THE PHILIPPINE NATIONAL PUBLIC KEY INFRASTRUCTURE IN PAMANTASAN NG LUNGSOD NG MUNTINLUPA TOWARDS DIGITAL SERVICES SECURITY MODEL FOR PUBLIC UNIVERSITIES

MARDYON BUMANLAG YONGSON
https://orcid.org/0000-0002-1305-7570
yongson.mardyon1026@gmail.com
Graduate Program, Philippine Christian University
Manila, Philippines

DOI: https://doi.org/10.54476/ioer-imrj/022761

ABSTRACT

The study explores the integration of the Philippine National Public Key Infrastructure (PNPKI) into the digital services framework of Pamantasan ng Lungsod ng Muntinlupa (PLMun), highlighting the urgent need for enhanced security measures in the academic digital landscape. It aims to evaluate the feasibility of PNPKI incorporation into PLMun's digital services, assess its potential to bolster data security and integrity, and propose a comprehensive security model for public universities utilizing PNPKI. Employing a systematic approach, the research delves into PNPKI's compatibility with existing digital infrastructures and compares it against current security models within educational institutions. Methods may include surveys or interviews for stakeholder feedback. The anticipated findings suggest that PNPKI implementation could significantly improve data security, authentication processes, and digital resilience for PLMun, setting a precedent for similar initiatives in other public universities. This abstract encapsulates the study's objective, methodology, and potential impact, offering valuable insights for policymakers, university administrators, and IT experts in advancing a unified security architecture.

Keywords: Information Technology, Public Key Infrastructure, Digital Services, Security Model

INTRODUCTION

In the modern age of technology, the security of online transactions is a high issue for both consumers and businesses. With the advent of e-governance and digital financial services.

It is vital to secure sensitive information such as e-signatures, and personal and financial data from cyber threats and assaults as described by Rezaei, S., Karami, M., & Nabizadeh, A. (2020). The usage of Public Key Infrastructure (PKI) technology is one technique to improve the security of digital transactions as elaborated by Singh, D., Sharma, N., & Singh, G. (2016). PKI is a system that uses public and private keys to communicate information securely across a network as described by Zheng, S., Wang, Q., & Zhang, Y. (2017). PKI enables secure authentication, encryption, and digital signatures, making it an indispensable tool for safeguarding digital transactions, as elaborated by Ibrahim, N. H., & Aslam, B. (2019). Through the use of PKI

created expressly for payments and financial transactions, as described by Shrivastava, S., & Singh, V. K. (2019), such as the Payment Network Provider Key Infrastructure (PNPKI), in particular, can provide a high level of security for digital financial transactions.

PNPKI use at a state university's digital transformation may provide various strategic advantages. For Pamantasan ng Lungsod ng Muntinlupa (PLMun), it may offer a safe and dependable platform for financial activities such as student tuition fees, wage payments, and vendor payments. PNPKI may increase trust and confidence in the university's financial transactions by protecting the integrity and confidentiality of financial data. Furthermore, PNPKI can safeguard access to digital resources and services such as online courses, research materials, and student data. This can improve students', faculty's, and staff's overall user experience and accessibility to digital services and its usage.

OBJECTIVES OF THE STUDY

The specific objectives of this research can be further specified as follows:

1. To evaluate the level of accuracy and consistency of knowledge and training of PLMun staff.
2. To assess user adoption of the PNPKI in terms of its efficiency and transparency.
3. To identify and analyze any regulatory and legal concerns related to the execution of E.O. 810 and PLMun's use of the PNPKI in terms of data privacy and security.

Conceptual Framework

It emphasizes the potential use of PNPKI in increasing the security and trustworthiness of e-government services. They highlight the significance of a strong and dependable public key infrastructure in boosting the adoption of e-government services, as well as important insights into the design and implementation of such systems.

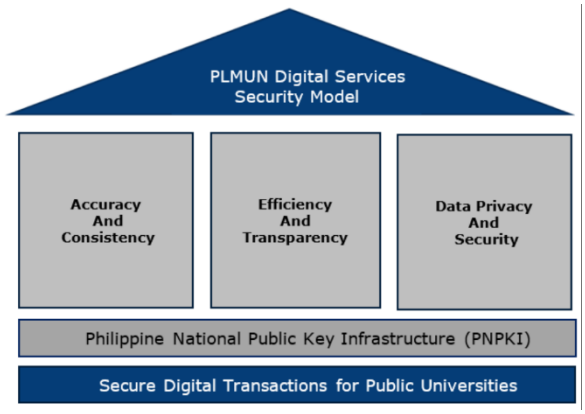

Figure 1. Security Model Framework

METHODOLOGY

The methods and techniques of data collection will include research questionnaires for the evaluation, semi-structured interviews, and focus group discussions.

