TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 11272 - 11275

A Cloud Based Framework for an Efficient Health Care Management

[1] B. Santhosh Kumar, [2] P. Praveen Yadav
[1] Associate Professor, Department of CSE, G Pulla Reddy Engineering College, Kurnool.
[2] Assistant Professor, Department of CSE, G Pulla Reddy Engineering College, Kurnool.
[1] santhoshkumar.bala@gmail.com, [2] praveenyadav.p@gmail.com

Article Info
Volume 82
Page Number: 11272 - 11275
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 21 February 2020*

Abstract
The work mainly focuses on building a framework for hospitals so that the patient's information can be exchanged with the doctors in a more secure way with the help of cloud technology. It also reduces the operational expenditures of the hospitals by developing a cloud environment which can be adapted according to the individual hospital's requirements. By employing the virtualization concept supported in the data centers in the cloud the processing speed can be improved. An API can be build which can be extended by future applications that involve in cloud based health care management.

Keywords: *API, Cloud, Virtualization.*

I. INTRODUCTION

In the present days Health care is considered to be an important aspect in every human's life. With the growth in technology many hospitals have converted their auditing system in to web applications where patient's information is stored and billing is done according to the treatment given to them. But proper care is not taken when the patient wants to consult a doctor with the specialization which is unavailable in his/her area. The patient has to travel long distances with all the reports so as to meet the doctors and get their suggestions.

The proposed work aims in building a cloud setup which will help the patients to send their diagnosis to the doctors who are located anywhere in the world and get their suggestions. By implementing the concept of Wireless Body Area Network (WBAN) sensitive information like ECG values can also be encrypted with digital signatures technique along with the patient's personal information, disease symptoms which can be stored in the central databases related to cloud. The patient can choose the specialized doctor.

The implementation of the cloud framework will help in reduction of expenditures related to maintenance of Electronic Medical Records (EMR). It makes the data processing easier as already stored data can be migrated to cloud with minimal changes.

II. MOTIVATION OR SOCIAL RELEVANCE

Many of the towns in India have medical hospitals which offer treatment to the people based on few specializations. The patients are asked to consult doctors who are very far away from their places just to take an opinion on their symptoms and treatment. This leads to increase in expenses of the patient which become a burden for the middle class families. In order to facilitate the patients to communicate with the doctor as well as to reduce the operational expenditures of the hospitals this work aims in implementing a framework through which communication is possible in a secure way and reduce the overhead on the patient.

III. LITERATURE SURVEY

The works proposed in [1] ,[2] and [3] in the area of consultation which will add t

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 11272 - 11275

discuss the implementation of SHA hashing techniques in a cloud based health care but the concept of digital signatures are not included which makes the encryption process more efficient. The various attacks that can happen in a cloud based health system are discussed in [4], [5] and [6]. The need for security in health care system and the various issues are elaborated by authors in their works proposed in [7], [8] and [9].

In the research works [10] and [11] the authors discussed various implementation of cloud environment based health care systems ignoring the security issues to a large extent. The importance of WBANs and their impact in health care monitoring is discussed in works [12], [13], [14] and [15]. Some of the very basic authentication schemes related to health care networks is elaborated in [16], [17] and [18] which are further adapted and used in cloud computing based health environment so as to improve privacy.

IV. ARCHITECTURE & FRAMEWORK

At first the patients and doctors go through a registration process which is supervised by the Registration Authority (RA) which in turn generates the pair of public key and the private key to every users of the application. The patient's personal details like name, address, disease symptoms etc.., can be updated manually by the staff through laptops provided at the particular departments in the hospital.

A Wireless Body Area Network (WBAN) sensor is attached to the patient to get the details like ECG, body temperature and many more symptoms which might be useful in the assessment of his condition. The recorded values along with the personal details are taken as input and a doctor related to the specialization needed is selected from the list of doctors all over. The input values are accepted and a hash function is generated using SHA-2 algorithm. The process followed in SHA-2 is shown below where input is divided in to 8 blocks of 32 bits each.

One iteration in SHA-256 is as shown in fig-1.

