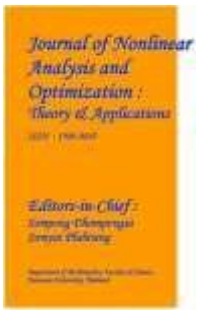
Journal of Nonlinear Analysis and Optimization
Vol. 16, Issue. 1: 2025
ISSN : 1906-9685



EFFICIENT DYNAMIC SEARCHABLE SYMMETRIC ENCRYPTION OVER MEDICAL CLOUD DATA

DANDU TEJASWI[1], Dr. A. RAMAMURTHY[2], Dr. G. SATYANARAYANA[3]
#1 M.Tech Scholar and Department of Computer Science Engineering,
#2 Professor, Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, AP, India.
#3 Professor, HOD Department of Computer Science and Engineering, DNR College Of Engineering and Technology, Bhimavaram, AP, India.

Abstract

Many web computing systems are running constant database services where their data change consistently and grow incrementally. In this unique circumstance, web data services have a noteworthy part and attract huge changes observing and controlling the data honesty and data spread. At present, web telemedicine database services are of focal significance to distributed systems. Be that as it may, the expanding many-sided quality and the fast development of this present reality social insurance testing applications make it difficult to instigate the database authoritative staff. The proposed approach is approved inside by measuring the effect of utilizing our computing services systems on different execution highlights like interchanges cost, reaction time, and throughput. The outcomes demonstrate that our incorporated approach essentially enhances the execution of web database systems and beats its partners. The strategies for workload-mindful anonymization for determination predicates have been examined in the writing. Notwithstanding, to the best of our insight, the issue of fulfilling the exactness limitations for different parts has not been examined some time recently. In our detailing of the previously mentioned issue, we propose heuristics for anonymization calculations and show observationally that the proposed approach fulfills imprecision limits for a bigger number of consents and has bring down aggregate imprecision than the present cutting edge and Fully Authenticated towards aggressor and data recovery.

Keywords: Computing Services, anonymization, web data services, clustering and Telemedical database.

I. Introduction

Telemedicine is unpretentious to utilize innovation and it is new, coquettish, and supposedly, there has a tendency to be a conviction among health service managers that in clinicians it can basically be made accessible who will consequently acknowledge and utilize the telemedicine systems. With the headway of correspondence innovation and data, Internet interfaces a huge number of hosts ecumenical has been getting increasingly well-known as of late. PC systems have made it conceivable to share through remote conference of electronic restorative records and to convey medicinal aptitude. Winning data Systems don't attractively bolster these attributes of telemedicine because of they are still record-situated in lieu of case arranged, and clients can't straightforwardly optically recognize an affiliation and an explicative photo of a case. The product application specialists to propose a few computing services methods to accomplish more proficient and compelling administration of web telemedicine database systems (WTDS). Noteworthy research advance has been made in the previous couple of years to enhance WTDS execution. Various types of patient data, for example, ECG, temperature, and heart rate should be gotten to by methods for different customer gadgets in heterogeneous interchanges conditions. WTDS empower brilliant persistent conveyance of patient's data wherever and at whatever point required. As of late, numerous specialists have focused on outlining web restorative database administration systems that fulfill certain execution levels. Such execution is ascertained by measuring the measure of significant and unessential data got to and the measure of exchanging medicinal data amid the exchanges

preparing time. Enhance database execution the few systems have been proposed all together, telemedicine, control therapeutic data multiplication and enhance restorative data conveyance. These methods trusted that superior for such systems can be accomplished by changing no less than one of the database web administration services, to be specific—data conveyance, database discontinuity, circulated reserving, database versatility and websites grouping. Data records might be covered or even repetitive with it, which increment the handling time, I/O exchanges thus the framework interchanges overhead. These works frequently examined fracture, now and again grouping issues and designation. The exchanges ought to be executed extremely speedy in an adaptable load adjusting database condition. At the point when the quantity of destinations in a web database framework increments to a massively goliath scale, the recalcitrant time complexity of handling a sizable voluminous number of therapeutic exchanges and dealing with a gigantically giant number of interchanges make the plan of such techniques a non-picayune assignment. The idea of security safeguarding for touchy data can require the implementation of protection arrangements or the insurance against personality exposure by fulfilling some protection necessities. The obscurity methods can be utilized with a get to control instrument [1] to guarantee both security and protection of the delicate data. The security is accomplished at the cost of precision and imprecision is presented in the approved data under a get to control strategy. A coordinated structure of accomplishing both protection and security is proposed however the joining of Access Control Mechanism with Privacy Preservation [2] Technique to keep the approved client from abusing the touchy data. The authorization of security approaches or the assurance against character revelation fulfilling some protection prerequisites are the pre-essentials for protection safeguarding of delicate data. Indeed, even after evacuation of distinguishing qualities, the delicate data is helpless to enjoying assaults by the approved clients.

