Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

A Fast Neighbour Search Algorithm Used To Outsourced Encrypted Medical Images

Mrs MARESWARAMMA P [1] , Mr.Yegiti Gunteiah [2]

#1 Assistant Professor in the department of AI&IT at DVR & DR HS MIC COLLEGE OF TECHNOLOGY (Autonomous), Kanchikacherla (NTR Dist, AP).

#2 MCA student in the department of DCA at DVR & DR. HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR District.

ABSTRACT:
Medical imaging is critical for medical diagnosis, and the delicate nature of medical images needs stringent security and privacy safeguards. Medical photos should be secured before being outsourced in a cloud-based medical system for the Healthcare Industry. However, at the moment, running queries over encrypted data without first performing the decryption step is difficult and impractical..
We present a secure and efficient approach for determining the precise nearest neighbour over encrypted medical photos in the project. Instead of measuring the Euclidean distance, we reject candidates by computing the lower bound of the Euclidean distance, which is connected to the data's mean and standard deviation. In contrast to most previous systems, ours can determine the precise nearest neighbour rather than an approximation. We then assess our proposed method to see if it is useful.

1.INTRODUCTION

CLOUD computing is becoming a norm in our society, and in such a deployment, the data owner can outsource databases and management functionalities to the cloud server. The latter stores the databases and supplies access mechanisms to query and manage the outsourced database. This allows data owners to reduce data management expenses and improve quality of service. However, the cloud may not be fully trusted because it may leak sensitive information to unauthorized entities (e.g., compromised) or foreign government agencies. The rapid evolution of cloud computing is revolutionizing e-Health and the whole Industry 4.0 in the field of healthcare. The cloud-based electronic healthcare system is one popular application for Healthcare Industry 4.0. A well-designe electronic healthcare system can obviously improve the quality of access and experience of healthcare users. In recent years

2.LITERATURE SURVEY

The Literature review plays a very important role in the research process. It is a source from here research ideas are drawn and developed into concepts and finally theories. It also provides the researchers a bird's eye view about the research done in that area so far. Depending on what is observed in the literature review, a researcher will understand where his/her research stands. Here in this literature survey, all primary, secondary and tertiary sources of information were searched. A literature survey or literature review means that researcher read and report on what the literature in the field has to say about the topic or subject. It is a study and review of relevant literature materials in relation to a topic that have been given.

1) Title: Computation partitioning for mobile cloud computing in big data environment Authors: J Li and D Yi

Description: The growth of Mobile cloud computing (MCC) is challenged by the need to adapt to the resources and environment available for mobile clients while working with the dynamic changes of network bandwidth. In this project, propose a model of computation partitioning for stateful data in the dynamic environment that will improve performance. First, constructed a model of stateful data streaming and studied the method of computation partitioning in a dynamic environment and developed a definition of direction and calculation of the segmentation scheme, including single frame data flow, task scheduling and executing efficiency. Second, we proposed a computation partitioning method for Single frame data flow and determined the data parameters of the application model, the computation partitioning scheme, and the task and work order data stream model

2) Title: Model-driven safety analysis of closed-loop medical systems

Authors: J M Goldman and I Lee

Description: In modern hospitals, patients are treated using a wide array of medical devices that are increasingly interacting with each other over the network, thus offering a perfect example of a cyber-physical system and study the safety of a medical device system for the physiologic closed-loop control of drug infusion. The main contribution of the project is the verification approach for the safety properties of closed-loop medical device systems and demonstrate, using a case study, that the approach can be applied to a system of clinical importance. Our method combines simulation-based analysis of a detailed model of the system that contains continuous patient dynamics with model checking of a more abstract timed automata model.

