CLOUD STORAGE REPOSITORY USING BGN CRYPTOSYSTEMS FOR HEALTHCARE DATA

J. Zahariya Gabriel[1], R. Ravi[2]

[1]Assistant Professor, Department of CSE, Francis Xavier Engineering College, Anna University, Tirunelveli, India

[2] Professor, Department of CSE, Francis Xavier Engineering College, Anna University, Tirunelveli, India

Abstract

This study has looked at the necessity of cloud data storage as well as the security concerns with data kept on third-party clouds. Industry standard solutions include the use of client-side, server-side, or both encryption in conjunction with appropriate policies for authorization and authentication to ensure that availability of the data transferred to the cloud is restricted. Even with these safeguards in place, security lapses have occurred in the past by exploiting framework flaws. Therefore, it is always welcome to try innovative approaches to cloud security. Part of the endeavor involves creating a framework, called SEC-EHRSAF, which is explained below for safe cloud data storage.

1. INTRODUCTION

Primary Health Centers (PHCs) and Community Health Centers (CHCs) are the primary providers of public healthcare services in India. The Indian government took the initiative to improve the services offered by Primary Health Centers (PHCs) with the Declaration of Alma-Ata. Here, we looked at the way PHCs operate, with health workers along with healthcare assistants working in the field to gather medical information from the 64 population [24]. They particularly prioritize programs like immunizations for infants, birth control, parenting support, anti-epidemic initiatives, and immediate medical attention in addition to standard medical care. Simply put, all of the patient data is stored on standalone computers or ledgers.

The following will help us achieve our aim of building a safe and private health cloud: primary health workers and medical assistants (immediate supervisors) will be provided with a mobile application to use for patient data collection. Patients' information is gathered in the following ways: i) through regular censuses; ii) during uncommon trips to primary health centers; iii) through regular visits (for example, for parental care or newborn immunization); iv) through vaccinations at polio medical facilities or different medical camps [1-5]. The key server authorizes and validates each health worker and health assistant before distributing encryption keys to them. The gathered information is transferred to a medical cloud encrypted [6-12].

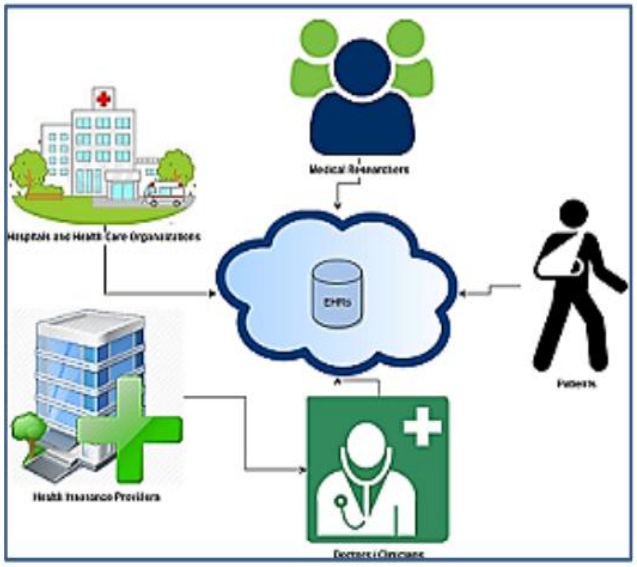

Medical Researchers
Hospitals and Health Care Organizations
EHRs
Patients
Health Insurance Providers
Doctors / Clinicians

Figure 1. Secure Cloud Model for health care

2. LITERATURE REVIEW

2.1 Challenges in Healthcare in India

The issues are solved with the help of the experience gained in metropolitan regions. FCA is employed to educate families about health issues and boost immunity and hygiene. The implementation of FCA is overseen by medical professionals and physicians [13-15]. The outcome of this strategy increased awareness among the members of the participating families. Numerous problems arise whenever the medical field is modernizing or reforming, which have an impact on the health care system.

2.2 Healthcare Data in Clinical Aspects

Amlan Majumder as well as Upadhyay (2004) state that information about female health care in India can be helpful in forecasting future social and economic factors. The essential data collection in the field of reproductive healthcare includes usage, availability and access of services, family features, ranging social structure, and quality of care. Keeping clinical records up to date is beneficial for comparative diagnosis [16-21]. According to research by Virostko et al. (2016), people with Type 1 diabetes can assess their pancreas size by keeping electronic medical data.

