INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY: APPLIED BUSINESS AND EDUCATION RESEARCH
2025, Vol. 6, No. 9, 4719 – 4760
http://dx.doi.org/10.11594/ijmaber.06.09.37

Research Article

# Securing Public Trust Through Blockchain Integration: The Case of the National Police Clearance System in the Philippines

Jhoanna Gracia M. Fabro[1]*, Solitaire M. Reyes[1], Arvin B. Fabro[1], Roque Q. Gelacio[2], Gary A. Reyes[1], Cedric G. Train[1], Yolanda G. Tanigue[1], Alrien F. Dausan[3]

[1]Philippine National Police
[2]United Nations Mission in South Sudan (UNMISS)
[3]De La Salle University – Dasmariñas, Graduate School

*Article history*:
Submission 03 August 2025
Revised 31 August 2025
Accepted 23 September 2025

**Corresponding author:*
E-mail:
jgmfabro@gmail.com

**ABSTRACT**

This study examined the use of blockchain technology in the PNP National Police Clearance System (NPCS) to improve public trust. It first assessed trust in the current Relational Database Management System (RDBMS) based on availability, security, immutability, and transparency. Using an explanatory sequential method, the research surveyed 950 applicants and 175 end-users, and conducted 20 key informant interviews. Findings showed that while the public generally trusts the RDBMS (Availability M=3.25; Security M=3.32; Immutability M=3.29; Transparency M=3.22), they also viewed challenges as serious (Availability M=2.95; Security M=2.83; Immutability M=2.79; Transparency M=2.84). Issues included limited access, weak security, data integrity problems, lack of history logs, and poor control mechanisms. Blockchain technology was recommended as an alternative (Availability M=3.18; Security M=3.23; Immutability M=3.27; Transparency M=3.21). Statistical tests revealed significant differences based on awareness, gender, occupation, application purpose, and location. Regression showed a low dependency of blockchain on RDBMS ($r^2$=0.27), but a moderate correlation between the two (0.52, t=16.75). Overall, the study recommends adopting blockchain in the NPCS to strengthen public trust.

**Keywords**: *Blockchain technology, Philippine National Police, National Police Clearance System, transactional system, availability, security, immutability, transparency, law enforcement, technological determination, relational database management system, explanatory sequential method*

*How to cite:*
Fabro, J. G. M., Reyes, S. M., Fabro, A. B., Gelacio, R. Q., Reyes, G. A., Train, C. G., Tanigue, Y. G., & Dausan, A. F. (2025). Securing Public Trust Through Blockchain Integration: The Case of the National Police Clearance System in the Philippines. *International Journal of Multidisciplinary: Applied Business and Education Research*. *6*(9), 4719 – 4760. doi: 10.11594/ijmaber.06.09.37

## Introduction

As technology enables more sophisticated crimes, the criminal justice system—particularly law enforcement—has increasingly turned to technological tools to keep communities safe (Purdue Global, 2018). Advances in technology have transformed many aspects of policing, allowing agencies to manage and analyze large volumes of data, from criminal records to intelligence reports. However, this reliance on technology has also raised concerns about the security of sensitive police data.

Traditionally, police data was stored in paper files or localized computer systems (McGregor, 2021). With the rise of cloud computing and internet-based storage, these records are now more vulnerable to cyberattacks. Criminals can exploit such vulnerabilities to access personal information, including names, addresses, and criminal histories (The Asia Foundation, 2022).

The Philippine National Police (PNP), as the country's primary law enforcement agency, relies heavily on information systems to identify suspects, trace firearms and vehicles, and review criminal histories. While these systems improve efficiency, they also pose risks to individual privacy and public trust.

Unauthorized access to police data could lead to identity theft, fraud, and compromised investigations.

The PNP's National Police Clearance System (NPCS), for example, faces threats such as hacking, data breaches, and possible tampering of records—issues that can foster bribery, falsification, and corruption. Recent data breach incidents, combined with cases of abuse of power, have further eroded public trust in the institution.

This study centers on securing public trust by enhancing the NPCS. It explores the potential of blockchain technology—a decentralized, tamper- resistant ledger—to strengthen the system's availability, security, immutability, and transparency. Specifically, it examines how blockchain integration can improve police clearance operations, which involve background checks and criminal record verification.

