IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 1, June 2022

Outsourced Encrypted Private and Secured Data Storage on Dynamic Server Using AES Algorithm

Mrs. S Saranya[1], Ramya P V[2], Vaishnavi R[3], Sathya Revathi I[4]

Assistant Professor, Department of Computer Science and Engineering[1]

Students, Department of Computer Science and Engineering[2,3,4]

Dhanalakshmi College of Engineering, Chennai, Tamil Nadu, India

Abstract: *Clinical imaging is vital for clinical assessment, and the delicate idea of clinical pictures requires thorough security and sequestration results to be set up. In the paper, we propose a protected and successful plan to find the specific closest neighbor over deciphered clinical pictures. Not at all like most extreme being plans, our plan can acquire the specific closest neighbor as opposed to a rough outcome. Our proposed conspire clearly meets the security conditions. It safeguards the mystery and sequestration of information as well as the stoner's feedback question while contemporaneously concealing information access designs. Our plan is intended to safeguard the classification of all subsidiary clinical pictures. To safeguard inquiry sequestration, the data set and question should be made an interpretation of prior to moving to the pall garçon. Proposed Homomorphic calculation is utilized to encode information pictures. The trendy framework is Advanced Encryption Standard framework (AES). There are various kinds of AES that can be utilized yet the best is AES-128. Thus, the finish of this study is to configuration picture cryptographic activity utilizing the AES-128 framework. Cycle of plan tasks with this framework is through a few phases, comparable as interaction of encryption, decoding, urgent age and testing of the styles utilized. The assaults test is given by editing, obscuring, and upgrading the ciphertext picture. To lessen the storage facility issue in Cloud we've settle the picture and train into various square and get put away, so storage facility issue get helped. The proposed plot necessities to lessen the computation cost on the end-stoner however much as could be expected.*

Keywords: Clinical imaging

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.

DOI: 10.48175/IJARSCT-4669

[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.

DOI: 10.48175/IJARSCT-4669