International Journal of Scientific and Academic Research (IJSAR) ISSN: 2583-0279
Volume 3, Issue 8, August– 2023
www.ijsar.net
CrossRef DOI: 10.54756/IJSAR.2023.V3.8.1

Review of Literature on a Secure Algorithm for Management of Cloud-Based PACS Using a Hybrid Cryptographic Scheme

Olusayo Samson Oluwadare[1], Okike Benjamin[2], and Isaac Abiodun[2]

[1]Department of Computer Science and Mathematics

[1]Fayetteville State University, Fayetteville, North Carolina, USA

[2]University of Abuja, Nigeria

ABSTRACT

This paper presents a review of the literature on a secure algorithm for the management of cloud-based Picture Archiving and Communication Systems (PACS) using a hybrid cryptographic scheme. The selected articles were analyzed based on their research methodology, outcome of research, and remarks. The review highlights the various approaches used in secure algorithm design, their strengths and limitations, as well as the metrics used to evaluate their performance and effectiveness. The findings emphasize the importance of efficient key management, confidentiality, integrity, non-repudiation, and resistance against different security attacks in the design of secure algorithms for PACS management.

Keywords: Cloud-Based PACS, Confidentiality, Hybrid Cryptographic Scheme, Integrity, Key Management, Secure algorithm.

1. INTRODUCTION

The management of medical images and patient data in cloud-based Picture Archiving and Communication Systems (PACS) requires robust security measures to ensure the confidentiality, integrity, and availability of sensitive information. This literature review aims to explore existing research related to the design of a secure algorithm for cloud-based PACS management using a hybrid cryptographic scheme. By conducting a systematic search in the Scopus database, relevant articles were selected for detailed analysis and review. The purpose of this review is to provide a comprehensive understanding of the theoretical and conceptual background in this area, identify research gaps, and highlight the significance of developing a secure algorithm for PACS management.

2. METHODOLOGY

A systematic literature search was conducted in Scopus using keywords such as "secure algorithm," "cloud-based PACS," "hybrid cryptographic scheme," and related terms. The search was limited to articles published in peer-reviewed journals within the past five years to ensure the inclusion of recent research findings. A total of 8 articles were selected for detailed analysis and review. The selected articles were analyzed based on their relevance to the topic, methodology, key findings, and implications for secure algorithm design in cloud-based PACS management.

3. REVIEW OF LITERATURE

1. Sahoo et al. (2022). Key management for better security.

- Methodology: The authors propose a method that uses an image as a key to encrypt another image using RSA.

- Outcome of Research: The encryption and decryption time were found to be higher than the traditional method.

- Remarks: The evaluation based solely on encryption and decryption time may not be sufficient. Other metrics, such as entropy and avalanche effects, should be considered.

2. Krishnapriya & Smitha (2017). Image security.

- Methodology: The researchers use a Linear Feedback Shift Register (LFSR) to generate random numbers and perform XOR operations to shuffle and encrypt the pixels.

- Outcome of Research: The output image is completely different from the original image, and the Number of Pixel Change Rate (NPCR) is 99.582%.

- Remarks: The study lacks coverage of key management, storage methods, and other important aspects. Evaluating security based solely on NPCR may not be sufficient for real-life applications.

3. Chen et al. (2005). Security measures in PACS image acquisition and transmission.

- Methodology: The researchers propose a PKI-based security approach, including digital signature and data encryption using various algorithms.

- Outcome of Research: The encryption and decryption algorithms of Blowfish and IDEA perform well on most DICOM images. SHA1 is recommended for security implementation.

- Remarks: The study provides insights into encryption and decryption performance but lacks a comprehensive evaluation using popular security metrics.

4. Mondal et al. (2015). Efficient and secure image encryption algorithm.

- Methodology: The researchers propose a permutation-substitution architecture using LFSR and RC4 key sequence for encryption.

- Outcome of Research: The proposed algorithm shows visual differences between the input and output images and exhibits resistance against statistical, differential, and brute force attacks.

- Remarks: The scope of the study is broader, covering efficient key management, but other objectives need to be addressed.

5. Anusudha, K. (2018). Provision of secure medical image transaction.

- Methodology: The researcher proposes a hybrid algorithm involving bit plane slicing, stream ciphering, spread spectrum watermarking, and Diffie Hellman key exchange.

- Outcome of Research: The algorithm demonstrates high effectiveness based on NPCR and entropy metrics.

- Remarks: Key management during image transmission is not covered in the study.

6. Navamani, T. M., Bharadwaj, A., Agrawal, R., Agarwal, U. (2019). Preservation of DICOM Images Confidentiality and Integrity during transmission.

