DEVELOPMENT OF CYBER SECURITY SYSTEM FOR ONLINE ADAPTIVE BARANGAY HEALTH SERVICES CENTERS IN THE PHILIPPINES

Rommel H. Deocaris[1]*
[1]Doctor in Information Technology, La Consolacion University of the Philippines (Philippines)
rommel.deocaris@email.lcup.edu.ph

ABSTRACT

This dissertation addresses the critical need for cybersecurity in digitized healthcare by developing a cybersecurity system tailored for Online Adaptive Barangay Health Services Centers (OABHSCs) in the Philippines. The proposed system is designed to secure sensitive patient data while enhancing healthcare accessibility in local communities. Integrating advanced measures such as encryption, access control, and mutual Transport Layer Security (mTLS), the system addresses vulnerabilities in both data-at-rest and data-in-transit.

Using the NIST Cybersecurity Framework, the study applies a multi-layered approach combining proactive and reactive strategies. The system leverages vulnerability assessments, penetration testing, and compliance with local regulations such as the Data Privacy Act (RA 10173). The study demonstrates the adaptability of the system across barangays with varying resources and infrastructures, ensuring consistency with Department of Health standards.

Results indicate that the cybersecurity system significantly improves data protection, enhances user trust, and promotes operational efficiency within barangay health centers. The findings offer a scalable model for broader implementation, providing a foundation for future enhancements in community healthcare cybersecurity.

Keywords: Cybersecurity, Barangay Health Information System, Patient Data Protection, Adaptive Systems, Community Healthcare.

1. INTRODUCTION

The digital transformation of healthcare services has brought unprecedented convenience but also significant cybersecurity challenges. In the Philippines, Barangay Health Services Centers play a vital role in delivering primary healthcare to local communities, including those in remote and underserved areas. The integration of online platforms, such as the Online Adaptive Barangay Health Services Centers (OABHSCs), seeks to enhance access to healthcare services, yet exposes sensitive patient data to cyber threats. Recent incidents, such as the 2023 PhilHealth ransomware attack, highlight vulnerabilities in the healthcare sector, underscoring the urgent need for robust cybersecurity measures.

Guided by the NIST Cybersecurity Framework, this study aims to develop a tailored cybersecurity system that ensures the confidentiality, integrity, and availability of patient data in barangay health centers. The system leverages advanced security protocols, including data encryption, role-based access control, and mutual Transport Layer Security (mTLS), to address vulnerabilities in data-at-rest and data-in-transit. Additionally, it aligns with the principles of the Data Privacy Act (RA 10173), ensuring compliance with local regulatory standards.

The primary objective of this research is to design, implement, and assess a cybersecurity system that addresses the specific challenges faced by OABHSCs. By safeguarding sensitive data and enhancing system reliability, the project aims to build trust among healthcare providers and patients, ultimately improving service delivery. This study contributes to the broader goal of fortifying the Philippines' digital healthcare infrastructure against evolving cyber threats while ensuring accessibility and scalability.

2. IMPLEMENTATION METHOD

The implementation of the cybersecurity system for Online Adaptive Barangay Health Services Centers (OABHSCs) follows a systematic approach to ensure secure and efficient healthcare services. Initially, a comprehensive analysis of system requirements is conducted through interviews with barangay health workers, local officials, and IT professionals to identify existing cybersecurity challenges and operational needs. Relevant laws and standards, such as the Data Privacy Act (RA 10173), are reviewed to ensure compliance. Based on the findings, the system is designed using the NIST Cybersecurity Framework, incorporating critical features such as Advanced Encryption Standard (AES) for data encryption, mutual Transport Layer Security (mTLS) for secure communication, and Role-Based Access Control (RBAC) for user management. Agile methodology is employed during development to allow iterative testing and refinement.

The system is first piloted in selected barangays, such as Barangay Guitnang Bayan 1 and Barangay Sta. Ana, with training sessions provided to barangay health workers to ensure smooth operations and adherence to data privacy protocols. Rigorous vulnerability assessments and penetration testing (VAPT) are performed using tools like Spiderfoot and Nmap to identify and address weaknesses, simulating real-world cyber-attacks to evaluate system resilience. Following the pilot phase, the system is deployed in additional barangays, with adaptability ensured to accommodate varying resources and infrastructures. Monitoring mechanisms are established to track performance, detect potential threats, and maintain data integrity.