3) Title: Ubiquitous data accessing method in IoT-based information system for emergency medical services

Authors: B Xu and J Hu

Description: The rapid development of Internet of things (IoT) technology makes it possible for connecting various smart objects together through the Internet and providing more data interoperability methods for application purpose. Recent research shows more potential applications of IoT in information intensive industrial sectors such as healthcare services. However, the diversity of the objects in IoT causes the heterogeneity problem of the data format in IoT platform. Meanwhile, the use of IoT technology in applications has spurred the increase of real-time data, which makes the information storage and accessing more difficult and challenging. In this research, first a semantic data model is proposed to store and interpret IoT data. Then a resource-based data accessing method (UDA-IoT) is designed to acquire and process IoT data ubiquitously to improve the accessibility to IoT data resources

3.PROPOSED SYSTEM

• To locate the exact nearest neighbor in encrypted medical images that have been outsourced, we propose a method that is both effective and efficient.

• In particular, we propose a safe and effective solution to the problem of exact nearest neighbor search on encrypted medical images in the project. Dynamic updates are supported by our plan. It permits information clients to effortlessly add or erase clinical pictures at whatever point important.

• Permitted users should also send their encrypted requests to the cloud for evaluation to safeguard query privacy. Even though the data and queries are encrypted, the cloud—or a malicious insider—can still obtain private information about the actual data items by analyzing the data access patterns.

• Rather than ascertaining the Euclidean distance, we reject competitors by figuring the lower bound of Euclidean distance that is connected with the mean and standard deviation of information.

• The proposed system's scalability performance is satisfactory. Also, the unique changes to the data set no affect our calculation.

3.1 IMPLEMENTATION

Data Owner

In this module, the data owner Collect Patient data and Upload to Cloudlet like pid, pname, paddress, pcno, pemail, ppulse, pecg,

pSymptoms, brwose and attach about symptoms with Digital sign, add pimage(Encrypt all parametes except pname) and View all patient collect data in enc format with digital sign.

Server A

The **s**erver-A manages which is to provide data storage service for the wearable devices and also View all patients and authorize and View all doctors and authorize ,Vliew all patient Cloudlet data with enc format ,View Patient data access request and authorize ,View all Cloudlet Intruders details and View patient details recovered details ,View No.Of same symptoms in Chart(Symptom name vs No. Of Patients), View No.Of Patients refered same doctor in Chart(Doctor name vs No.Of Patients).

Data User

In this module, the patient Register and Login, View profile ,Request Data Access permission from cloudlet and view Response, Access Your data and select doctor from combo box and send to corresponding doctor and View doctor response with Medical prescription, Verify your data and recover and View and delete your details.

Server-B

The Server-B is the one who will perform the following operations such as Register and Login, View Profile, View patient details and give solution like Medicine details, Medical prescription details View all patient Medical prescription Details.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