- Methodology: The researchers implement a solution using AES and Blake Hash Function algorithms to ensure confidentiality and integrity during DICOM image transmission.

- Outcome of Research: The AES algorithm provides confidentiality, and the Blake Hash Function ensures integrity. The solution supports encrypted storage and transmission of DICOM files.

- Remarks: The study lacks an evaluation with popular security metrics to benchmark the strength of the solution.

7. Leelasantitham & Kiattisin (2013). Encrypting DICOM header to protect patient information.

- Methodology: The authors propose a technique that encrypts the DICOM header using the jerk chaotic system.

- Outcome of Research: The technique provides confidentiality and has high key sensitivity. The power spectrum analysis supports its effectiveness.

- Remarks: The study lacks a comprehensive evaluation of other security aspects and relies on the analysis of the power spectrum.

8. Song et al. (2022). Efficient encryption and decryption of medical image.

- Methodology: The researchers propose a parallel computing approach based on a permutation-substitution architecture of chaotic encryption.

- Outcome of Research: The parallel processing shows superior efficiency compared to serial processing, and the proposed cryptosystem exhibits resistance against various attacks.

- Remarks: The performance efficiency depends on the system architecture.

DOI:10.54756/IJSAR.2023.V3.8.1

4. CONCLUSION

This review presents a summary of the methodologies, outcomes, and remarks of each reviewed article, highlighting the various approaches and their implications for the design of a secure algorithm for cloud-based PACS management. The findings emphasize the importance of efficient key management, confidentiality, integrity, and resistance against security attacks. Further research should consider a comprehensive evaluation using multiple security metrics to ensure the effectiveness and robustness of the proposed algorithms.

REFERENCES

[1].Desjardins, B., Mirsky, Y., Ortiz, M. P., Glozman, Z., Tarbox, L., Horn, R., & Horii, S. C. (2020). DICOM Images Have Been Hacked! Now What?. AJR. American journal of roentgenology, 214(4), 727–735. https://doi.org/10.2214/AJR.19.21958

[2].Kumar, A. M. & Kumar, K. A. (2022). A Survey on Cloud Computing Security Threats, Attacks and Countermeasures: A Review. *International Journal of Human Computations & Intelligence*, *1*(3), 13–18. https://milestoneresearch.in/JOURNALS/index.php/IJHCI/article/view/34

[3].Reynolds S. I. (2003). Imaging: new electronic tool for clinicians. *AMIA ... Annual Symposium proceedings. AMIA Symposium*, 984. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1480347/

[4].Pianykh, O. (2012). Brief History of DICOM. In book: Digital Imaging and Communications in Medicine (DICOM), 19-25. 10.1007/978-3-642-10850-1_4.

[5].National Electrical Manufacturers Association – NEMA (2023). DICOM PS3.1 2023a - Introduction and Overview. https://dicom.nema.org/medical/dicom/current/output/pdf/part01.pdf

[6].Hailegebreal., S., Sedi, T.T., Belete, S. Mengistu, K., Getachew, A., Bedada, D., Molla, M., Shibiru, T. & Mengiste, S.A. (2022). Utilization of information and communication technology (ICT) among undergraduate health science students: a cross-sectional study. *BMC Med Educ* **22(**215). https://doi.org/10.1186/s12909-022-03296-9.

[7].Addo, K. & Agyepong, P.K. (2020). The Effects of Information and Communication Technology on Health Service Delivery at Tafo Government Hospital. *E-Health Telecommunication Systems and Networks*, 9, 33-48. https://doi.org/10.4236/etsn.2020.93003

[8].Mildenberger , P., Eichelberg, M., & Marti, E. (2002). Introduction to the DICOM standard. *Eur Radiol*, *12*(4), 920-927. https://doi.org/10.1007/s003300101100.

[9].Genereaux, B.W., Dennison, D.K., Ho, K. et al. (2018). DICOMweb™: Background and Application of the Web Standard for Medical Imaging. *J Digit Imaging 31*, 321–326. https://doi.org/10.1007/s10278-018-0073-z

[10].Jozić, K., Frid, N., Jović, A., Mihajlović, Z. (2022). DICOM SIVR: A web architecture and platform for seamless DICOM image and volume rendering. *SoftwareX*, *18*(101063). https://doi.org/10.1016/j.softx.2022.101063.

[11].Eapen, B.R., Kaliyadan, F. & Ashique, K.T. (2022). DICODerma: A Practical Approach for Metadata Management of Images in Dermatology. *J Digit Imaging, 35*, 1231–1237. https://doi.org/10.1007/s10278-022-00636-5

[12].Chen, D., Wronka, A., Al-Aswad, L.A. (2022). Furthering the Adoption of Digital Imaging and Communications in Medicine Standards in Ophthalmology. *JAMA Ophthalmol, 140*(8), 761–762. https://doi.org/10.1001/jamaophthalmol.2022.2114.