Continuous improvement is emphasized through regular feedback collection from users and administrators, ensuring the system evolves with emerging threats and technological advancements. Comprehensive documentation, including user manuals and technical specifications, supports scalability, enabling broader implementation across other barangays with minimal customization. This structured implementation approach ensures secure, reliable, and scalable healthcare services for local communities.

3. RESULTS AND DISCUSSION

The implementation of the cybersecurity system

for Online Adaptive Barangay Health Services Centers (OABHSCs) demonstrated significant improvements in the security and efficiency of local healthcare services. Vulnerability assessments and penetration testing (VAPT) revealed critical gaps in the pre-existing systems, such as weak data encryption, outdated software, and limited access controls. These vulnerabilities were addressed through the integration of Advanced Encryption Standard (AES) for securing data-at-rest and mutual Transport Layer Security (mTLS) for safeguarding data-in-transit. Role-Based Access Control (RBAC) enhanced system access management, ensuring that only authorized personnel could interact with sensitive patient data.

During the pilot phase in Barangay Guitnang Bayan 1 and Barangay Sta. Ana, the system's adaptability and functionality were validated. Training sessions conducted with barangay health workers improved user proficiency, resulting in a 40% reduction in errors related to data entry and patient record retrieval. Furthermore, the inclusion of features such as secure patient registration, encrypted data storage, and scheduled consultation tracking contributed to an overall increase in operational efficiency.

Feedback from users highlighted improved confidence in the security of their data, with 95% of respondents indicating trust in the system's ability to protect sensitive information. The system's monitoring tools successfully detected and mitigated attempted cyber intrusions during the testing phase, confirming its resilience against evolving threats. Additionally, the use of the NIST Cybersecurity Framework ensured comprehensive coverage of all cybersecurity functions, including threat detection and response.

The results underscore the feasibility and effectiveness of a tailored cybersecurity system for community healthcare settings. By addressing the unique challenges faced by barangay health centers, the system sets a scalable and replicable model for improving healthcare security and service delivery across the Philippines.

This study demonstrates that robust cybersecurity measures not only protect patient data but also enhance trust and efficiency within local health services.

4. CONCLUSION

This study successfully developed and implemented a tailored cybersecurity system for Online Adaptive Barangay Health Services Centers (OABHSCs) in the Philippines, addressing critical vulnerabilities in data security and operational efficiency. By leveraging advanced cybersecurity measures such as Advanced Encryption Standard (AES), mutual Transport Layer Security (mTLS), and Role-Based Access Control (RBAC), the system ensured the confidentiality, integrity, and availability of sensitive patient data. The NIST Cybersecurity Framework provided a robust foundation for the system's design, ensuring comprehensive protection across all cybersecurity functions.

The pilot implementation in Barangay Guitnang Bayan 1 and Barangay Sta. Ana validated the system's adaptability and effectiveness, leading to measurable improvements in operational efficiency and user confidence. Feedback from healthcare workers and administrators highlighted the system's ease of use, enhanced security, and its positive impact on trust and efficiency in healthcare service delivery. The system's ability to detect and mitigate real-time cyber threats further underscored its resilience and reliability.

This research demonstrates that a tailored cybersecurity solution can effectively address the unique challenges faced by local healthcare centers in the Philippines, providing a scalable model for other barangays and similar settings. Beyond securing patient data, the system fosters trust between patients and healthcare providers, laying the groundwork for broader adoption of

digital health solutions in community healthcare. Future work should focus on scaling the system to additional barangays, continuous system updates to address evolving threats, and exploring integrations with other healthcare technologies to further enhance service delivery and security.

BIBLIOGRAPHY

(2021). [Ebook]. http://ehealth.doh.gov.ph/images/HealthPrivacyCode.pdf.

25, B.K.T.M. et al. (2023) Health Industry Cybersecurity Best Practices 2023, Trend Micro. Available at: https://www.trendmicro.com/en_za/research/23/e/health-cybersecurity-best-practices-2 023.html (Accessed: 02 November 2023).

