage of clear substance in the cloud arrange by the private space of customer process subject to the VMM. The proposed structure well guarantees the security of customers' sensitive data. Meanwhile the data owner has the complete control of their own data, which possible answer for equality the upsides of included social occasions under the semi-trusted in conditions. Later on, we will upgrade the profitability of encryption. Moreover, decreasing the overhead of the correspondence among included gatherings is likewise an important future work.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute-based encryption, in Proc. IEEE Symposium on Security and Privacy, Oakland, USA, 2007, pp. 321–334.

[2] J. Li, G. Zhao, X. Chen, D. Xie, C. Rong, W. Li, L. Tang, and Y. Tang, Fine-grained data access control systems with user accountability in cloud computing, in Proc. 2nd Int. Conf. on Cloud Computing, Indianapolis, USA, 2010, pp. 89–96.

[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 cryptography-Pairing, Ishikawa, Japan, 2010, pp. 327– 346.

[4] C. Gentry, A fully homographic encryption scheme, PhD dissertation ,Stanford University, California, USA, 2009.

[5] 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.

[6] H. Hu, J. Xu, C. Ren, and B. Choi, Processing private queries over untrusted data cloud through privacy homomorphism, in Proc. 27th IEEE Int. Conf. on Data Engineering, Hannover, Germany, 2011, pp. 601–612.

[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, Privacypreserving multi-keyword ranked search over encrypted cloud data, in Proc. 30th IEEE INFOCOM, Shanghai, China, 2011, pp. 829–837.

[8] C. Hong, M. Zhang, and D. Feng, AB-ACCS: A cryptographic access control scheme for cloud storage, (in Chinese), Journal of Computer Research and Development, vol. 47, no. 1, pp. 259–265, 2010.

[9] N. Zeldovich, S. Boyd-Wickizer, and D. Mazieres, Securing distributed systems with information flow control, in Proc. 5th USENIX Symposium on Networked Systems Design and Implementation, San Francisco, USA, 2008, pp. 293–308.

[9] Z. Lv, C. Hong, M. Zhang, and D. Feng, 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, 2012, pp. 545–550.

[10] 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.

[11] A. M. Azab, P. Ning, Z. Wang, X. Jiang, X. Zhang, and N. C. Skalsky, HyperSentry: Enabling stealthy in-context measurement of hypervisor integrity, in Proc. 17th ACM Conference on Computer and Communications Security, Chicago, USA, 2010, pp. 38–49. [12] Trusted Computing Group, TNC architecture for interoperability, http://www.trustedcomputinggroup.org/ resources/tnc architecture for interoperability specification, 2014.

[13] H. Zhang, L. Chen, and L. Zhang, Research on trusted network connection, (in Chinese), Chinese Journal of Computers, vol. 33, no. 4, pp. 706–717, 2010.

[14] D. Feng, Y. Qin, D. Wang, and X. Chu, Research on trusted computing technology, (in Chinese), Journal of Computer Research and Development, vol. 48, no. 8, pp. 1332–1349, 2011.

[15] F. Zhang, J. Chen, H. Chen, and B. Zang, Cloudvisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization, in Proc. 23rd ACM Symposium on Operating Systems Principles, Cascais, Portugal, 2011, pp. 203–216.

[16] X. Chen, T. Garfinkel, E. C. Lewis, and B. Spasojevic, Overshadow: A virtualization-based approach to retrofitting protection in commodity operating systems, in Proc. 13th Int. Conf. on Architectural Support for Programming Languages and Operating Systems, Seattle, USA, 2008, pp. 2–13. 80 Tsinghua Science and Technology, February 2015, 20(1): 72-80.

.