2.3 Healthcare Data in Non-Clinical Aspects

The economic elements that are significant for the well-being of nurses in Indian healthcare systems have been enumerated by Abhijit et al. (2008). Three states and all of north India's primary health care workers' economic statistics have been examined by Shankar Prinja et al. (2014) & Shankar Prinja et al. (2016). For the sake of future reference, this type of data requires a time and date stamping method. The next step is to compare the performance to the beneficiary's cost of the service.

2.4 Information and Communication Technology (ICT) in Healthcare

An ICT tool called mHealth PHC has been proposed by Ondale et al. (2013) to support primary healthcare in India [22-23]. The device is an application for mobile phones that facilitates communication between patients and members of the health organization, such as midwives and medical officers. Regional language assistance is offered by tool 32. Numerous data are sent through the application server & transcription server that are connected to this tool. It provides a scalable solution that can serve a larger clientele in the meantime.

3. PROPOSED METHOD

EHR encryption employs the Boneh, Goh, with Nissim (BGN) cryptosystem with cloud storage for safe data storage; 66 BGN decryption is used by data owners to decode EHRs in order to retrieve data. The EHRs are transferred to the cloud and re-encrypted using the AFGH scheme if the physician wants to share the patient's records with different HCs or GHs. When storing EHRs in a cloud repository, data is encrypted using the BGN algorithm if sharing is not intended. GHs can diagnose patients more quickly by using the pooled EHRs. In order to rank the PHCs and give logical orders to the appropriate government departments, administrators in DoHFW can employ data analytics to create assessments on the accomplishments of HCs. For instance, medication inventories can be updated in accordance with PHC requirements. Using EHRs, government hospitals may additionally safely analyze patient data to classify patients based on visit frequency, disease severity, and other factors.

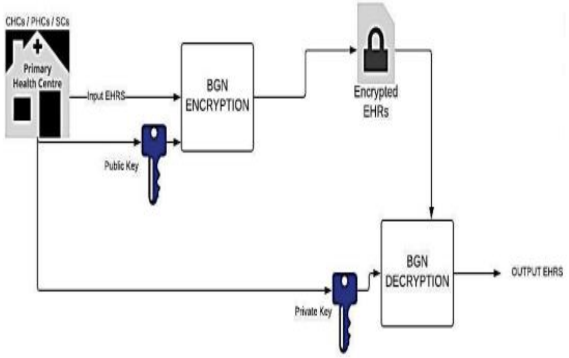
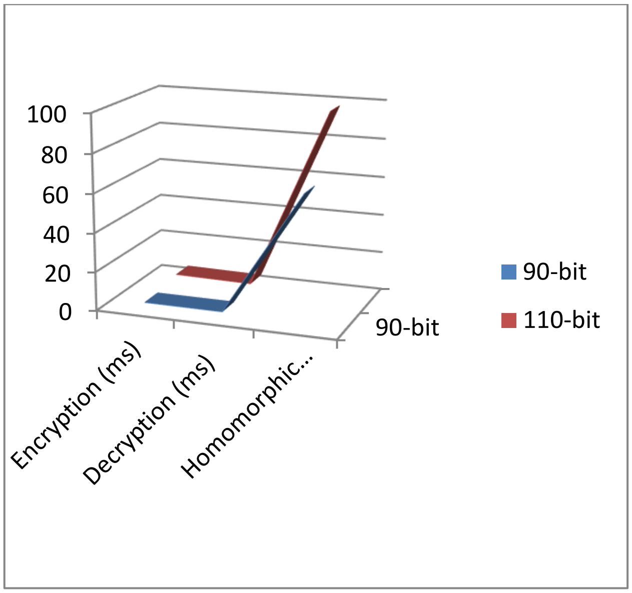


Figure: Cloud Storage Model

4. RESULTS AND DISCUSSION

Hospital apps that need to handle and keep sensitive data are assessed using our proposed framework. Applications for monitoring the health of senior citizens, fitness levels of those 75 years of age or older, heart patients' health information, fertility and menstrual cycle tracking, data processing from wearable sensors, etc., are a few examples. Sensitive data handled by these apps may be obtained by unauthorized users if it is transferred to the cloud for processing. Two apps have been considered to gather the data. The Blue Color indicates BGN and Red color indicates Paillier.

Table 1: Performance – Storage Mode



The typical setup time for the mobile device is displayed in Table 1. The BGN algorithm uses a relatively little amount of time 0.30 milliseconds compared to the Paillier technique.

When evaluating the SEC-EHRSAF framework's performance, we take into account the following KPIs.