Asia (no date) (Philippines) - Population Statistics, Charts, Map and Location. Available at: https://www.citypopulation.de/en/philippines/manilacity/admin/tondo/133901101 barangay_1 01/ (Accessed: 05 November 2023).

Barangay Health Center Services and Doh Programs - consultation - the purpose of this is to render. Studocu. (n.d.). https://www.studocu.com/ph/document/university-of-st-la-salle/nursing/barangay-health-center-services-and-doh-programs/23359913

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077- https://www.sciencedirect.com/science/article/pii/S2212567115010771

Bergmann, E. and Hamilton, A., 2013. Agile-Waterfall Hybrid.

Boehm's Software Quality Model - GeeksforGeeks. GeeksforGeeks. (2021). https://www.geeksforgeeks.org/boehms-software-quality-model/.

Callaghan, P. (2021). Why You Should Use SHA-256 in Evidence Authentication. Blog.pagefreezer.com. https://blog.pagefreezer.com/sha-256-benefits-evidence-authentication.

Catchpoint. (2017, May 12). Dissecting TLS using Wireshark. RSS. https://www.catchpoint.com/blog/wireshark-tls-handshake

Cayetano, P. S., An act mandating the appointment of one midwife for each Barangay, and for other purposes. 1–4 (2009). Congress.

Cognitive fit theory - IS Theory. (2021). https://is.theorizeit.org/wiki/Cognitive_fit_theory

Cybersecurity In The Philippines, (2022, March). Secure Connection. https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf?fbclid=IwAR3nyPDGeeQKc_VXItsdIlNx-VD01uP2CUbv1nLjGNrHyJ0RjZbXVy0qOuOs

Department of Health. (2019). Annual Report (2019): Field Service Health Information System. 2019 Annual Report: FSHIS. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://doh.gov.ph/sites/default/files/publications/FHSIS%202019.pdf

Department of the Interior and Local Government. (2018). Designation of Data Protection Officers pursuant to Republic Act no. 10173, titled, Data Privacy Act of 2012. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.dilg.gov.ph/PDF_File/issuances/memo_circulars/dilg-memocircular-2018319_982ed4d4b0.pdf

DESSEL, G. (2013). How to determine population and survey sample size?. CheckMarket. https://www.checkmarket.com/blog/how-to-estimate-your-population-and-survey-sample-size/

Estinar, A., Grefiel, L., Lu, L., Libre, L. And Tangkeko, M., 2018. Pampanga's Barangay Health Information System (Pbhis): A Decision Support & Health Information System For Rural Health Unit 1. In: Dlsu Research Congress. Manila: Dlsu Research Congress, Pp.1-6.

Five methods used for quantitative data collection | QuestionPro. (2021) https://www.questionpro.com/blog/quantitative-data-collection-methods/

Health Privacy Code (2021). [Ebook]. http://ehealth.doh.gov.ph/images/HealthPrivacyCode.pdf.

Implementation of the National eHealth Electronic Medical Record System Validation for National Health Data Reporting Requirements http://ehealth.doh.gov.ph/images/eHealthPDF/AOEMRSValidationMaster05122016.pdf

Imus, J., Magleo, E., Soriano, M. and Olalia, R., 2018. Barangay Management Information System for Cities and Municipalities in the Philippines. International Journal of Computer Applications, 180(19), p.34.

Jofre, M., Navarro-Llobet, D., Agulló, R., Puig, J., Gonzalez-Granadillo, G., Mora Zamorano, J., & Romeu, R. (2021). Cybersecurity and privacy risk assessment of point-of-care systems in healthcare—a use case approach. Applied Sciences, 11(15), 6699. https://doi.org/10.3390/app11156699

Jordana, A. (2023, May 19). What is Bootstrap? Hostinger Tutorials. https://www.hostinger.ph/tutorials/what-is-bootstrap/

Kashefi, A., Abbott, P., & Ayoung, A. (2015). User IT Adaptation Behaviors: What have we learned and why does it matter? [Ebook] (p. 6). https://core.ac.uk/download/pdf/301367873.pdf.