II. Related Work

The accumulation of advanced data by governments, companies, and people has made colossal open doors for learning and data based basic leadership. Driven by common advantages, or by controls that require certain data to be distributed, there is an interest for the trade and production of data among different gatherings. Data in its unique frame, in any case, commonly contains touchy data about people, and distributing such data will abuse singular protection. The present practice in data distributing depends for the most part on arrangements and rules in the matter of what sorts of data can be distributed and on concessions to the utilization of distributed data. This approach alone may prompt over the top data mutilation or deficient insurance. Protection safeguarding data distributing (PPDP) gives strategies and instruments to distributing valuable data while saving data security. As of late, PPDP has gotten impressive consideration in inquire about groups, and many methodologies have been proposed for various data distributing situations. In this overview, we will methodicallly abridge and assess diverse ways to deal with PPDP, ponder the difficulties in functional data distributing, clear up the distinctions and necessities that recognize PPDP from other related issues, and propose future research headings [3] [4]. The greater part of these methodologies accepted a solitary discharge from a solitary distributer, and therefore just secured the data up to the main discharge or the principal beneficiary. We additionally looked into a few takes a shot at all the more difficult distributing situations, security insurance and protection safeguarding components [5]. Security assurance is an intricate social issue, which includes strategy making, innovation, brain science, and governmental issues. Security assurance inquire about in software engineering can give just specialized answers for the issue. Fruitful use of protection safeguarding innovation will depend on the collaboration of strategy creators in governments and chiefs in organizations and associations. Lamentably, while the organization of protection undermining innovation, for example, informal communities, develops rapidly, the usage of security safeguarding innovation, all things considered, applications is exceptionally restricted. As the hole ends up noticeably bigger, we anticipate that the quantity of occurrences and the extent of protection rupture will increment soon. Underneath, we talk about a couple of potential research headings in protection conservation, together with some attractive properties that could encourage the overall population, leaders, and systems specialists to receive security saving innovation. Most past security saving strategies were proposed for data distributers, yet singular record proprietors ought to likewise have the privilege and obligation to ensure their own private data. There is a critical requirement for customized security protecting apparatuses, for example,

protection safeguarding web programs and negligible data revelation conventions for web based business exercises. It is vital that the security protecting thoughts and apparatuses created are instinctive for amateur clients. Xiao and Tao's work on "customized security conservation" gives a decent begin, however little work has been led on this course since. Security assurance in emerging advances, similar to area based services; bioinformatics, and squash up web applications, improve our personal satisfaction. These new innovations enable organizations and people to approach already inaccessible data and data; notwithstanding, such advantages likewise raise numerous new protection issues. These days, once another innovation has been received by a little group, it can turn out to be extremely well known in a brief timeframe. A run of the mill case is the interpersonal organization application called Facebook. Since its sending in 2004, it has gained 70 million dynamic clients. Because of the huge number of clients, the mischief could be broad if the new innovation is abused. One research heading is to redo existing protection saving models for rising innovations. The

III. HIT (Health Information Technology)

Health information technology provides the umbrella framework to describe the comprehensive management of health information across computerized systems and its secure exchange between consumers, providers, government and quality entities, and insurers. Health information technology (HIT) is in general increasingly viewed as the most promising tool for improving the overall quality, safety and efficiency of the health delivery system. Broad and consistent utilization of HIT will:

- Improve health care quality
- Prevent medical errors
- Reduce health care costs
- Increase administrative efficiencies
- Decrease paperwork
- Expand access to affordable care

IV. Healthcare System

A health system, sometimes referred to as health care system, is the organization of people, institutions and resources that deliver health care services to meet the health needs of target populations. The recent advances in the growth of medical sciences, engineering studies, communications and information technologies have been supported by the growth of internet technology. Internet technology provides us effective, efficient and improved health care information about the patients and their health related problems. In healthcare field, face to face meetings between patients and doctors, doctors and doctors are essential and important. The situations where these meetings are not possible, there the designed models play a very important role in obtaining information about better treatments and care. It also covers all forms of communication between users: patients and health workers through electronic equipment from remote locations and areas.