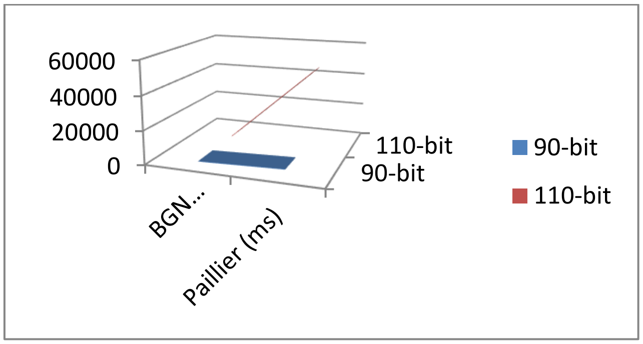
1) Execution time: The amount of time the CPU needs to finish a task. The energy utilized by mobile devices and the delays brought on by applications directly impact this time.

2) The size of the generated ciphertext is a crucial statistic for programs that rely on cryptographic primitives, such as SEC-EHRSAF. The size of the ciphertext is correlated with the network's communication requirements due to the bandwidth of the network.

3) Throughput: This is the speed at which operations are performed on the encrypted data.

The execution times for homomorphic additions on the cloud platform and decryption and encryption processes on the data owner's device are shown in Figure 2. The typical Average setup time for the mobile device is displayed in Table 2. The BGN algorithm uses a relatively lesser than Paillier technique in terms of Average setup time in msec. The Blue Color indicates BGN and Red color indicates Paillier.

Table.2 : Average setup Time



5. CONCLUSION

Using partial homomorphic encryption, a secure cloud storage system was created to hold patient electronic health records. Proposed Cryptosystem is used for the online storage of health data in order to maintain the integrity and security of sensitive patient data

FUTURE RESEARCH WORK

To improve task scheduling performance, valid parameters aside from data access complete time and cost need to be further researched.

• Performance in load balancing can be further improved by adding more performance measures. But caution must be exercised to avoid invalid parameters and to ensure that a multi-objective problem is feasible.

• To enhance the object & block storage system, which facilitates data interchange.

• To create a framework for applying deep learning techniques to rate the parameters of Service Level Agreements (SLAs).

• Multimedia applications need to have data security extended to them.

References

[1] M. I. B. Nordin and M. I. Hassan, "Cloud resource broker in the optimization of medical image retrieval system: A proposed goal-based request in medical application," 2011 National Postgraduate Conference, Perak, Malaysia, 2011, pp. 1-5, doi: 10.1109/NatPC.2011.6136316.

[2] M. Joshi, K. Joshi and T. Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018, pp. 932-935, doi: 10.1109/CLOUD.2018.00139.

[3] R. Kabilan, E. K. Devi, R. M. Bhuvaneshwari, S. Jothika, R. Gayathiri and R. Mallika Pandeeswari, "GPS Localization for Enhancement of Military Fence Unit," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 811-816,
doi: 10.1109/ICAIS53314.2022.9742959.

[4] Ravi, R., Zahariya Gabriel, J., Kabilan, R and Mallika Pandeeswari, R, "Hardware Implementation of OFDM Transceiver Using Simulink Blocks for MIMO Systems", Smart Antennas, Electromagnetic Interference and Microwave Antennas for Wireless Communications, River Publishers, 2022, pp. 95–110.

[5] Kabilan, R., Ravi, R., Shargunam, S and Mallika Pandeeswari, R, "VLSI Implementation on MIMO Structure Using Modified Sphere Decoding Algorithms", Smart Antennas, Electromagnetic Interference and Microwave Antennas for Wireless Communications, River Publishers, 2022, pp. 59–69.

[6] Ravi, R., Kabilan, R., Shargunam, S and Mallika Pandeeswari, R, "Joint Relay-source Escalation for SINR Maximization in Multi Relay Networks and Multi Antenna", Smart Antennas, Electromagnetic Interference and Microwave Antennas for Wireless Communications, River Publishers, 2022, pp. 47–58.

[7] M. Marwan, A. Kartit and H. Ouahmane, "Secure cloud-based medical image storage using secret share scheme," 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, Morocco, 2016, pp. 366-371, doi: 10.1109/ICMCS.2016.7905649.

[8] A. F. M. Hani, I. V. Paputungan, M. F. Hassan, V. S. Asirvadam and M. Daharus, "Development of private cloud storage for medical image research data," 2014 International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 2014, pp. 1-6, doi: 10.1109/ICCOINS.2014.6868433.

[9] R. Kabilan, R. Ravi, A. Antony Christian Raja, T. Prem Kumar, "Various Metal Sandwich Layer Oriented Efficiency Enhancement Superiority on CuInGaSe2 Thin Film Solar Cells", Advances in Chemical Engineering and Science, Vol.9 No.2, 2019.

