Intelligent Systems and Computer Technology
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC200156

Privacy Preserving and Sensitive Attribute Based Cloud Storage: A Survey

Muthulakshmi K [a], Valarmathi K [b]
[a]Research Scholar, Anna University, Chennai, India
[b]Professor, Dept of CSE, Panimalar Engineering College, Chennai, India

Abstract. Cloud computing is a recent methodology to store and retrieve huge volume of data in a cost effective way. Distributed computing undertakes security to the system as its main role. Recently, the owners of the data need to think about the level of security provided to their information during storage and its movement while performing various tasks. Current security technique offers security to the entire information with encryption/decryption time, cost incurred due to loading while providing less security to the sensitive attributes without the information about the owner of the data. Thus, an exchange off between high security and low capacity cost to the sensitive attributes are identified from the information provided and security techniques are applied to these information. This Survey paper portrays the thought of Searchable encryption (SE) with regards to human services applications and portrays the SE use cases into four situations in health care. The data contains in the medical image are sensitive in this way it is important to shield it from unapproved users. By utilizing different encryption strategy. We can give the security and privacy to the Electronic Health Record.

1. Introduction

Privacy preserving information distribution is the fundamental worry right now, the information being distributed through web has been expanding step by step. This tremendous measure of information was named as Big Data by its size. Huge voluminous measure of information is been created using different sources such as, medical, online business, retail, clinics etc., due to computerized innovations. Humans too add to this by site logs, CCTV etc., large volumes of data is being created every minute due to a web based life. These information gathered from various sources can be handled and broken down to provide leadership though, it may lead to violation of protection.[13]

In the present distributed computing condition, wellbeing cloud saves the individual explicit delicate data for a few purposes, for example, bio-medicinal research, medical coverage organizations, restorative information examination, and so on. At the point when any approved individual gets to these mists, the discharged information ought not bargain any people's security and it stays valuable too. In the wellbeing cloud framework, the information must be discharged in such a way that any people's personality can't be uncovered. The database the executive's framework alone can't guarantee any person's security. The Access Control (AC) models are

1 Muthulakshmi.K, Research Scholar,Anna University, Chennai, India;
E-mail: akmuthube@gmail.com

likewise not ready to shield the information from circuitous access or numerous questions. To expel such issues derivation control is one of the systems which guarantees the information privacy from backhanded information get to. [2].

The sensitive data are encrypted by using Attribute Based Encryption (ABE) technology, searchable encryption with inverted index, outsourcing technology and equality test mechanism.

ABE analyze the security under general group model it combine with block chain to protect malicious attack of user. ABE concepts are mainly used in cloud computing storage and health records. Index is not set in Searchable encryption with inverted index scheme. Server must ensure the entire file later static and dynamic searchable encryption scheme was proposed to achieve fine grained access control. Outsourcing technology decreases the burden of high computation by two step outsourcing operation during encryption and decryption phase for reducing the amount of computation. Equality test mechanism is performed by two different public keys based on bilinear pairing in two cipher text encryption. Secure data sharing in cloud is achieved by testing two pair of cipher text which containssame plain text.[3]

The Attribute based Signature(ABS) method gives the authority as five basic steps Global set up, authority setup, Attribute generation signing phase and verification phase.LPP-MSA (Light weight Privacy Preserving Medical Service Access) follows the eight basic steps which include Global setup, Authority setup, key generation ,offline signature, online signature , Transform, CS(Cloud Server)-verify and MSP(Medical Service Provider) verify . By these basic steps, the security and performance isanalyzed using enforceability model. Unknown recognition and consent resistance between outward attacker and aided server is implemented. Performance is analyzed by using computation cost and storage cost[4].

The data amount of Electronic Medical Record (EMR) generated by health care industry has too increased aggressively. Health care data is in form of heterogeneous and insecure form. In EMR (Electronic Medical Record) various semantic structure and text mining can be developed to retrieve specific data from EMR collection. PBDSF (secure Pattern-Based Data Sensitivity Framework) is used to find and estimate the sensitivity of data by using frequent count of data and pattern matching of the data with ID or person name using second generate public/private key pair. Third elliptic curve integrated encrypted scheme used to encrypt sensitive data.it is done by using the following methods. Key agreement(KA),Key derivation function, encryption, message authentication code and authentication function. After encryption Hadoop and map reduce is used for resource management and parallel distribution. This security level reduces the processing power and less usage of memory. It can be decrypted using private key[5].