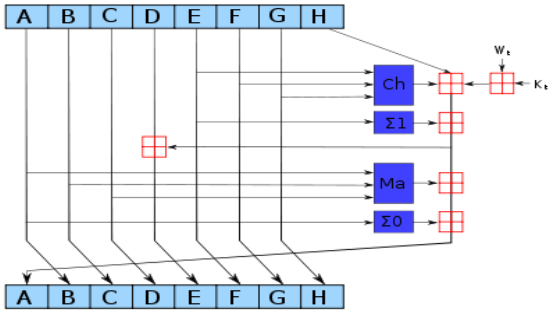

Fig-1:SHA-256 one iteration.

$$\mathrm{Ch}(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$
$$\mathrm{Ma}(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

For SHA-512 different constants are used in bitwise rotations. The numbers presented here are given for SHA-256. The red ⊞ notation displayed here is for addition modulo 2^{32}.The hash values along with the inputs are submitted to the Certificate Authorities (CA) which will encrypt the data using patient's private key, doctor's public key and generate the digital signatures to store them for authentication purposes.

The data at each hospital is updated regularly at the local database as a backup and it is submitted to the central cloud database for communication. When the data is submitted the doctors who are assigned a patient will request the information which goes through the CA.

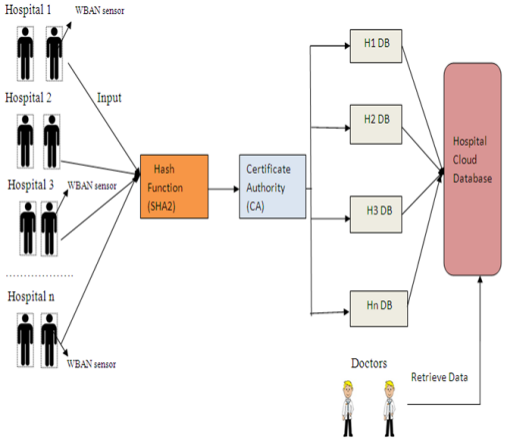

Fig-2:A Cloud Based Health Care Framework

Then CA assures the doctors identity and verifies the digital signature of the submitted data. Once the hash values are same the data is decrypted using patient's public key and doctor's private key. The doctor verifies

January - February 2020
ISSN: 0193 - 4120 Page No. 11272 - 11275

all the symptoms and gives his feedback and suggestions. If it is a critical issue the patient might be asked to meet in person.

V. RESULT ANALYSIS

The proposed framework is simulated using .NET framework and the results are mainly analyzed based on the number of Hashes generated in a millisecond. The result analysis suggests that the proposed work SHA-256 will surely execute in a better way than the other existing algorithms in the literature when compared. The analysis is shown in fig.3.

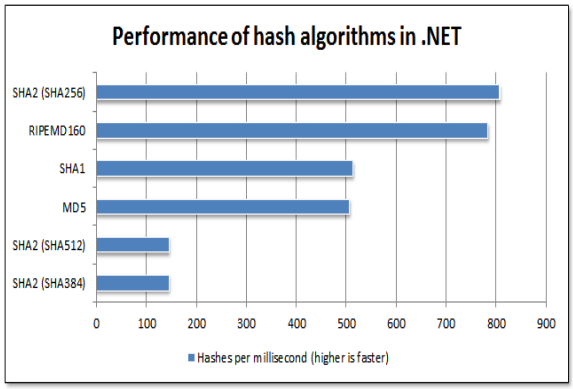

Fig-3: Comparison of different hashing Techniques

The analysis can be further enhanced by live implementation of the work in an existing cloud service provider environment and applying several hashing techniques with digital signatures.

VI. CONCLUSION

To overcome the difficulties faced in existing hospitals this work aims in communication of patients with doctors through a cloud environment. The doctors can provide their valuable suggestions depending upon the health condition of patient which would reduce the expenses of a patient to a large extent. If the work is implemented successfully many patients would get benefitted and hospitals can also reduce their maintenance costs by migration of their data in to cloud environment.

REFERENCES

[1] Purwanti, Sirep & Nugraha, Beny & Alaydrus, Mudrik. (2017). Enhancing security on E-health private data using SHA-512. 1-4. 10.1109/BCWSP.2017.8272557.

