Secure Hybrid Method for Safe Transfer of Medical Image

R. Kavitha[1], K. Mithra[2], N. Nivetha[3] and P. Saravanan[4]

[1, 2, 3, 4]Department of Computer Science and Engineering, VCET, TN, India.
rkavibaskar1221@gmail.com1, mithushanthi04@gmail.com, nehanivetha@gmail.com, saravanankarthi002@gmail.com

Received Date: 17th March, 2017, Revised Date: 29th March, 2017, Accepted Date: 15th April, 2017.

Abstract - Security and privacy are important issues in Cloud computing. Existing scheme has Centralized Nature. It uses a Key approach and does not support Authentication. The proposed algorithm is region-based and Blowfish public key method was used to provide secure transmission. The algorithm combines Quantization Index Modulation (QIM) and AES block cipher algorithm in the Cipher Block Chaining mode. The system operates by encrypting the patient Information and embedding the encrypted data in the Medical image by Bitwise operation. Digital watermarking is the process that hides watermark data into a multimedia object such that the watermark can be detected or extracted from the object to prove its ownership or validate its integrity. Numerous numbers of effective schemes have been proposed for digital watermarking. As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data. The drawback of encrypting data and it can be selectively shared only at a coarse-grained level. Authors developed a new cryptosystem for fine-grained sharing of re-encrypted data called Key-Policy Attribute-Based Encryption (KP-ABE). In the cryptosystem, ciphertexts are labeled with the set of attributes and private keys are associated with access Particle Swarm Optimization (PSO) algorithm structure controls in which ciphertexts are decrypted. Authors demonstrate the applicability of construction to share audit log information and broadcasting re-encryption with TPA. This construction supports private keys which involve Hierarchical Identity-Based Re-Encryption (HIBR). These experiments highlight that one of the most important factors for efficient and accurate indexing for De-duplication and security is the proper definition of blocking keys.

Keywords - Security**,** Cloud computing, De-Duplication, Encryption, Digital Watermark.

I. INTRODUCTION

Online External storage is used by many people to share their data using Networking and Computer Technology. People share their private pictures and messages with Doctors for cost effective [4]. New Technologies impressed the people by their services so that the access control has been arising. People will allow access only to the Authorized users but unauthorized users hack the data and it causes the potential threats [2]. Attribute-Based Encryption (ABE) achieves fine-grained data access control, which provides access policies based on different attributes of the requester, environment [7]. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) defines an encryption to attribute set and decryption to decrypt the cipher text. De-Duplication Identifies records which refer to real world entity. It focused on simple Attribute similarities and based on Entity behavior. Straightforward Strategy matches the two Entities to measure the similarity between their behaviors [1]. Complete knowledge of Entity behavior is not available. Comparison between "Behavior" and "partial Behavior" are easily misleading. Applying CP-ABE in data sharing system has many challenges. The Key Generation Center (KGC) generate private keys to users, the primary benefit of this approach is to Reduce the need for processing and to store public key certificates. The advantage of the CP-ABE comes with a drawback which is known as a key Escrow problem [6]. The KGC can decrypt cipher text addressed to specific users by generating their attribute keys [3]. It could be a potential threat to the data confidentiality or privacy in the data sharing systems. Another challenge is the key revocation. Since some users change their associate attributes or some private keys might be compromised, key revocation or update for each attribute is necessary to make systems secure. It is tough. Since multiple users share each attribute. This implies that revocation of any attribute or any single user in a quality group would affect all users in the group, results in bottleneck during rekeying procedure or security degradation due to the windows of vulnerability [5].

II. MATERIALS AND METHODS

A. Approximate String Comparison

It deals with typographical error can be important in a record linkage context. If comparisons of pairs of strings are done in the exact character-by-character manner, then many matches may be lost. If matching performed on a character-by-character basis, then more than 30 percent of matches have been missed by computer algorithms that were intended to delineate matches automatically. These scenarios require manual review and matching error have greatly increased.