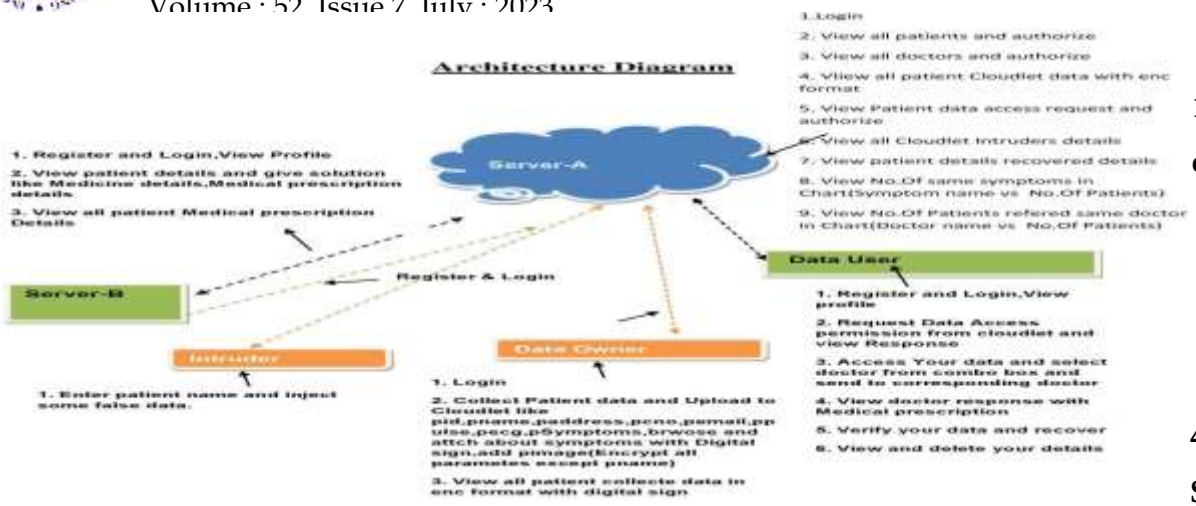

Fig 1:Architecture

4.RESULTS AND DISCUSSION

Fig 2;Doctor Main Page

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

Fig 2:Server-A Main Page

5.CONCLUSION

Cloud-based electronic healthcare systems will become more popular, owing to their capacity to share and access data in real-time between organisations (for example, between medical practitioners and healthcare providers) and countries. One process becomes difficult, if not impossible.

We provided a secure and efficient approach for locating the precise nearest neighbour over encrypted medical photos stored on a remote cloud server in the project. Our technique securely computes the lower bound of the squared Euclidean distance between a data point in the database and the query performed by a legitimate user in order to reject candidate data points. The effectiveness of our method is assessed using real-world medical photos.

REFERENCES

1. J. Li, L. Huang, Y. Zhou, S. He, Z. Ming, "Computation partitioning for mobile cloud computing in big data environment," IEEE Trans. Ind. Informat., vol. 13, no. 4, pp. 2009-2018, Feb. 2017.

2. K.-K. R. Choo, "Cloud computing: Challenges and future directions," Trends & Issues in Crime and Criminal Justice, vol. 400, no. 400, pp. 1– 6, Oct. 2010.

3. M. Pajic, R. Mangharam, O. Sokolsky, D. Arney, J. M. Goldman, and I. Lee, "Model-driven safety analysis of closed-loop medical systems," IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 3– 16, Feb.

2014.

4. B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT- based information system for emergency medical services," IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1578– 1586, May. 2014.

5. G. Yang et al., "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2180–2191, Nov. 2014.

6. H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System," IEEE Trans. Ind. Informat., vol. 13, no.3 pp. 1227-1237, June. 2017.

7. M. Li, S. Yu, W. Lou, and Y. T. Hou, "Toward privacy-assured cloud data services with flexible search functionalities," in Proc. ICDCSW. IEEE, Macau, CHN, 2012, pp. 466–470.

8. P. Williams, R. Sion, and B. Carbunar, "Building castles out of mud: practical access pattern privacy and correctness on untrusted storage," in Proc. CCS. ACM, Alexandria, VA, USA, 2008, pp. 139–148.

9. M. S. Islam, M. Kuzu, and M. Kantarcioglu, "Access pattern disclosure on searchable encryption: Ramification, attack and mitigation," in NDSS, San Diego, CA, USA, 2012.

10. D. E. Knuth, "Sorting and searching," in The art of computer programming, vol. 3, Boston, USA: Addison-Wesley, 1973.

11. D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in Proc. of IEEE S&P, DC, USA, 2000, pp. 44-55.

12. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," J. Comput.Secur., vol. 19, no. 5, pp. 895-934, 2011.

13. S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic Searchable Symmetric Encryption," in Proc. of ACM CCS, Raleigh, NC, USA, 2012, pp. 965–976.

14. S. Kamara, C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2013, pp. 258-274.

15. G. S. Poh, J.–J. Chin, W.-C. Yau, K.-K. R. Choo, and M. S. Mohamad, "Searchable Symmetric Encryption: Designs and Challenges," ACM Comput. Surv. vol. 50, no. 3, pp. 40:1- 40:37, 2017.