A) Interoperability in healthcare System

Interoperability is the ability of two or more components, applications or systems to exchange and use information. There is currently a major challenge for the healthcare industry in achieving interoperability among applications provided by different vendors each hospital department or medical clinic may use multiple applications to share clinical and administrative information among applications.

For health professionals, it improves access to health record data and health information anytime, anywhere. For patients, quality and safety of care is improved by improving data exchange, quality of data flow and access of patients' information by health professionals. For health managers, data collection is improved and statistical and economic analysis is facilitated. For health researchers, availability of medical data is increased.

B) Distributed Patient Record

Distributed systems have a great importance in handling distributed patient records. The patient record has a distributed architecture and each client computer have local database. In distributed database architecture the data is not stored entirely at a single physical location instead it is spread across a network of computers and connected via communication links. We have therefore a large database capacity, reliable, available and flexible database. The most important advantage is that a distributed database allows faster local queries and can reduce network traffic.

V. Problem Definition

Several methods have been proposed in order to ameliorate telemedicine database performance, optimize medical data distribution, and control medical data expansion. These techniques believed that high performance for such systems can be gotten through using at least one of the database web management services, namely—database fragmentation, websites clustering ,database scalability. However, the intractable time intricacy of processing an immensely colossal number of medical transactions and managing a sizable voluminous number of communications makes the design of such methods a non-picayune task. Moreover, none of the existing methods consider the threefold service together, which makes them impracticable in the field of web database systems. Additionally, using multiple medical services from different web database providers may not fit the needs for improving the telemedicine database system performance. Further, the accommodations from different web data-base providers may not be compatible or in some cases it may increase the processing time because of the constraints of on the network. Finally, there has been a lack in the tools that support the design, analysis and cost-effective deployments of web telemedicine database systems. Designing and developing fast, efficient, and reliable incorporated techniques that can handle a huge number of medical transactions on a large number of web health care sites in near optimal polynomial time are key challenges in the area of WTDS. To improve the performance of medical distributed database systems, we incorporate data fragmentation, websites clustering, and Fragmentation allocation computing services together in a new web telemedicine database system approach. This new approach intends to decrease data communication, increase system throughput, reliability, and data availability. [6][7][8]

VI. Access Control Enforcement

The correct tuple values in a relation are replaced by the generalized values subsequent to the anonymization process. During this case, access control enforcement over the generalized data has to be defined.

- Relaxed: Use overlap semantics and let access to all or any partitions that are overlapping the permission.

- Strict: Use enclosed semantics to authorize access to exclusively those partitions that are totally encircled by the permission. [9]

Both of these schemes have their own strengths and weaknesses. Relaxed enforcement violates the authorization predicate by giving access to additional tuples on the other hand it is helpful for applications where low cost of a warning is tolerable as compared to the risk related to a missed event. On the other hand, strict enforcement is appropriate for applications where a high risk is related to a false alarm as compared to the value of a missed event. Associate example could be a false arrest just in case of breaking and entering. During this paper, the focal point is on relaxed enforcement. But the planned strategies for anonymization are valid for strict enforcement because the considered heuristics decrease the overlap between partitions and queries. We have a tendency to any assume that under relaxed enforcement if the imprecision bound is violated for permission then that permission isn't assigned to any role [10]

VII. Proposed Methodology:

Our approach integrates three enhanced computing services' techniques namely, database fragmentation, network sites clustering and fragments allocation. We propose an estimation model to compute communications cost which helps in finding cost-effective data allocation solutions. We perform both external and internal evaluation of our integrated approach. In the proposed system we introduce a high speed clustering service technique that groups the web telemedicine database sites into sets of clusters according to their communications cost. This helps in grouping the websites that are more suitable to be in one cluster to minimize data allocation operations, which in turn helps to avoid allocating redundant data. We propose a new computing service technique for telemedicine data allocation and redistribution services based on transactions' processing cost functions. Access control is also relevant in the context of workload-aware anonymization. The framework is a combination of access control and privacy protection mechanisms. The access control mechanism allows only authorized query predicates on sensitive data. The privacy preserving module anonymizes the data to meet privacy requirements and imprecision constraints on predicates set by the access control mechanism. If any attacker attacks and modifies the details, we can find out easily that our data has been attacked and that data is also recovered.

Clustering Algorithm: K-Means Clustering:

The k-means algorithm is the most extensively studied clustering algorithm and is generally effective in producing good results. The major drawback of this algorithm is that it produces different clusters for different sets of values of the initial centroids. Quality of the final clusters heavily depends on the selection of the initial centroids. The k-means algorithm is computationally expensive and requires time proportional to the product of the number of data items, number of clusters and the number of iterations.