Survey: To gather data from the sample, a standardized questionnaire will be employed. The poll will be done online, with participants notified through their respective email addresses.

Interviews: Semi-structured interviews with chosen participants will be done to acquire a better understanding of their experiences and viewpoints on the usage of PNPKI.

Focus Group talks: Selected participants will be invited to participate in focus group talks to get insight into the variables affecting PNPKI

uptake as well as the regulatory and legal problems associated with its implementation.

RESULTS AND DISCUSSION

The study gathered information and data through research, interviews, and questionnaires. The study entailed the use of weighted mean and percentage formulas to arrive at the result according to its effectiveness.

1. PNPKI Outcome in terms of Accuracy and Consistency
2. PNPKI Outcome in terms of Efficiency and Transparency
3. PNPKI Outcome in terms of data privacy and security

1. Result of PNPKI Survey

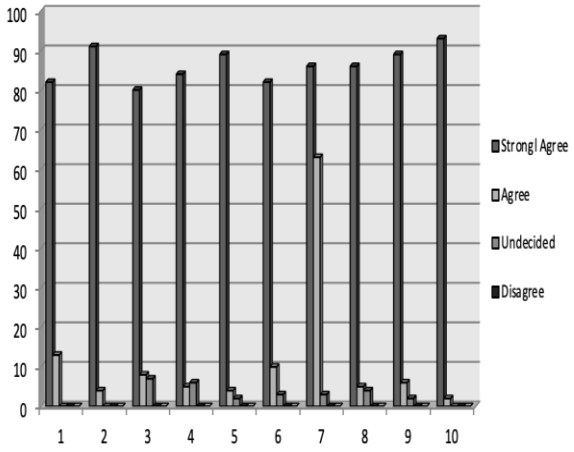

Figure 2. Overall Result of PNPKI Survey

Based on the results, the study found out that the majority of the respondents strongly agreed that the proposed study has met its expected output using different criteria such as; Accuracy, Functionality, Reliability, Efficiency, and Security to evaluate its performance. The study identified the effectiveness of the PNPKI in public universities in providing fast, accurate, and reliable information to its users.

The successful implementation of the PNPKI in PLMun demonstrates its effectiveness in enhancing digital services security in public universities. The adoption of digital certificates has enabled secure communication, protected sensitive information, and facilitated interoperability with external stakeholders.

2. Summary of findings based on the five criteria of the PNKI

Table 1
Summary of findings based on the five criteria of the PNKI

PNPKI Outcome	Average	Status
1. PNPKI Outcome in terms of Accuracy and Consistency		
1.1. The PNPKI provides an accurate response to users' query	4.86	Strongly Agree
1.2. The PNPKI can perform without error	4.96	Strongly Agree
Total:	**4.91**	
1.3 The PNPKI performs it goals and functions with consistency	4.77	Strongly Agree
1.4 The PNPKI handles a wrong input, or it has a consistent validation mechanism	4.82	Strongly Agree
Total:	**4.79**	
2. PNKI Outcome in terms of Efficiency and Transparency		
2.1. The PNPKI provides efficient results based on the user's query	4.92	Strongly Agree
2.2 The PNPKI provides efficient results in terms of speed	4.83	Strongly Agree
Total:	**4.87**	
2.3 The PNPKI provides transparency results	4.87	Strongly Agree
2.4 The PNPKI provides logs for the integrity of the results	4.86	Strongly Agree
Total:	**4.87**	
3. PNPKI Outcome in terms of data privacy and security		
3.1 The PNPKI is highly secure and adheres to data privacy	4.94	Strongly Agree
3.2 The PNPKI has a security mechanism in securing the personal information of its user	4.98	Strongly Agree
Total:	**4.96**	
Average Weighted Mean	**4.88**	**Strongly Agree**

Table 1 shows the summary of findings based on the five criteria of the PNKI with their weighted mean average and interpretation. These criteria include accuracy, consistency, efficiency, transparency, and security of the system

After the survey questionnaire has been tallied, the researchers came up with the total result of the software evaluation based on its criteria. To facilitate the tabulated data, the Lickert scale was used as an instrument to determine the altitude of opinion of the respondents. It contains several declarative statements with a scale after each statement ranging from “Strongly Agree” to “Strongly Disagree”.