[10] R. Ravi, S. Pasunkili, R. Kabilan, R. Muthukousalya, R. Mallika@ pandeeswari, M. Pavithran, S. Kannadhasan, "A Consumer Application with An Integrated Real-Time Power Theft Detection And Management System", Proceedings of the International Conference on Intelligent Technologies in Security and Privacy for Wireless Communication, ITSPWC 2022, 14-15 May 2022, Karur, Tamilnadu, India, doi: 10.4108/eai.14-5-2022.2318898

[11] M. F. Li and J. Feng, "Healthcare Road Map to Modernization in Clouds: Healthcare Forum for Healthcare Professionals, Medical Device Manufacturers, Pharmaceutical Companies and Average People on Virtual Private Clouds," 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Philadelphia, PA, USA, 2017, pp. 247-248, doi: 10.1109/CHASE.2017.86.

[12] Ravi, R., Mallika Pandeeswari, R., Kabilan, R and Shargunam, S, "Overcrowding Cell Interference Detection and Mitigation in a Multiple Networking Environment", Smart Antennas, Electromagnetic Interference and Microwave Antennas for Wireless Communications, River Publishers, 2022, pp. 71–82.

[13] X. Qu, Z. Wei and J. Zhang, "Research on architecture of medical data interaction platform based on cloud services," Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, Dalian, China, 2013, pp. 130-133, doi: 10.1109/ICCSNT.2013.6967079.

[14] V. Aswin and S. Deepak, "Medical Diagnostics Using Cloud Computing with Fuzzy Logic and Uncertainty Factors," 2012 International Symposium on Cloud and Services Computing, Mangalore, India, 2012, pp. 107-112, doi: 10.1109/ISCOS.2012.29.

[15] Kabilan, R., Ravi, R and Shargunam, S, "High Performance Fiber-Wireless Uplink for CDMA 5G Networks Communication", Smart Antennas, Electromagnetic Interference and Microwave Antennas for Wireless Communications, River Publishers, 2022, pp. 13–27.

[16] L. Wang, X. -l. Wang and K. -h. Yuan, "Design and implementation of remote medical image reading and diagnosis system based on cloud services," 2013 IEEE International Conference on Medical Imaging Physics and Engineering, Shenyang, China, 2013, pp. 341-347, doi: 10.1109/ICMIPE.2013.6864565.

[17] Ravi, R., Kabilan, R., Shargunam, S and Mallika Pandeeswari, R, "Joint Relay-source Escalation for SINR Maximization in Multi Relay Networks and Multi Antenna", Smart Antennas, Electromagnetic Interference and Microwave Antennas for Wireless Communications, River Publishers, 2022, pp. 47–58.

[18] Z. Xu, D. He, P. Vijayakumar, B. B. Gupta and J. Shen, "Certificateless Public Auditing Scheme With Data Privacy and Dynamics in Group User Model of Cloud-Assisted Medical WSNs," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 5, pp. 2334-2344, May 2023, doi: 10.1109/JBHI.2021.3128775.

[19] Kabilan, R and Ravi, R, "Speech Signal Extraction from Transmitted Signal Using Multilevel Mixed Signal", Smart Antennas, Electromagnetic Interference and Microwave Antennas for Wireless Communications, River Publishers, 2022, pp 1–11.

[20] H. T. Jung, K. H. An, J. C. Park, S. D. Kim and H. J. La, "MIaaS: Medical Image Archival and Analytics as-a-Service," 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2016, pp. 766-773, doi: 10.1109/CLOUD.2016.0106.

[21] Kabilan, R., Ravi, R and Shargunam, S, "Improving the Performance of Cooperative Transmission Protocol Using Bidirectional Relays and Multi User Detection", Smart Antennas, Electromagnetic Interference and Microwave Antennas for Wireless Communications, River Publishers, 2022, pp. 29–45.

[22] D. Ravichandran, R. Nimmatoori and M. R. A. Dhivakar, "Performance of wavelet based image compression on medical images for cloud computing," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, pp. 297-302.

[23] Y. Zhou et al., "XCloud-pFISTA: A Medical Intelligence Cloud for Accelerated MRI," 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Mexico, 2021, pp. 3289-3292, doi: 10.1109/EMBC46164.2021.9630813.

[24] R. Kabilan, "GSM-Based Power Administration of Intelligent Buildings" IRO Journal on Sustainable Wireless Systems, volume 5, Issue 3, 2023, pp:183-193.