Elliptic Curve Cryptography technique used many schemes for encryption namely pseudo random generator using X and Y coordinates. The generation of random numbers is quite complex. Elliptic Curve Cryptosystem is used for hierarchical access control which changes the secret key based on hierarchical relationship. The EECC method avoids many attacks such as offline dictionary attack, man in the middle attack and brute force attack [6].

Electronic Health Record (HER) must have 3 basic cases for patient control.

Approving each requirement, setting rule for each authority and setting rule for central authority. SE-AC deals with setting rule for central authority with only one access for different kind of users. Organization Central Authority (OCA) is to avoid delay and congestion to distribute and balance responsibilities. It is done by setup and key generation for user requesting and description of 3 measures. These measures include Token generation, Time receiving encrypted cipher text and description time. [7]

External Quasi Identifier (EQI) uses two methods of operations concept covering and concept reducing. Constructing I dimension concept and redundant concept gets eliminated. Counting query, linear query and batch linear querying are kind of statistical query in querying phase. Global and local data are anonym zed by using k anonymity set value context. [9]

The issue of successfully taking care of Map reduce information was briefly represented in a cloud based virtualized method. [11]Search option and trust algorithm are used to get the query by using some search method in a limited amount of time. The maximum floating or exactness and manual searching are reduced. Relevant documents are processed by query search with three, two or single combination of keyword with reduced time. [12].

2. Literature Survey

Saad A. Abdelhameedaet. Al., [1] proposed the work of Restricted Sensitive Attributes based RSA-SA approach for privacy-preserving data stream publishing. A data stream publishing may publish the sensitive information about individual data. In this paper propose the work of giving security for sensitive attribute by using two approach semantic based and sensitive based approaches with multiple sensitive attribute. Through this method, efficient and more accurate data is maintained in mining analytical result with minimum delay and loss time. Butit cannotbe apply different mining method on sensitive attribute.

YingjieXue, KaipingXueet. Al., [2] proposed the work of Attribute-based encryption(ABE) method end up being an amazing cryptographic device to communicate get to approaches over characteristics, which can give a delicate, adaptable, and safe entree power above re-appropriated information. Collaboration access policy is allowed to gain access permission of many users with more than one attribute sets. Security investigation shows our proposed plan adequately bolsters information classification, client collusion resistance, controlled coordinated effort inside a similar gathering, unknown key privacy, Co-operation and secure denial and non-reusability of middle of the results.

Shangping Wang et. al.,[3] proposed the scheme of KS-ABESwETfor keyword search equality mechanism and converted index to adopt a pattern search. Cloud server and determine and authorize the cipher text and equality test mechanism. Datauser no needs to decrypt all cipher text, it leads to less storage and less resource utilization of IOT devices and complex operation gets simplified. It perform few calculation so it reduce storage difficulty. This equality algorithm may be simplified for further storage.

JINGWEI Liu et. al.,[4] proposed the work of Light weight Privacy

Preserving Medical Service Access(LPP-MSA) for health care cloud users privacy information. He identified the problem that ABS techniques not suitable for resource limited storage device. ABS (Attribute Based Signature is useful for anonymous authentication and privacy access control is overloaded computation in entering and confirmation phase. To make it's suitable for large scale and resource constraint mobile device use the LPP-MSA created on many authorities for health care cloud. Confirmation and signing phase it is very efficient.

Yiu Chung Yauet. al.,[5] proposed the work of PBDSFpractices machine learning mechanism to set of attributes of patient data gets identified. Hadoop and HDFS cluster method are used to process sensitive information about patient from huge amount of data. he does not give solution and among health care industry it gets shared.M.Sumathiet. al.,[6] proposed the work of Enhanced Elliptic Curve Cryptographic (EECC) algorithm to generate accidental key with data owner private key and exact association admin key. Achieves better efficiency and security for both customer and administrator of organization.in this paper does not deal with public auditing system.

KHALED RIADet. al.,[7] proposed the work of a sensitive and energetic access control (SE-AC) for electronic health record in the cloud. It maintains confidentiality of patient's data and fine gained control. SE-AC device is secure and unauthorized access gets prevented, performance analysis is efficient for different context.

