International Journal of Engineering & Technology, 7 (4.19) (2018) 340-342

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Medi-Care Database Maintenance System

S.M. Keerthana[1], L.Priyanga Devi[2], D.Kavinya[3], N.Sharmila[4]

[1]*Assistant Professor, Sri Krishna College of Engineering and Technology, Coimbatore*
[2,3,4] *Assistant Professor, K S R Institute for Engineering and Technology, Tiruchengode*

Abstract

The recent advances in information and communication technology are congregation; storage and information sharing are simple and faster. We propose the architecture that guarantees the personal exchange of knowledge between patients and doctors through the SAS (storage aggregation server) by using asymmetric cryptography, the encoding technique. The random key enhances the security for the biomedical data of each patient. We introduce the concept of double-phase micro aggregation to restrict the intruder entities without the loss of information. We have derived that double phase multivariate micro aggregation properly and also the reduction of memory storage.

Keywords: *Memory storage, sharing, retrieval, confidentiality*

1. Introduction

Personal Health Record Maintenance System (PHRMS) is the most significant data storage system which is used for gathering, storing and retrieval of patient medical data for analysis. PHRMS makes use of Cloud computing technique for the storage of immense biomedical data. Cloud Computing is useful in allowing clients to provide storage and make computational models faster. The major influencing factors of this technology are the development in machine architecture, the need of collect and process large data sets and high bandwidth network channels for transmission of data.

PHRMS guarantees private exchange of biomedical data between patients and doctors without any intermediate entities. The security of the biomedical data of patients is enhanced by the Rivest Cipher4 cryptographic technique without the loss of information. To ensure confidentiality, we should constantly perform encryption. In a virtualized cloud environment, trustworthiness of data will not be guaranteed.

In PHRMS, there is no need of constant encryption and decryption of data. Here the patients (clients) can upload their medical report in encrypted format in the cloud which can be accessed by authorized Doctors by using the encryption key. The biomedical information in the cloud cannot be viewed by administrator because only a part of the key will be available to the administrator. In this way, the project provides trust to clients in an insecure data environment for the security of their medical report. It has been verified whether our proposed protocols will withstand against the man-in-the-middle attack. Hence PHRMS solves the security issues of biomedical data and also reduction of memory storage.

2. Existing System

In our existing system, confidentiality on the cloud is only done through encryption. but this is impractical because of its high computational cost and system can be easily compromised at the receiver side. the malicious acts of intruders are not fully addressed in our existing system. The major organizations such as military and healthcare are hesitating to move to cloud because of this. Therefore we are in a situation to move or adopt a secure cloud based services.

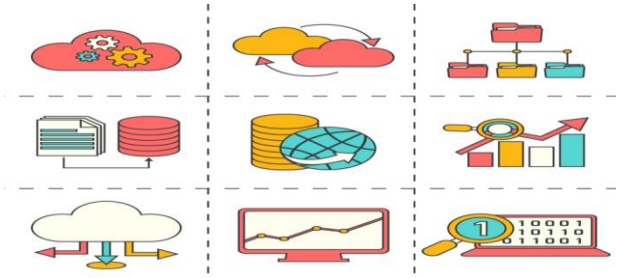

Fig. 1: Network of sharing data

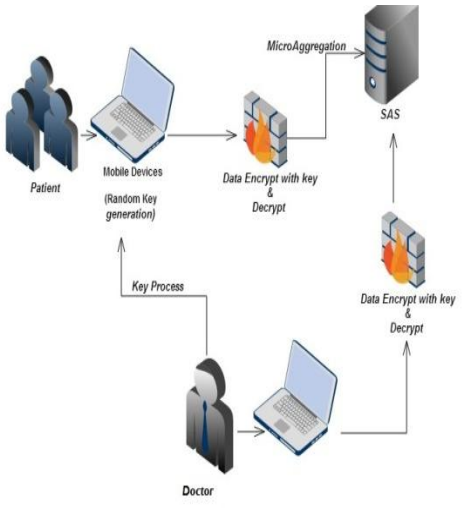

Fig. 2: Architecture for Securing Bio Medical Data

3. Proposed System

In proposed system, we introduce a mechanism for encrypted use of a Virtual machine in trusted cloud. Our next convention empowers a customer to ensure the secrecy and uprightness of its information and calculation from other customer applications in the cloud and from the cloud framework overseer. In the proposed show, the trusted computing base(TCB) decreased the size prerequisite of glint based code. The product stack from the BIOS up to the virtual Machine Monitor (VMM) level is in this way expelled from the proposed TCB of customer touchy code executed on the cloud stage. We have confirmed the privacy and respectability security properties of our proposed conventions utilizing the Prove if programmed cryptographic convention verifier. We have additionally checked that our proposed conventions are secure against man-in-the-center assaults

