USE OF IOT IN HEALTHCARE: A DETAILED REVIEW

M. Vivek Anand, Assistant Professor, Department of Computer Science & Engineering, Galgotias University.

Abstract

Due to the rapid expansion of the Internet of Things (IoT) in the healthcare industry, the security and integrity of medical data have become major concerns for healthcare service applications. This article presents a hybrid security approach for the protection of diagnostic text data embedded in medical pictures. The suggested model is built by merging either a two-dimensional discrete wavelet transform 1 level (2D-DWT-1L) or a two-dimensional discrete wavelet transform 2 level (2D-DWT-2L) steganography approach with a suggested hybrid encryption system. The suggested hybrid encryption scheme is based on a mixture of AES plus Rivest, Shamir, and Adleman algorithms. The suggested methodology begins by encrypting the secret data; it then uses 2D-DWT-1L or 2D-DWT-2L to disguise the output in a cover picture. Cover pictures are used in both colour and grayscale to disguise a variety of text sizes. The peak signal-to-noise ratio (PSNR), mean square error (MSE), bit error rate (BER), structural similarity (SSIM), structural content (SC), and correlation were used to assess the suggested system's performance.

Keywords: IOT, Healthcare, Monitoring, Data.

Introduction

By integrating the virtual and physical worlds, the Internet of Things generates an integrated communication ecosystem of networked devices and platforms [1]. With the introduction of remote digital healthcare IoT devices, medical data transmission has become a regular occurrence. As a result, an efficient approach is required to assure the security and integrity of diagnostic data sent and received from the IoT environment [2]–[8]. This objective is accomplished by using steganography methods and system encryption methods to conceal digital data inside a picture [9]–[16].

Another name for data encryption is cryptography [17]. Encryption cryptography is the technique of encrypting messages in such a manner that only authorised persons may read them. The Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithms are the two primary methods employed in this study for data encryption [18]. AES is a symmetric encryption in which both sides use the same key [19]. It uses a fixed message block size of 128 bits of text (plain or encrypted) and keys of 128,192, or 256 bits in length. When sending lengthier messages, they are split into 128-bit pieces. Lengthier keys, it seems, make the encryption harder to crack, but also require a longer encrypt and decrypt procedure. RSA, on the other hand, is a public key method that is extensively used in commercial

and personal communication [20]. It has the benefit of being able to generate keys with a changeable key size of between (2-2048) bits.

Medical Uses

The core study on data concealment began with steganography, a term that refers to the science and art of concealment. data included inside a picture. The advantage of steganography is that it enables the delivery of classified communications without the transmission itself being discovered. The DWT has exceptional spatial localization, frequency dispersion, and multi-resolution features that correspond to the human visual system's theory of forms. This article demonstrates both one-level and two-level DWT steganography methods in the frequency domain. It segmented the picture into sections with a high and low iteration count. The high-iteration section provides information about the edges, while the low-iteration section is typically separated into high- and low-iteration sections [21].

The objective of steganography is not just to prevent others from discovering the concealed information, but also to eliminate any suspicion that the information is concealed. The message is a private document that must be conveyed and concealed inside the carrier in order to avoid detection. Any steganography system has two primary characteristics: steganography capability and imperceptibility. However, these two features are incompatible since it is difficult to expand capacity while keeping the steganography system's imperceptibility. Additionally, there are still a limited number of ways for concealing information for use with data transfer communication protocols, some of which are unorthodox, but have a bright future.

Conclusion

Study conducted a detailed analysis on IoT network security challenges. Numerous security criteria were considered, including authentication, integrity, and secrecy. A comparative study of various types of attacks, their behaviour, and threat level was conducted. These attacks were classified as low-level, medium-level, high-level, and extremely high-level attacks, with suggested countermeasures. Findings offered three colour picture steganogra- phy techniques for securing data in an Internet of Things infrastructure. The first and third techniques use three channels (red, green, and blue), whereas the second technique utilises two channels (green and blue). With the use of a shared secret key, dynamic positioning methods were employed to conceal information in the deeper layer of the picture channels. Study devised a method for securing all types of photos, but particularly medical photos. They sought to safeguard the integrity of electronic medical information by assuring its availability and authenticating it to guarantee that only authorised individuals could access it. To begin, the first section was encrypted using the AES algorithm. The ear print is also included in this study, where seven values were retrieved from the ear picture as a feature vector. By transmitting medical photos through the internet, the suggested methodology enhanced their security and protected them from illegal access.