CONCLUSIONS

The research on the review of PNPKI and its application in the PLMun for secured digital transactions using the PNPKI can conclude that the use of digital signatures in e-government services can significantly improve security and efficiency in government transactions. The PNPKI provides a safe and dependable public key infrastructure for digital signature authentication and integrity, assuring the authenticity and non-repudiation of digital transactions. PLMun was able to develop a secure digital signature scheme for its internal operations such as registration and enrollment thanks to the PNPKI, leading to a more streamlined and efficient system. However, the successful adoption of digital signatures and the PNPKI need substantial institutional support, capacity building, and stakeholder awareness. It is critical to guarantee that the technological infrastructure, laws, and legislation required to facilitate the implementation of digital signatures and the PNPKI are in place. Furthermore, effective training and education for both government personnel and residents is critical in fostering confidence and encouraging wider usage of e-government services.

Along with enhancing security within PLMUN, the PNPKI integration has made it possible to work and communicate with external stakeholders. The university's overall efficiency and effectiveness in academic and administrative procedures are increased by the standardized digital certificates, which provide secure data sharing and enable smooth communication.

The efficiency of the PNPKI integration is demonstrated by the outcomes, but it is crucial to remember that continual efforts are required to maintain the security of digital services. To keep ahead of new threats and preserve the efficiency of the security model, regular upgrades, training programs, and partnerships with industry experts are essential.

Overall, using PNPKI for safe digital transactions has the potential to greatly improve the efficiency, transparency, and security of government transactions, resulting in improved service delivery and greater citizen trust in government organizations.

RECOMMENDATION

Based on the results and discussion, the following recommendations can be made to further enhance the integration of the Philippine National Public Key Infrastructure (PNPKI) towards a digital services security model for public universities like Pamantasan ng Lungsod ng Muntinlupa (PLMUN):

1. Continuous Security Awareness and Training Programs
2. Regular Evaluation and Updating of Security Awareness
3. Regular Updating of Security Measures
4. Collaboration and Information Sharing
5. Integration of Advanced Security

Technologies
6. Regular Review and Enhancement of Policies and Procedures
7. Research and Development Initiative

By implementing these recommendations, PLMUN can further strengthen the integration of the PNPKI and enhance the digital services security model. This will provide a secure and reliable digital environment for all users, support academic and administrative processes, and protect sensitive information within the university.

REFERENCES

Alghamdi, W. G., Alsayyed, N., & Altuwairqi, A. (2020). Exploring the readiness of government agencies to adopt public key infrastructure in the digital transformation era: A study in Saudi Arabia. *Journal of Information Security and Applications*, 55, 102570.

Al-Harbi, F. A., & Abuhussein, A. A. (2021). An empirical investigation of the factors affecting the adoption of public key infrastructure (PKI) for e-government services in Saudi Arabia. *Journal of Information Security and Applications,* 58, 102782.

Alharthi, M. M., & Al-Amri, A. M. (2019). Examining the factors affecting the adoption of public key infrastructure (PKI) in the digital transformation era: Evidence from Saudi Arabia*. Journal of Theoretical and Applied Information Technology*, 97(16), 4816-4830.

Alsanea, M. A., & Altuwaijri, M. M. (2020). Exploring the adoption of public key infrastructure (PKI) in the context of digital transformation: A case study of Saudi Arabia. International *Journal of Electronic Governance,* 11(3), 292-309.

Alshurideh, M. T., & Abu-Awwad, A. M. (2019). Utilizing Public Key Infrastructure (PKI) for E-Government Services in Jordan: *An Empirical Study. International Journal of Advanced Computer Science and Applications,* 10(1), 355-363. https://doi.org/10.14569/IJACSA.2019.0104050

Abu-Shanab, E., Al-Sharafi, N., & Weerakkody, V. (2020). Investigating the antecedents of trust in e-government services adoption: A case study of Jordan. Information Systems Frontiers, 22(2), 463-477. https://doi.org/10.1007/s10796-019-09953-8

Ali, M. H., & Abdeen, M. A. (2018). Improving public trust and e-government service adoption in Saudi Arabia through national public key infrastructure (NPKI). Journal of Theoretical and Applied Information Technology, 96(24), 8397-8406.

Al-Sharafi, N., Love, R., & Irani, M. (2015). E-government: A strategic operations management perspective. *International Journal of Public Sector Management,* 28(4/5),330-346. https://doi.org/10.1108/IJPSM-09-2014-0147

Arca, R. B. (2019). Evaluating the readiness of the Philippine government for implementing the national public key infrastructure. In Proceedings of the 2019 4th International Conference on Information Management and Processing (pp. 227-231).