4. Results

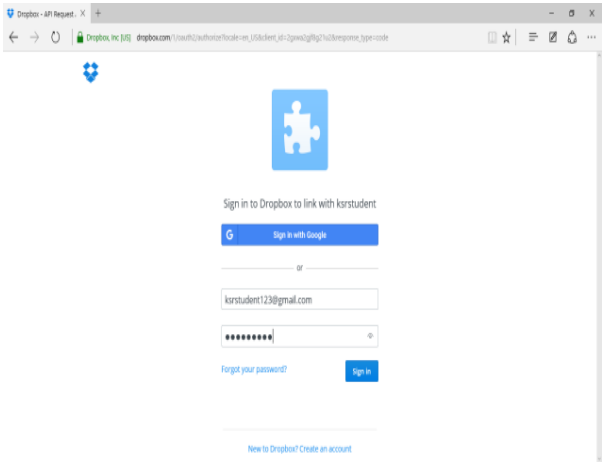

Fig. 3: Upload page

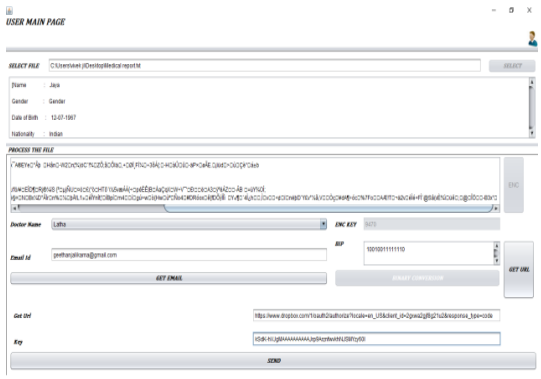

Fig. 4: User Main page

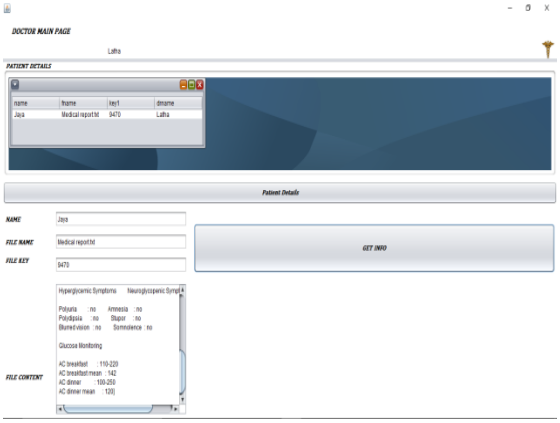

Fig. 5: Doctor Main page

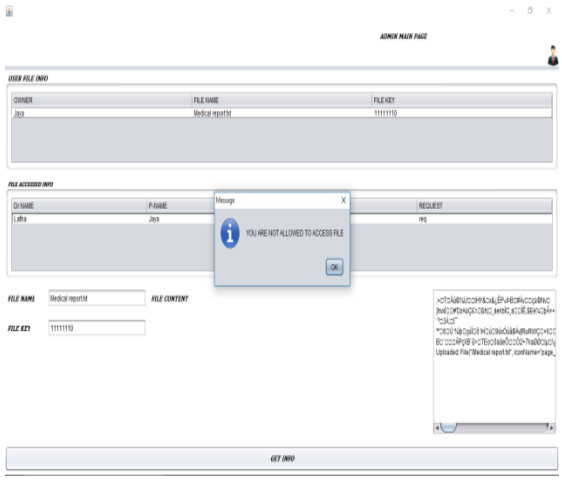

Fig. 6: Admin Main page

5. Conclusion

Distributed computing has encountered high development rates and is demonstrating extraordinary prospects. One of the greatest difficulties of cloud based administrations is classification and trustworthiness concerns. The records kept up and shared confronted a few information misfortune and system mistake. Despite the fact that the information are as a rule still kept up in the printed copy and exchanged with misuse of the cash. In this paper, we have introduced and formally checked a useful answer for address this issue. Our answer incorporates a convention for secure VM dispatch which empowers customers to check cloud stage setup before propelling their VMs on the cloud. A convention for performing delicate calculations in a cloud domain is introduced. We have formally confirmed the security properties of our proposed conventions utilizing ProVerif. Our framework can be received for both intel and AMD based frameworks. Results demonstrate that our answer is useful as far as execution.