[2] Prabhleen Kaur Soul , Sunil Saini, "Data Security Approach in Cloud computing using SHA" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 06 | June -2017.

[3] Varalakshmi P, & Deventhiran H. (2012, April). Integrity checking for cloud environment using encryption algorithm. In 2012 International Conference on Recent Trends in Information Technology (pp. 228-232). IEEE.

[4] Garkoti, G., Peddoju, S. K., & Balasubramanian, R. (2014, December). Detection of insider attacks in cloud based e-healthcare environment. In 2014 International Conference on Information Technology (pp. 195-200). IEEE.

[5] Chen, C. L., Yang, T. T., Chiang, M. L., & Shih, T. F. (2014). A privacy authentication scheme based on cloud for medical environment. Journal of medical systems, 38(11), 143.

[6] Yehia, L., Khedr, A., & Darwish, A. (2015). Hybrid security techniques for Internet of Things healthcare applications. Advances in Internet of Things, 5(03), 21.

[7] Kant, D. C., & Sharma, Y. (2013). Enhanced security architecture for cloud data security. International journal of advanced research in computer science and software engineering, 3(5).

[8] Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data, 5(1), 1.

[9] Ali, A., Irum, S., Kausar, F., & Khan, F. A. (2013). A cluster-based key agreement scheme using keyed hashing for Body Area Networks. Multimedia tools and applications, 66(2), 201-214.

[10] Marwan, M., AlShahwan, F., Sifou, F., Kartit, A., & Ouahmane, H. (2019). Improving the Security of Cloud-based Medical Image Storage. Engineering Letters, 27(1).

[11] Vladimir Stantchev, Ricardo Colomo-Palacios, and Michael Niedermayer," Cloud Computing Based Systems for Healthcare", Hindawi Publishing Corporation The Scientific World Journal Volume 2014, Article ID 692619.

January - February 2020
ISSN: 0193 - 4120 Page No. 11272 - 11275

[12] Lin Y H Jan, IC, Chow In Ko, P Chen Y Wong JM Jan GJ'A wireless PDA-based physiological monitoring system for patient transport' IEEE vol. 8, no. 4, pp. 439-447, Dec 2004.

[13] Malan D Fulford Jones, T Welsh, M Moulton, S CodeBlue- 'An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care.' International Workshop on Wearable and Implantable Body Sensor Networks, London, UK, 6-7 April 2004.

[14] Halteren, AV Bults, RWac, K Konstantas, D Widya, I Dokovsky, N Koprinkov, G Jones,V HerzogR. 'Mobile patient monitoring- the MobiHealth system'. Journal on Information Technology in Healthcare, vol. 2, no. 5, pp. 365–373, 2004.

[15] Venkatasubramanian K, Banerjee A, GuptaS.K.S. 'EKG-based Key Agreement in Body Sensor Networks', In Proc. of 2nd Mission Critical Networks Workshop, IEEE INFOCOM workshops, Phoenix, AZ, April 2008.

[16] Ali A, Khan F A. 'An Improved EKG-Based Key Agreement Scheme for Body Area Networks'. In Proc. of International Conference on Information Security and Assurance, Miyazaki, pp. 298-308, 2010.

[17] Mayrhofer R. 'The candidate key protocol for generating secret shared keys from similar sensor data streams'. In Proceedings of the fourth European conference on Security and privacy in ad-hoc and sensor networks (ESAS-07), Berlin, pp. 1-15, 2007.

[18] MayrhoferR, Gellersen H. 'Shake well before use: authentication based on accelerometer data. In: Proceedings of the fifth international conference on Pervasive computing (Pervasive-07), Berlin, pp. 144-161, 2007.

AUTHORS PROFILE

B.Santhosh Kumar completed his PhD from Pondicherry University. He is currently working as an associate professor in CSE department in G.Pulla Reddy Engineering College, Kurnool. His interested areas of study are Cloud Computing, Data Mining and Machine Learning. He has published papers in eleven international journals and one international conference.

P.Praveen Yadav finished his M Tech degree from JNTU Pulivendula. He is now working as an assistant professor in CSE department in G.Pulla Reddy Engineering College, Kurnool. He is interested in the areas of Big data, Cloud Computing and Machine Learning. He has published papers in three International journals and one National conference.