Algorithm 1: The k-means clustering algorithm

Input:

D = {d1, d2, ...,dn} //set of n data items.

k // Number of desired clusters

Output:

A set of k clusters.

Steps:

1. Arbitrarily choose k data-items from D as initial

centroids;

2. Repeat

Assign each item di to the cluster which

has the closest centroid;

Calculate new mean for each cluster;

Until convergence criteria is met.

Attack sequence mining algorithm

Input:

The set of Sequence Database, S;

The minimum support threshold, min support;

Output:

The set of sequential patterns, S;

1: Scanning the Database S to extract the set of Items whose frequency is bigger than min support,

Items < −scan (sequenceDatabase)

2: for each item ∈ Items do

3: α < −item;

4: for all sequences ∈ sequenceDatabase

5: Suff ixSequence = Suff ix(α).removeitem(α)

6: S |α= AppendSuff ixSequence(Suff ixSequence);

7: end for

8: for all itemsequence ∈ α do;

9: // extend the item in independence sequence like a.iadd() = {a, b}

10: α < −item.iadd();

11: l < −α

.length;

12: pref ixspan(α

, l, S |α);

13: // extension the item in a sequence like a.sadd() = {(a, b)}

14: α < −item.sadd();

15: l < −α.length;

16: pref ixspan(α, l, S |α);

17: end for

18: end for

Experiment,

VIII. Conclusion

An access control framework for relational data has been proposed. The framework is a combination of access control. The access control mechanism allows only authorized query predicates on sensitive data. This anonymizes the data to meet privacy requirements and imprecision constraints on predicates set by the access control mechanism. In the current work, static access control and relational data model has been assumed. Formulate the accuracy and privacy constraints. Finds the attackers and data will be recovered.

In future, we plan to extend the access control to incremental data and cell level access control.

References

[1] Ismail Hababeh, Issa Khalil, and Abdallah Khreishah “Designing High Performance Web-Based Computing Services to Promote Telemedicine Database Management System” IEEE

TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 1,
JANUARY/FEBRUARY 2015.

[2] P. Samarati, "Protecting Respondents' Identities in Microdata Release," IEEE Trans. Knowledge and Data Eng., vol. 13, no. 6, pp. 1010-1027, Nov. 2001.

[3] B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-Preserving Data Publishing: A Survey of Recent Developments," ACM Computing Surveys, vol. 42, no. 4, article 14, 2010.

[4] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-Diversity: Privacy Beyond k-anonymity," ACM Trans. Knowledge Discovery from Data, vol. 1, no. 1, article 3, 2007.

[5] K. LeFevre, D. DeWitt, and R. Ramakrishnan, "Workload-Aware Anonymization Techniques for Large-Scale Datasets," ACM Trans. Database Systems, vol. 33, no. 3, pp. 1-47, 2008.

[6] T. Iwuchukwu and J. Naughton, "K-Anonymization as Spatial Indexing: Toward Scalable and Incremental Anonymization," Proc. 33rd Int'l Conf. Very Large Data Bases, pp. 746-757, 2007.

[7] J. Buehler, A. Sonricker, M. Paladini, P. Soper, and F. Mostashari, "Syndromic Surveillance Practice in the United States: Findings from a Survey of State, Territorial, and Selected Local Health Departments," Advances in Disease Surveillance, vol. 6, no. 3, pp. 1-20, 2008.

[8] K. Browder and M. Davidson, "The Virtual Private Database in oracle9ir2," Oracle TechnicalWhite Paper, vol. 500, 2002.

[9] A. Rask, D. Rubin, and B. Neumann, "Implementing Row-and Cell-Level Security in Classified Databases Using SQL Server 2005," MS SQL Server Technical Center, 2005.

[10] S. Rizvi, A. Mendelzon, S. Sudarshan, and P. Roy, "Extending Query Rewriting Techniques for Fine-Grained Access Control," Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 551-562, 2004.

Authors

DANDU TEJASWI Pursing M. Tech in Department of Computer Science & Engineering From D.N.R College of Engineering & Technology, Bhimavaram, Andhra Pradesh, West Godavari, 534201, India. Her area of interest in cloud computing services.

Dr A Ramamurthy is working as a Professor & Dean Administration, department of Computer Science and Engineering in D.N.R College of Engineering & Technology, Bhimavaram, Andhra Pradesh, West Godavari 534201, India.

Dr. G. Satyanarayana is working as professor & HoD in the Department of Computer Science and Engineering in D.N.R College of Engineering & Technology, Bhimavaram, Andhra Pradesh, West Godavari District, 534201, India.