6. Future Enhancements

Implementing this Personal Health Record Maintenance system in all hospitals helps the Hospital management to preserve the patient's history in a secured manner. To make ease of use the Personal Health Record Management System is to be developed as a web application which can be accessed anywhere.
To improve the retrieval facility of the health record for the second opinion by any other doctor aside, the login credentials can be created in advanced measures. As do we have some the standards that allow people to access the paper launched by the authors on the journals and international conference, the common membership can be provided by the standard authority for the security purpose to maintain the login credentials. By also in future the videos of the scanned report could also be added as detailed data of patient. These all could more be used to improve this heath record maintenance for accurate diagnosis.

References

[1] Nishita Ramakrishnan and Sreerekha "Enhancing Security of Personal Health Records in Cloud Computing by Encryption". International Journal of Science and Research.
[2] M. Naehrig, K. Lauter, and V. Vaikuntanathan. "Can homomorphic encryption be practical?" In Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pp. 113-124, New York, USA, 2011.
[3] S.Sheeba Rani, R.Maheswari, V.Gomathy and P.Sharmila, "Iot driven vehicle license plate extraction approach" in International Journal of Engineering and Technology(IJET) , Volume.7, pp 457-459, April 2018

[4] G. Coker, J. Guttmann, P. Loscocco, A. Herzog, J. Millen, B. OHanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen. "Principles of remote attestation". International Journal of Information Security, Volume 10, Issue 2, pp. 63-81, 2011.

[5] X. Lei, X. Liao, T. Huang, H. Li and C. Hu. "Outsourcing Large Matrix Inversion Computation to a Public Cloud". IEEE Transactions on Cloud Computing, Volume 1, Issue 2, pp. 78-89, 2013.

[6] Trusted-Java: Jsr321: Trusted computing api for java(tm) (2009) Available at: http://jcp.org/en/jsr/detail?id=321. Accessed on 06/09/2013.

[7] P. Tysowski and M. Hasan. "Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds". IEEE Transactions on Cloud Computing, Volume 1, Issue 2, pp. 172-186, 2013.

[8] S. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi and P. Samarati. "Integrity for Join Queries in the Cloud". IEEE Transactions on Cloud Computing, Volume 1, Issue 2, pp. 187-200, 2013.

[9] X. Leroy. "Formal certification of a compiler back-end, or: programming a compiler with a proof assistant". In 33RD Proceedings of ACM Symposium on Principles of Programming Languages, 2006.

[10] M. S. Simi , K. Sankara Nayaki "Data analytics in medical data : A review" , 10.1109/ICCPCT.2017.8074337, 2017.

[11] Subhash Chandra Pandey , "Data mining techniques for medical data: A review", 10.1109/SCOPES.2016.7955586, 2017.

[12] S. Balakrishnan, J. Janet, K.N. Sivabalan, "Secure Data Sharing In A Cloud Environment By Using Biometric Leakage resilient Authenticated Key Exchange", Pak. J. Biotechnol. Vol. 15 (2) 293-297 (2018).

[13] J. Janet, S. Balakrishnan and E. Murali, "Improved data transfer scheduling and optimization as a service in cloud," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-3. doi: 10.1109/ICICES.2016.7518895.

[14] Balakrishnan S., Janet J., Spandana S. "Extensibility of File Set Over Encoded Cloud Data Through Empowered Fine Grained Multi Keyword Search". In: Deiva Sundari P., Dash S., Das S., Panigrahi B. (eds) Proceedings of 2nd International Conference on Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 467. 2017. Springer, Singapore.

[15] J. Janet, S. Balakrishnan and K. Somasekhara, "Fountain code based cloud storage mechanism for optimal file retrieval delay," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-4. doi: 10.1109/ICICES.2016.7518901.

[16] J. Janet, S. Balakrishnan and E. R. Prasad, "Optimizing data movement within cloud environment using efficient compression techniques," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-5. doi: 10.1109/ICICES.2016.7518896.