B. Discovering Duplicate Records

Record linkage is the process of combining multiple overlapping data collections such that records are believed to refer to the same entity are treated as a single entity. It has many applications, one of which is Genealogical Record Linkage (GRL). It considers more than exact-match pedigrees that may differ drastically, but it refers to the same individual. It

has significant to genealogical research because it links numerous databases, resulting in condensed search results which have a broad range of highly related information. The basic method compares the name and addresses information across pairs of files to determine those pair of records that are associated with the same entities. The main challenge is to design a function that can resolve when a pair of records has same entity instead of various data inconsistencies. Data quality has many dimensions one of which is accuracy. It is compromised by accidental errors in a database system. Errors may be inconsistent, incomplete or erroneous data elements. To improve the accuracy of a data store, it's necessary to compare it with other data stored in the same or a different system.

III. IMPLEMENTATION

Construct a user's private key which acts as a set of private key components, one for each attribute in the user's identity. The proposed method uses Shamir's method of secret sharing. It distributes a share of a master secret in the exponents of the user's private key components. Exponent gives our scheme the crucial property of being error-tolerant since only a subset of private key components is needed to decrypt the message. This scheme is resistant to collusion attacks. Different users have their private key components generated with different random polynomials. If multiple users collude, then they are unable to combine their private key components. In the first version of scheme, the public key size grows linearly with the number of potential attributes in the universe. The public growth is manageable for a biometric system where all the possible attributes are defined at the system creation time. However, this becomes a limitation in a more general system where an attribute can be defined by an arbitrary string. The proposed scheme is secured under an adapted version of the Selective-ID security model first. Our construction does not use random oracles. In previous methods allow a party to encrypt data to a particular user, but unable to handle more expressive types of encrypted access control such as the key authentication. Our construction has a delegation of private keys which subsumes Hierarchical Identity-Based Re-Encryption (HIBR) to share information in secure manner.

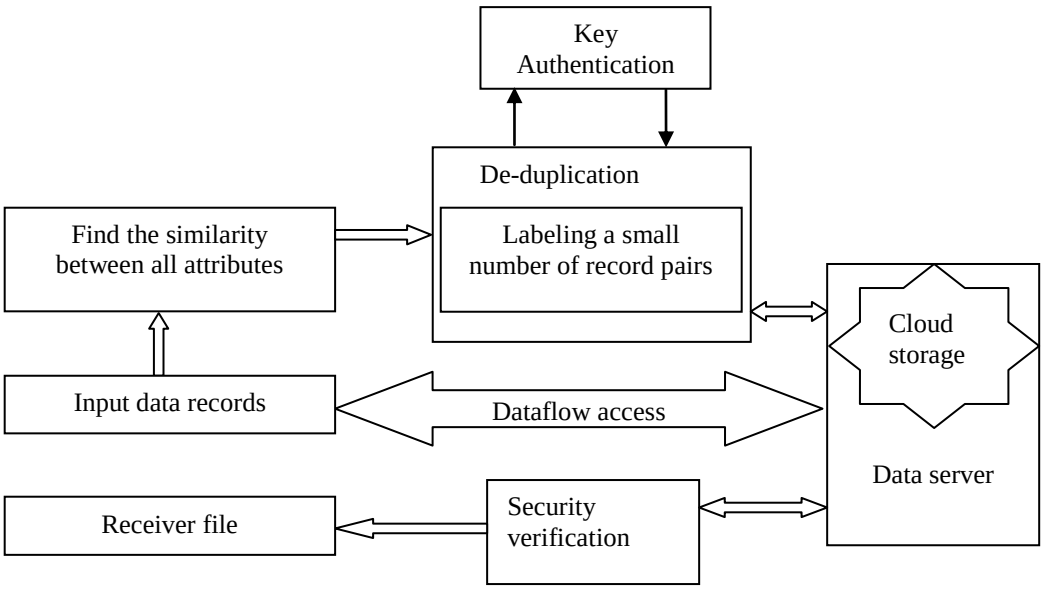

Fig. 1 Architecture of the Proposed System

IV. RESULTS AND DISCUSSION

A. Learning Based De-duplication

The proposed method is an interactive learning based on de-duplication system called Active Learning led Interactive Alias Suppression (ALIAS). This technique automatically constructs the de-duplication function by interactively finds the challenging training pairs. An active learner picks the subset of instances. It is easing that the de-duplication task by limiting the manual effort for simple, domain-specific attributes similarity functions. It labels a small number of record pairs. First, they took the small subset of the pair of records