References:

1. Alharbe, N., Atkins, A. S., & Akbari, A. S. (2013). Application of ZigBee and RFID technologies in healthcare in conjunction with the internet of things. *ACM International Conference Proceeding Series*, 191–195. https://doi.org/10.1145/2536853.2536904

2. Castellani, A. P., Dissegna, M., Bui, N., & Zorzi, M. (2012). WebIoT: A web application framework for the internet of things. *2012 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2012*, 202–207. https://doi.org/10.1109/WCNCW.2012.6215491

3. Espin Riosa, M. I., Pérez Flores, D., Sánchez Ruiz, J. F., & Salmerón Martinez, D. (2013). Prevalence of childhood obesity in the Murcia Region; An assessment of different references for body mass index [Prevalencia de obesidad infantil en la Región de Murcia, valorando distintas referencias para el indice de masa corporal]. *Anales de Pediatria*, *78*(6), 374–381. https://doi.org/10.1016/j.anpedi.2012.09.007

4. Fok, C.-L., Julien, C., Roman, G.-C., & Lu, C. (2011). Challenges of satisfying multiple stakeholders: Quality of service in the internet of things. *Proceedings - International Conference on Software Engineering*, 55–60. https://doi.org/10.1145/1988051.1988062

5. Gachet, D., De Buenaga, M., Aparicio, F., & Padrón, V. (2012). Integrating internet of things and cloud computing for health services provisioning: The virtual cloud carer project. *Proceedings - 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012*, 918–921. https://doi.org/10.1109/IMIS.2012.25

6. Han, C., Jornet, J. M., Fadel, E., & Akyildiz, I. F. (2013). A cross-layer communication module for the Internet of Things. *Computer Networks*, *57*(3), 622–633. https://doi.org/10.1016/j.comnet.2012.10.003

7. Istepanian, R. S. H., Sungoor, A., Faisal, A., & Philip, N. (2011). Internet of m-health things "m-IoT." *IET Seminar Digest*, *2011*(13611). https://doi.org/10.1049/ic.2011.0036

8. Kang, K., Pang, Z.-B., & Wang, C. (2013). Security and privacy mechanism for health internet of things. *Journal of China Universities of Posts and Telecommunications*, *20*(SUPPL-2), 64–68. https://doi.org/10.1016/S1005-8885(13)60219-8

9. Lopez, P., Fernandez, D., Jara, A. J., & Skarmeta, A. F. (2013). Survey of internet of things technologies for clinical environments. *Proceedings - 27th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2013*, 1349–1354. https://doi.org/10.1109/WAINA.2013.255

10. Lu, J.-W., Chang, N.-B., & Liao, L. (2013). Environmental informatics for solid and hazardous waste management: Advances, challenges, and perspectives. *Critical Reviews in Environmental*

Science and Technology, *43*(15), 1557–1656. https://doi.org/10.1080/10643389.2012.671097

11. Pang, Z., Chen, Q., Tian, J., Zheng, L., & Dubrova, E. (2013). Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things. *International Conference on Advanced Communication Technology, ICACT*, 529–534. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84876220797&partnerID=40&md5=1aa069a3afe6682e3d07702e9fdfb009

12. Rassam, M. A., Zainal, A., & Maarof, M. A. (2013). Advancements of data anomaly detection research in Wireless Sensor Networks: A survey and open issues. *Sensors (Switzerland)*, *13*(8), 10087–10122. https://doi.org/10.3390/s130810087

13. Rodríguez-Molina, J., Martínez, J.-F., Castillejo, P., & López, L. (2013). Combining Wireless Sensor Networks and semantic middleware for an internet of things-based sportsman/woman monitoring application. *Sensors (Switzerland)*, *13*(2), 1787–1835. https://doi.org/10.3390/s130201787

14. Sung, W.-T., & Chiang, Y.-C. (2012). Improved particle swarm optimization algorithm for android medical care iot using modified parameters. *Journal of Medical Systems*, *36*(6), 3755–3763. https://doi.org/10.1007/s10916-012-9848-9

15. Swiatek, P., & Rucinski, A. (2013). IoT as a service system for eHealth. *2013 IEEE 15th International Conference on E-Health Networking, Applications and Services, Healthcom 2013*, 81–84. https://doi.org/10.1109/HealthCom.2013.6720643

16. Vong, C.-M., Wong, P.-K., & Ip, W.-F. (2011). Framework of vehicle emission inspection and control through RFID and traffic lights. *Proceedings 2011 International Conference on System Science and Engineering, ICSSE 2011*, 597–600. https://doi.org/10.1109/ICSSE.2011.5961973

17. Xu, J., Zhang, T., Lin, D., Mao, Y., Liu, X., Chen, S., Shao, S., Tian, B., & Yi, S. (2013). Pairing and authentication security technologies in low-power bluetooth. *Proceedings - 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-IThings-CPSCom 2013*, 1081–1085. https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.185

18. You, L., Liu, C., & Tong, S. (2011). Community Medical Network (CMN): Architecture and implementation. *2011 Global Mobile Congress, GMC 2011*. https://doi.org/10.1109/GMC.2011.6103930

19. Zhang, G., Li, C., Zhang, Y., Xing, C., & Yang, J. (2012). SemanMedical: A kind of semantic medical monitoring system model based on the IoT sensors. *2012 IEEE 14th International Conference on E-Health Networking, Applications and Services, Healthcom 2012*, 238–243. https://doi.org/10.1109/HealthCom.2012.6379414