Azores, F. G., & Bautista, J. A. (2019). Utilization of Philippine National Public Key Infrastructure (PNPKI) for Secured Digital Transactions in the Public Sector. *International Journal of Computer Science and Information Security,* 17(10), 131-138.

Balogun, A. G., & Falohun, A. S. (2019). Digital signature-based eGovernment system: an assessment of its effectiveness and adoption factors. Heliyon, 5(6), e01855.10.1016/ j.heliyon.2019.e01855

Cabahug, R. P., & Jacildo, G. S. (2019). Towards the adoption of e-signature in the Philippines: A public key infrastructure (PKI) perspective. In Proceedings of the 2019 3rd International Conference on Education and Multimedia Technology (pp. 53-58).

Cao, W., Wu, X., & Tang, X. (2020). A PKI-based secure and efficient data transmission scheme for

mobile cloud computing. *Journal of Systems and Software, 1*64, 110614.

DICT (2018) circular memorandum No. 007: Guidelines on the adoption and use of the Philippine National Public Key Infrastructure (PNPKI) for secure electronic transactions in the government. Retrieved from https://dict.gov.ph/dict-circular-memorandum-no-007-guidelines-on-the-adoption-and-use-of-the-philippine-national-public-key-infrastructure-pnpki-for-secure-electronic-transactions-in-the-government/

Ibrahim, N. H., & Aslam, B. (2019). Digital transactions and the development of electronic commerce in Malaysia. *Journal of Business Research*, 98, 365-375.

Ibrohim, M. N., Sukemi, S., & Murtadlo, M. (2021). Public key infrastructure adoption for e-government service: Perceived ease of use and perceived usefulness perspectives. *Journal of Physics: Conference Series*, 1739(1),

Kesharwani, A., Chauhan, A., & Singh, S. P. (2019). Understanding the factors influencing adoption of e-government services: A case of India. *International Journal of Public Sector Management*, 32(2), 141-160. https://doi.org/10.1108/IJPSM-03-2018-0095

Kim, S. S., & Chun, S. A. (2014). Electronic government adoption: An empirical study of individual and organizational factors. Government Information Quarterly, 31(3), 441-448. https://doi.org/10.1016/j.giq.2014.02.003

Kusuma, H., & Hidayat, R. (2020). National Public Key Infrastructure (NPKI) as a trust model for e-Government services. *Journal of Physics: Conference Series*, 1489(1), 012054

Llobrera, J. D. (2018). Towards a secure and reliable e-government through the use of public key infrastructure in the Philippines. In Proceedings of the 2018 5th International Conference on Industrial Engineering and Applications (pp. 39-42).

Manalo, C. M. (2019). Electronic signatures and public key infrastructure: A review of legal frameworks and implications for the Philippines. In Proceedings of the 2019 4th International Conf. on Computer and Communication Systems (pp. 51-57).

McLaughlin, S., & Polk, W. T. (2004). Public key infrastructure: building trusted applications and web services. John Wiley & Sons.

Mukherjee, A., & Kekre, S. (2014). Analysis of public key infrastructure (PKI) implementation in e-government: A case study of India. *Electronic Government, an International Journal,* 11(4), 338-356. doi: 10.1504/EG.2014.066812

Nengsih, R. N., & Mufidah, N. (2021). Enhancing security in e-government through National Public Key Infrastructure (NPKI). *Journal of Physics: Conference Series,* 1739(1), 012062.

Philippine National Police. (2022). Guidelines and procedures on the application of and utilization of PNKPI for digital certificates of PNP Personnel. Memorandum Circular No.2022-001. https://www.pnp.gov.ph/images/Announcements/2022/mc_2022-001.pdf

Kesharwani, A., Chauhan, A., & Singh, S. P. (2019). Understanding the factors influencing adoption of e-government services: A case of India. *International Journal of Public Sector Management,* 32(2), 141-160. https://doi.org/10.1108/IJPSM-03-2018-0095

Kim, S. S., & Chun, S. A. (2014). Electronic government adoption: An empirical study of individual and organizational factors. Government Information Quarterly, 31(3), 441-448. https://doi.org/10.1016/j.giq.2014.02.003

Kim, T. J., & Chung, Y. J. (2018). An empirical study on the adoption of public key infrastructure (PKI) for e-government services. Sustainability, 10(10), 3705.