Praneeta K. Maganti,et. al.,[8] proposed the work of Mobile health care Application (MHealth) to view health record in mobiles. Similar health condition records are found by giving more security among n number of records. In this patient's doctor encrypt health record and update it in the cloud by using ID-Based Encryption.

HongliZhanget. al.,[9] proposed the work of secrecy attentive set value data set for feasible publishing on the hybrid cloud. Feasibility is tested by using two phase data publishing phase and data querying phase. External Quasi Identifier (EQI) technique is used to partition data in publishing phase. The performance is evaluated using real life data sets. Through this method data privacy gets protected. It does not focus on reducing loss of information.

Mazhar Ali et. al.,[10] proposed the work ofDROPS. T colouring methods are used to store the data which is represented as number of fragments so that the attacker not gets meaningful data when tries to attack. It provides higher level of security.

3. Conclusion

We presented a survey of Searchable Encryption various techniques for sensitive attributes in the cloud storage.Sensitive Attributesbased Sequential approach,Attribute Based Encryption (ABE),Restricted Sensitive Attributes basedSequential Anonymization (RSA-SA) approach,Light weight Privacy Preserving Medical Service Access(LPP-MSA),Secure Pattern-Based for Big Data in Healthcare (PBDSF),Enhanced Elliptic Curve Cryptographic (EECC) algorithm,sensitive and energetic access control (SE-AC) are discussed briefly.

References

[1] Saad A. Abdelhameed , Sherin M. Moussa , Mohamed E. Khalifa, Restricted Sensitive Attributes-based Sequential Anonymization (RSA-SA) approach for privacy-preserving data stream publishing, Knowledge-Based Systems 164, pp.1–20, 2019.

[2] YingjieXue, KaipingXue, Na Gai, Jianan Hong, David S.L. Wei and Peilin Hong, AnAttirbute-Based Congtrolled Collaborative Access Control Scheme for Public Cloud Storage.IEEE Transactions on Information Forensics and security, Vol.14 ,Issue 11,November 2019.

[3] Jingwei Liu, Huifang Tang, Rong Sun, Xiaojiang Du and Mohsen Guizani, Lightweight and Privacy-Preserving Medical Services Access for Healthcare Cloud. IEEE Access,Volume 7, August 2019.

[4] Yiu Chung Yau, Praveen Khethavath and Jose A. Figueroa .Secure Pattern-Based Data Sensitivity Framework for Big Data in Healthcare.IEEE BCD IEEE Computer Society, May 2019.

[5] Shangping Wang,Lishayap, Juan Juanchen and Yaling Zhang .A Keyword Searchable AttributeBased Encryption Scheme With Equality Test in the Internet of Things. IEEE access on July 2019.

[6] M.Sumathi, and S.Sangeetha,Enhanced Elliptic Curve Cryptographic Technique for Protecting Sensitive Attributes in Cloud Storage. in 2018 IEEE International Conference on Computational Intelligence and Computing Research.

[7] khaled riad, rafik hamza, and hongyang yan .Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records.in IEEE Access on July 2019.

[8] Praneeta K. Maganti and P. M. Chouragade .Secure Application for Sharing Health Records using Identity and Attribute based Cryptosystems in Cloud Environment. in International Conference on Trends in Electronics and Informatics on 2019.

[9] HongliZhang, Zhigang Zhou, Lin Ye ,Xiaojian Du .Towards Privacy Preserving Publishing of Set-Valued Data on Hybrid Cloud. IEEE Transactions on Cloud Computing on . April-June 2018.

[10] Mazhar Ali, Kashif Bilal, Samee U. Khan, , BharadwajVeeravalli, Keqin Li, and Albert Y. Zomaya, DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security. in IEEE transactions, vol. 6, no. 2, april-june 2018.

[11] 1 S.Thilagavathi, 2 S.Vimala, 3K.Valarmathi, 4R.Priya, 5 S.Sathya .massive data processing using mapreduce aggregation to make digitized india. in International Conference for Phoenixes on Emerging Current Trends in Engineering and Management on 2018.

[12] Sridharan, K. , M. Chitra .trust based automatic query formulation search on expert and knowledge users systems.Journal of Computer Science 10 (7) on 2014.

[13] P. Ram Mohan Rao, S. MuraliKrishna , A. P. Siva Kumar .Privacy preservation techniques in big data analytics: a survey. in Journal of Big Data volume in 2018.