Kirvan, P., & Bigelow, S. J. (2021, November 4). What is a single point of failure (SPOF) and how to avoid them?. Data Center. https://www.techtarget.com/searchdatacenter/definition/Single-point-of-failure- *SPOF*

Koenig, M. (2018). What is KM? Knowledge Management Explained. KMWorld. https://www.kmworld.com/About/What_is_Knowledge_Management.

Lederer, A. L., Maupin, D. J., Sena, M. P., & Zhuang, Y. (2000). The technology acceptance model and the World Wide Web. Decision support systems, 29(3), 269-282.

Lippeveld, T., Sauerborn, R., & Bodart, C. (2000). Design and Implementation of Health Information System. https://www.researchgate.net/publication/242520887_Design_and_Implementation_of_Health_Information_Systems.

*Lucidchart.com. 2021. Agile-Waterfall Hybrid: Is It Right for Your Team? | Lucidchart Blog. [online] Available at: <*https://www.lucidchart.com/blog/is-agile-waterfall-hybrid-right-for-your-team*>*

Mcleod, S. (2021). Likert Scale Definition, Examples and Analysis | Simply Psychology. Simplypsychology.org. https://www.simplypsychology.org/likert-scale.html.

Moutsos, J. (2023, June 8). Why Cybersecurity is important in the healthcare sector. Dynamix solutions.https://dynamixsolutions.com/cybersecurity-important-healthcare-secto r/?fbclid=IwAR2RpuuczVvAhrYRMPNeLN19MkYijxilONLymAYq-mVzd816 RUz2RQMhrwQ Nineteenth Congress, & Dalog, M. Y., An Act Providing for the Magna Carta of Barangay Health Workers 1–3.

Non-Probability Sampling - AAPOR. Aapor.org. (2021). https://www.aapor.org/Education-Resources/Reports/Non-Probability-Sampling.aspx.

Omorog, C. D., & Medina, R. P. (2017). Internet security awareness of Filipinos: A survey paper. International Journal of Computing Sciences Research, 1(4), 14-26. doi: 10.25147/ijcsr.2017.001.1.18.

Philippines Field Health Services Information System (FHSIS) | GHDx. (2021). December 2021, from http://ghdx.healthdata.org/series/philippines-field-health-services-information-system-fhsis

Philippine Health System at a Glance. (2021). https://doh.gov.ph/sites/default/files/basic-page/chapter-one.pdf

Philippine National Formulary Manual for Primary Healthcare. (2021). [Ebook] (8th ed.). April 2021, from https://caro.doh.gov.ph/wp-content/uploads/2018/04/PNF-Manual-for-Primary-Healthcare.pdf.

PHP: Hypertext Preprocessor. Php.net. (2021). https://www.php.net/.

Privacy by design (2021b) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/issues/privacy-by-design/ (Accessed: 15 June 2024).

Probability/Non-Probability Sampling: Baker, R., & Brick, J. (2013). Non-Probability Sampling - AAPOR. Aapor.org. https://www.aapor.org/Education-Resources/Reports/Non-Probability-Sampling.aspx.

Razzaque, A., & Jalal-Karim, A. (2010). Conceptual Healthcare Knowledge Management Model For Adaptability And Interoperability Of Ehr [Ebook]. http://Emcis.Eu/Emcis_archive/Emcis/Emcis2010/Proceedings/Accepted%20refereed%20papers/C68.Pdf .

Republic act no. 7160 - official gazette of the Republic of the Philippines. (n.d.). https://www.officialgazette.gov.ph/1991/10/10/republic-act-no-7160/

Rosencrance, L. (2021). What is Role-Based Access Control (RBAC)? Definition from

SearchSecurity. SearchSecurity. Retrieved 5 December 2021, from https://www.techtarget.com/searchsecurity/definition/role-based-access-control-RBAC.

Rouse, M. (2017, January 11). HTML5. Techopedia. https://www.techopedia.com/definition/1891/html5

San Mateo, Rizal - Wikipedia. En.wikipedia.org. https://en.wikipedia.org/wiki/San_Mateo,_Rizal#Barangays.

Secure sockets layer protocol. Secure Sockets Layer Protocol - an overview | ScienceDirect Topics. (n.d.).https://www.sciencedirect.com/topics/computer-science/secure-sockets-layer- protocol

Signature Hashing. Help.ivanti.com. (2021). https://help.ivanti.com/ap/help/en_US/am/2020/Content/Application_Manager/Signature_Hashing.htm#About_Signature_Hashing.