[13].Bidgood, D. W., Horii, S. C., Prior, W. F., & Van Syckle, E. D. (1997). Understanding and Using DICOM, the Data Interchange Standard for Biomedical Imaging. *J Am Med Inform Assoc*., *4*(3): 199–212. https://doi.org/10.1136/jamia.1997.0040199

[14].Patel, G. N. (2012). DICOM Medical Image Management the challenges and solutions: Cloud as a Service (CaaS). *Third International Conference On Computing Communication & Networking Technologies (ICCCNT)*, 1, 1-5. https://doi.org/10.1109/ICCCNT.2012.6396083.

[15].Çığgın, A. S., Orhon, D., Rossetti, S., & Majone, M. (2011). Short-term and long-term effects on carbon storage of pulse feeding on acclimated or unacclimated activated sludge. *Water Research*, *45*(10), 3119-3128. https://doi.org/10.1016/j.watres.2011.03.026.

DOI:10.54756/IJSAR.2023.V3.8.1

[16].Wang, X., Huang, J., & Gao, D. (2021). Effects of three storage conditions on the long-term storage and short-term reactivation performances of anammox granular sludge. *International Biodeterioration & Biodegradation*, *164*(105310). https://doi.org/10.1016/j.ibiod.2021.105310.

[17].Zhou, F., Wang, J., Li, B., & Kim, J. (2014). Security issues and possible solutions in PACS systems through public networks. *Advanced Science and Technology Letters, 79*, 118-123. http://dx.doi.org/10.14257/astl.2014.79.23.

[18].Stites, M., & Pianykh, O. S. (2016). How secure is your radiology department? Mapping digital radiology adoption and security worldwide. *AJR Am J Roentgenol*, *206*(4), 797-804. http://dx.doi.org/10.2214/AJR.15.15283

[19].Bhadouria, A. (2022). Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches. *International Journal of Scientific and Research Publications*, *4*(2) http://dx.doi.org/10.29322/IJSRP.X.2022.p091095.

[20].Alghawazi, M., Alghazzawi, D., Alarifi, S. (2022). Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *J. Cybersecur. Priv.2*, 764–777. https://doi.org/10.3390/jcp2040039

[21].DICOM (2023). Security. *The Medical Imaging Technology Association (MITA), a division of NEMA*. https://www.dicomstandard.org/using/security

[22].DICOMweb™ (2023). DICOM web. *The Medical Imaging Technology Association (MITA), a division of NEMA*. https://www.dicomstandard.org/using/dicomweb

[23].DICOM (2019). ITEM: DICOM FAQ Response to 128-byte preamble vulnerability. *The Medical Imaging Technology Association (MITA), a division of NEMA*. DICOM_FAQ_1_2019. https://www.dicomstandard.org/docs/librariesprovider2/dicomdocuments/wp-cotent/uploads/2019/05/faq-dicom-128-byte-preamble-posted1-1.pdf

[24].Ortiz, M. O. (2019). HIPAA-Protected Malware? Exploiting DICOM Flaw to Embed Malware in CT/MRI Imagery," Cylera Labs, 2019. https://labs.cyler a.com/2019/04/16/pe-dicom -medic almalware/.

[25].NIST National Vulnerability Database (2019). CVE-2019-11687 Detail. https://nvd.nist.gov/vuln/detai l/CVE-2019-11687.

[26].DICOM Committee (May 2019). DICOM 128-Byte Preamble – Press Release. https://www.dicom stand ard.org/wp-conte nt/uploa ds/2019/05/Press -Relea se-DICOM -128-Byte-Pream ble-Poste d1-2.pdf.

[27].Ujgare, N. S. & Baviskar, S. P. (2013). Conversion of DICOM Image in to JPEG, BMP and PNG Image Format. *International Journal of Computer Applications*, *62*(11), 22-26. https://research.ijcaonline.org/volume62/number11/pxc3884886.pdf

[28].Tsui, G. K. & Chan, T. (2012). Automatic Selective Removal of Embedded Patient Information From Image Content of DICOM Files. *Medical Physics and Informatics, Technical Innovation, AJR 198*, 769-772. https://doi.org/10.2214/AJR.10.6352.

[29].Priyadarshini, P., Prashant, N., Narayan, D.G., Meena S.M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science, 78*, 617-624. https://doi.org/10.1016/j.procs.2016.02.108.

DOI:10.54756/IJSAR.2023.V3.8.1