Secure Sensitive Data Transmission On Bigdata Platform

[1]J.Vimala Roselin, [2] G.M.Nasira
[1]Research Scholar, Bharathiyar University, Coimbatore-46 Tamilnadu .India.
[2]Head, Department of Computer Applications Chikkanna Government College, Tiruppur-2 Tamilnadu, India

Abstract: Big data is huge volumes of structured and unstructured data that is very difficult to process this data using traditional databases . The organisation contains huge data storage, data delivery on semi-trusted big data platform. It increases the expenditure. An enterprise can acquire enormous amount of sensitive data by storing , analysing , processing these data. Logging, vulnerability and encryption are essential to keep sensitive secure in computerized world. It decreases the costs of enterprises for users to provide value added data and personalized services. It becomes essential to give the security in big data platform. Customers are looking at the field level of encryption, tokenization, and anonymization technologies to secure the information. This conceptual presents a system to share the sensitive data on a big data platform utilizing effective encryption algorithm. We process identity-based conditional proxy encryption (IBCPRE) based on heterogeneous ciper text transformation technique to guarantee the security of big data in cloud. However, the concept updating has always been a challenging problem when (IBCPRE) is used to establish the access control strategy. It also gives security to share the sensitive data.

Key words: Sensitive data, Secure sharing, big data, identity-based conditional proxy re-encryption

1. Introduction

Data generated organisation are expanding use of the data. Big data is generates big volume of data set that it is difficult to process using traditional database system and software trends. Big data contains structured, unstructed, semi structured data. These types of data have sensitive data. The huge amount of sensitive data is stored on a big data platform. Big data platform is not only stores large volume of data but also protect the appropriate policies. Most of the data processing happens on the secured data. Enterprise needs proper authentication and authorisation. Sharing sensitive data provides personalised services and non-core services to the users with minimum cost. We use identity-based conditional proxy encryption (IBCPRE) to re-encrypt a cipher text .Cipher text will decrypted, if a condition is satisfied. It gives the proxy re-encryption and secure the sensitive data on big data platform. When transmitting the sensitive data from local system to big data platform, we need to face security issues, sensitive data computing, security problem while storing the data, data use issues in cloud environment. Existing system provides the partial solution for sharing and securing the sensitive data. I am also includes algorithms to provides end-to-end

security of sensitive data guaranteed secured storage on Big data using Identity Based Conditional Proxy Re-Encryption (IBCPRE) using private space process based on VMM.

Cloud Environment Software Requirement:

JAVA, Spark, HTML5

2. Literature survey

More sensitive data is shared by third party sites on the Internet; we need to encrypt data stored at these sites. The main disadvantage of encrypting data is it can be selectively shared only at a coarse-grained level .The author used new system for sharing the encrypted data that is called Key-Policy Attribute-Based Encryption(KP_ABE).KP-ABE decryption distributes the keys in cipertext access control. When the access control changed, the data owner needs to re-encrypt the data.

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.

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, some services are available to transfer of sensitive data. It provides huge data storage, value added and computational services. These types of services are provided for high-level computational intelligence based on emerging analytical techniques.

3. Preliminary Safety aspects in secure sensitive data sharing

The Secure sensitive data sharing have some security 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 issues happened when the sensitive data is transmitted from a data owner's local server to a big data platform. Existing technologies is not supply the appropriate 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).

4. A systematic structure of sensitive data sharing in a big data platform

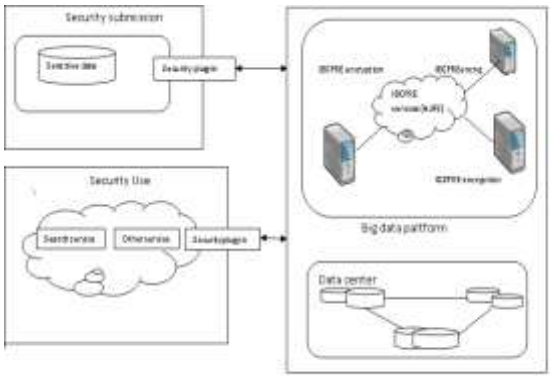

Fig 1.Standardized structure of sensitive data.

We have planned Identity-Based Conditional Proxy Re-Encryption (IBCPRE) for secure sensitive data. An IBCPRE algorithm is an augmentation of proxy re-encryption on two viewpoints. The primary angle is to stretch out the re-encryption to the character based open key cryptographic setting. The second perspective is to expand the list of capabilities of Proxy Re-Encryption to help Conditional Proxy Re-Encryption .Utilizing proxy re-encryption, conditional can utilize an IBCPRE plan to re-encode a figure message however the figure content would be very much shaped for unscrambling if a condition connected onto the figure message together with the reencryption key is fulfilled. For example, secure sharing over encoded cloud information are saved. IBCPRE is exceptionally valuable in encoded email sending. One of the key highlights of IBCPRE is that when Alice as an information proprietor scrambles messages, the encryption is improved the situation her and just Alice herself can decode the encoded messages utilizing her mystery key. There is no requirement for Alice to know ahead of time about whom that she might want to share the scrambled messages with. As it were, picking the companions to impart to by Alice should be possible after she encodes the messages and transfers to the Server. The other component of IBCPRE is that it gives end-to-end encryption. The server which stores the encoded messages can't decode the messages both when the re-encryption. IBCPRE supports one-to-many encryption. The information owner Alice can pick various customers to impart her information to. For many customers to share the encoded messages with, Alice basically needs to produce Identity-Based Conditonal Proxy Re-Encryption eliminates for every one of her partner and sends all the re-encryption keys to the server for completing the re-encryption. The quantity of re-encryption keys that Alice needs to create relies upon the quantity of companions that Alice needs to share the encoded messages with. It doesn't rely upon the quantity of disordered messages. One re-encryption key will enable the Server to change over all the encoded messages gave the tag of the disordered messages and the tag of the re-encryption key matches.

The fundamental concept of the system is as per the following.

In the first place, sensitive data to be pre-set those specialist organizations that need to share this touchy data store the comparing encrypted data on a major information stage. Second, we ought to play out the required activity with the submitted information utilizing IBCPRE on the huge information stage. At that point, cloud stage specialist organizations that need to share the delicate data download and unscramble the relating information in the private. 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, the required operation has to be 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.

Mathematical model:

Set theory analysis:

1. Let 'T' be the set as the final set
2. T = {..... Identify the inputs as C, Q, E, P T= {d, q, i, p, ... D = {d1, d2, d3,d4, ... | 'C' given cloud storage},Q= {Q1,Q2, Q3, ... | 'Q' gives the request by user to secure the data}, E = {E1, E2, ... |'E' gives user EmailID for login} P= {P1, P2, ...| 'P' gives corresponding password for login ID}
3. Identify the outputs as O T = {d, q, i, e, n, r ... N = {n1, n2, n3, n4 ... | 'n' data is secure in cloud environment} R= {R1, R2 ... | 'R' is the response for secure data}
4. 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

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.

References

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

2. G. Hanaoka; Y. Kawai; J. Weng; R. Zhang; Y. Zhao (2012). Generic construction of chosen cipher text secure proxy re-encryption. vol. 7178: Springer. pp. 349–364.

[3] J. Weng; R. H. Deng; X. Ding; C. K. Chu; J. Lai (2009). Conditional proxy re-encryption secure against chosen-cipher text attack. ASIACCS: ACM. pp. 322–332.

[4] K. Liang; Z. Liu; X. Tan; D. S. Wong; C. Tang (2012). A CCA-secure identity-based conditional proxy re-encryption without random oracles. Springer. pp. 231–246.

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