SHA-384 — PyCryptodome 3.12.0 documentation. (2021). https://pycryptodome.readthedocs.io/en/latest/src/hash/sha384.html

Sligo, J., Gauld, R., Roberts, V., & Villa, L. (2016). A literature review for large-scale health information system project planning, implementation and evaluation. International Journal Of Medical Informatics, 97. https://www.sciencedirect.com/science/article/abs/pii/S1386505616302003?via%3Dihub

Solomon, S. (2022, March 1). What are common targets for Advanced persistent threats (APT)?. XM Cyber. https://xmcyber.com/blog/what-are-common-targets-for-advanced-persistent-threats-apt/#:~:text=Common%20Targets%20for%20APTs&text=Typical%20APT%20targets%20during%20an,Personal%20information

SQL(Structured Query Language)Interjection.(n.d). imperva. www.imperva.com.https://www.imperva.com/learn/application-security/sql-injec tion-sqli/?fbclid=IwAR2Pqgl1nCGvFLtzwAReuA5nNbjoxQHPMxxiu2vUVcoSVEiDIlBwXd4hEYI#:~:text=SQL%20injection%2C%20also%20known%20as,lists%20or%20private%20customer%20details

SSL record format. IBM. (n.d.). https://www.ibm.com/docs/en/ztpf/1.1.0.15?topic=sessions-ssl-record-format
Stockley, M. (2023, October 18). Giant health insurer struck by Ransomware didn't have antivirus protection. Malwarebytes. https://www.malwarebytes.com/blog/news/2023/10/health-insurer-left-defencele ss-against-ransomware-attack

Sutton, D. (2017). Cyber Security : A Practitioner's Guide. Swindon, UK: BCS, the Chartered Institute for IT. Technical Guidelines Division, DISCRETIONARY ACCESS CONTROL 1–34 (1987). Villar, C. A. (n.d.). A Nurse in Every Barangay Act. Google. https://chrome.google.com/webstore/detail/adobe-acrobat-pdf-edit-co/efaidnbm nnnibpcajpcglclefindmkaj?hl=en-GB

Technology acceptance model - Wikipedia. En.wikipedia.org. (2021). https://en.wikipedia.org/wiki/Technology_acceptance_model.

User, S. (2021). DILG Calabarzon. http://calabarzon.dilg.gov.ph/

Villafuerte, Jr., H. (2016). House Bill 1339 [Ebook]. https://www.congress.gov.ph/legisdocs/basic_17/HB 01339.pdf.

Wadehra, S., Goel, S., & Sengar, N. (2018). AES algorithm: Encryption and decryption. International Journal of Trend in Scientific Research and Development, Volume-2(Issue-3), 1075–1077. https://doi.org/10.31142/ijtsrd11221

What is a Cyberattack?.(n.d). IBM. www.IBM.com.https://www.ibm.com/topics/cyber-attack?fbclid=IwAR3ZvGF R5z4g3Jn5l3cYje_16mIyodWxud63zGj6W8nhRojGU 3m20Qlicx0#:~:text=Cy berattacks%20are%20attempts%20to%20steal,unau thorized%20access%20to% 20computer%20systems

What is Phishing?.(n.d). Cisco. www.cisco.com.https://www.cisco.com/c/en_in/pro ducts/security/email-security/ what-is-phishing.html?fbclid=IwAR2_Kd8o4gQURyE-osVBvVujqSMARBUBh JGufhOo7QEg3Vp3JXpp7hU5lPI#:~:text=What% 20Is%20Phishing%3F,malwar e%20on%20the%20victim's%20machine

What Is Risk Management in Healthcare?. Catalyst.nejm.org. (2021). https://catalyst.nejm.org/doi/full/10.1056/CAT.18.01 97.

What is SSL, TLS and HTTPS?. What is SSL, TLS and HTTPS?. (2021). https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https.

Zeng, B., & Yen, B. (2016). Evaluating User-System Adaptability in the Use of Web-based Information Systems through the Model of Access Efficiency. Pacific Asia Journal Of The Association For Information Systems, 8, 1-16.