B. Indexing Techniques

The Basic idea is to map records into multi-dimensional space and by a mapping into a second lower-dimensional metric space in which distance calculations are performed. The strings are mapped into a multidimensional space by R-tree. Clusters of similar objects are retrieved using indexing approach.

C. Unsupervised Duplicate Detection (UDD)

The unsupervised, online record matching method called Unsupervised Duplicate Detection (UDD). There are two classifiers in UDD for iteratively identifying the duplicate records where the same sources are removed by the exact matching method. Here relative distance of each field of the records is calculated. According to this value, the weight of the field will be assigned. Weighted Component Similarity Summing Classifier utilizes the weight set for matching records from various data sources. It places duplicate records in positive set and non-duplicate records in the negative set.

D. Key issuing secured access

Escrow-Free Key Issuing Protocol for KP-ABE The KGC and data-storing center are involved. A user is required to contact the two parties before having a set of keys. The KGC is responsible for authenticating a user and issues attribute keys to them if the user is entitled to its attributes. The secret key is to generate through a secure 2PC protocol between KGC and data-storing center. They engage in arithmetic secure 2PC protocol with master secret keys of their own, and issue independent key components. Then, the user is able to generate the whole secret keys with their key components received from two authorities. It deters them from knowing each other's master secrets so that none of them can generate the whole secret keys of a user alone.

V. CONCLUSION

In this paper, a survey of indexing techniques with twelve variations of them is presented in a detailed manner. The number of candidate record pairs generated by these techniques has been estimated and their efficiency, scalability had been tested using various data sets. Three tests were applied; ownership authentication, integrity verification test, and tamper localization test. By using these techniques transfer of medical images and reports are highly secured and cannot be operated by the unauthorized person. The results of this project will contribute a secure transmission of dates in cloud computing infrastructure.

REFERENCES

[1] D. Nilanjan, P. Moumita, D. Achintya, "A Session Based Blind Watermarking Technique Within the NROI of Retinal Fundus Images for Authentication Using DWT, Spread Spectrum and Harris Corner Detection", Intl. J. of Modern Engineering Research, Vol.2, No. 3, pp. 749-757, 2010.

[2] M. Soliman, A. Hassanien, N. Ghali, and H. Onsi, "An Adaptive Watermarking Approach for Medical Imaging using Swarm Intelligent", Intl. J. of Smart Home", Vol. 6, No. 1, 2012.

[3] X. Zhou and H. Huang, "Authenticity and Integrity of Digital Mammography Images", IEEE Trans. Med. Imag. Vol. 20, No. 8, pp. 784-791, 2001.

[4] W. Puech, "An Efficient Hybrid Method for Safe Transfer of Medical Images", 2nd Intl. Conf. E-Medical Systems, TUNlSIA, pp. 29-31, 2008.

[5] A. Umamageswari, U. Ferni, and G. Suresh, "A Survey on Security in Medical Image Communication", Intl. J. Computer Applications, Vol. 30, No. 3, 2011.

[6] D. Bouslimi, and G. Coatrieux, "A joint Watermarking/Encryption Algorithm for Verifying Medical Image Integrity and Authenticity in Both Encrypted and Spatial Domains", 33rd Annual Intl. Conf. IEEE EMBS Boston, Massachusetts USA, 2011.

[7] P. Viswanathan and P. Krishna, "Randomized Cryptographic Fusion Watermarking Medical Image with Reversible Property", Intl. J. of Computer Information Systems, Vol. 2, 2011.