Kusuma, H., & Hidayat, R. (2020). National Public Key Infrastructure (NPKI) as a trust model for e-

Government services. Journal of Physics: Conference Series, 1489(1), 012054.

Llobrera, J. D. (2018). Towards a secure and reliable e-government through the use of public key infrastructure in the Philippines. In Proceedings of the 2018 5th International Conference on Industrial Engineering and Applications (pp. 39-42).

Manalo, C. M. (2019). Electronic signatures and public key infrastructure: A review of legal frameworks and implications for the Philippines. In Proceedings of the 2019 4th International Conference on Computer and Communication Systems (pp. 51-57).

McLaughlin, S., & Polk, W. T. (2004). Public key infrastructure: building trusted applications and web services. John Wiley & Sons.

Mukherjee, A., & Kekre, S. (2014). Analysis of public key infrastructure (PKI) implementation in e-government: A case study of India. Electronic Government, an International Journal, 11(4), 338-356. doi: 10.1504/EG.2014.066812

Nengsih, R. N., & Mufidah, N. (2021). Enhancing security in e-government through National Public Key Infrastructure (NPKI). *Journal of Physics: Conference Series,* 1739(1), 012062.

Philippine National Police. (2022). Guidelines and procedures on the application of and utilization of PNKPI for digital certificates of PNP Personnel. Memorandum Circular No.2022-001. https://www.pnp.gov.ph/images/Announcements /2022/mc_2022-001.pdf

Tandiono, S., Susanto, A. B., & Saputra, A. (2020). The effect of security awareness and perceived ease of use on public key infrastructure (PKI) adoption for digital signature in Indonesia. *Journal of Physics: Conference Series, 1*527(1), 012010.

Ugwu, C. I., Ogbu, F. O., & Iwu, C. G. (2020). Electronic government and cybersecurity in developing countries: The case of Nigeria. *Journal of Cybersecurity,* 6(1), taaa001. https://doi.org/10.1093/cybsec/taaa001

Vasiu, R., Stanciu, C. V., & Constantin, F. (2019). The impact of cybersecurity on the e-government system. Sustainability, 11(16), 4298. https://doi.org/10.3390/su11164298

Verma, A., & Sethi, A. (2019). A secure PKI-based key management scheme for smart grid communication networks. Journal of Ambient Intelligence and Humanized Computing, 10(4), 1573-1584.

Villaluna, G. V. (2018). A legal framework for e-commerce in the Philippines: Opportunities and challenges for public key infrastructure. In Proceedings of the 2018 International Conference on Cyberlaw, Cybercrime & Cybersecurity (pp. 144-150).

Wang, R., Wang, H., & Xu, R. (2018). A PKI-based authentication scheme with privacy preservation for VANETs. Wireless Personal Communications, 101(2), 801-817.

Yang, X., Huang, L., & Xu, X. (2019). Analysis of the influential factors of public key infrastructure adoption for e-government services: An empirical study in China. *Journal of Theoretical and Applied Information Technology*, 97(19), 5345-5356.

Zhao, Y., Zhang, Y., & Guo, Y. (2020). A new PKI-based secure messaging scheme for mobile devices. *Journal of Ambient Intelligence and Humanized Computing*, 11(9), 3817-3831.

Zheng, S., Wang, Q., & Zhang, Y. (2017). A PKI-based certificateless signature scheme without bilinear pairing. Journal of Computational and Theoretical Nanoscience, 14(8), 4001-4005.

Zolbahari, A., Osman, S., & Yusuf, L. M. (2019). The impact of public key infrastructure (PKI) adoption on organizational performance in digital transformation. Journal of Theoretical and Applied Information Technology, 97(15), 4271-4284.

AUTHOR'S PROFILE

Mr. Mardyon Yongson, a resident Putatan, Muntinlupa City, has known as an IT Industry Practitioner. He has made several significant contributions to the technology industry. With an extensive background in various roles, including Application Support Analyst and Project Management, Yongson has demonstrated exceptional skills and dedication throughout his career. In addition to his professional achievements, Yongson has actively participated in research endeavors. His notable research project, titled "Towards the Development of Music Mood Classification of Original Pilipino Music (OPM) Songs Based on Audio and Lyrics Keyword" and "Simulated Intelligent Module with Speech Integration and Recognition Interface (SIM - SIRI)," and demonstrates his commitment to exploring innovative solutions. He has enhanced his research writing skills, gained insights into research ethics and culture, and acquired knowledge about data privacy and data security and protection.

COPYRIGHTS