The NPCS currently uses a Relational Database Management System (RDBMS) (https://pnpclearance.ph/), which consolidates data from various PNP databases such as the Case Information and Database Management System (CIDMS), Crime Information, Reporting and Analysis System (CIRAS), e-Rogue Gallery, and Wanted Persons Information System (WPIS) (PNP MC 2018- 020). This study will assess public trust in the existing RDBMS, particularly regarding the protection of personal information submitted to the PNP, and evaluate awareness of its security features.

Blockchain works by recording transactions in blocks linked chronologically through hash functions and timestamps. Once validated by a peer-to-peer network of nodes, the transaction becomes part of an immutable ledger (IBM, n.d.). Applied to the NPCS, blockchain could minimize corruption, improve accountability, and ensure greater transparency, ultimately restoring public confidence in the PNP.

In conclusion, this research aims to demonstrate how blockchain integration can strengthen the PNP's critical processes, enhance transparency and accountability, and contribute to the broader goal of public safety as part of the criminal justice system.

## Theoretical Framework of the Study

Technological determinism suggests that technology drives social change and shapes society by influencing human behavior and social structures (Zaeid, 2016). Zaeid argues that technological innovations have

created new forms of communication and information sharing, transforming the way people work, learn, and interact. In this context, Blockchain Technology (BCT) represents a force that reshapes how organizations manage transactions and data.

For the Philippine National Police (PNP), blockchain offers a secure and decentralized means of storing and managing sensitive records. Its features— decentralization, transparency, immutability, and security—serve as drivers of change, potentially redefining the relationship between citizens and law enforcement. By minimizing tampering, fraud, and corruption, blockchain could strengthen public trust in the National Police Clearance System (NPCS).

Cabugwang, et. al. (2023) proposed blockchain as a solution to improve accountability and efficiency in Philippine government services, highlighting its potential to reduce corruption and fraud. Similarly, Dafoe (2015) emphasized that technological determinism operates in different forms—strong or weak—depending on the extent of influence. He noted that technology creates new opportunities and constraints that shape human behaviour and institutions. In this light, blockchain can be seen as a technological innovation that not only ensures secure transactions but also promotes decentralized governance and new models of digital identity management.

Applied to the PNP, blockchain's integration into the NPCS could trigger profound organizational changes. Enhanced transparency and reduced susceptibility to fraud would not only improve trust in the clearance system but also encourage wider user acceptance. These deterministic effects underscore blockchain's potential to transform data management and verification processes in law enforcement.

## Legal Framework

The Philippines recognizes the importance of Information and Communications Technology (ICT) in national development. President Ferdinand R. Marcos Jr., in his 2022 and 2023 State of the Nation Addresses (SONA), emphasized the role of digitalization in ensuring transparency, improving public service delivery, and combating corruption.

This study is anchored on key legal frameworks governing data protection, cybercrime, and public service efficiency:

Data Privacy Act of 2012 (RA 10173): Protects personal information in both public and private information systems. It requires the PNP, as a data controller, to ensure that data collection, storage, and processing comply with privacy rights and consent provisions.

Cybercrime Prevention Act of 2012 (RA 10175): Criminalizes cyber offenses such as hacking, identity theft, and data breaches. The PNP is mandated to enforce this law, ensuring blockchain adoption aligns with cybersecurity requirements.

Ease of Doing Business and Efficient Government Service Act of 2018 (RA 11032): Aims to streamline government processes and reduce bureaucratic inefficiencies. This law encourages technological innovation, making it relevant for blockchain integration in the NPCS.

In addition, PNP-specific policies reinforce these laws:

PNP Memorandum Circular (MC) 2021-179: Establishes the Privacy Management Program, ensuring compliance with the Data Privacy Act.

PNP MC 2022-049: Provides revised guidelines and procedures for NPCS implementation, serving as the operational foundation for this study.

PNP ICT Master Plan (2022–2025): Known as the PNP S.M.A.R.T. Policing framework, this plan outlines the agency's ICT strategy to support its mission and modernization efforts.

Together, these frameworks provide the legal and institutional basis for integrating blockchain technology into the NPCS. By aligning with national laws and PNP policies, blockchain adoption can improve transparency, strengthen accountability, and contribute to restoring public trust in law enforcement.

## Conceptual Framework of the Study

The conceptual framework visually illustrates the key concepts, variables, and relationships that underpin our study, showcasing the central role of technological determinism and the anticipated impact of blockchain integration on processes structures, people, and organizational culture which surrounds the change in the availability, security, immutability, and transparency of the NPCS in enhancing public trust to the PNP (See figure 1).

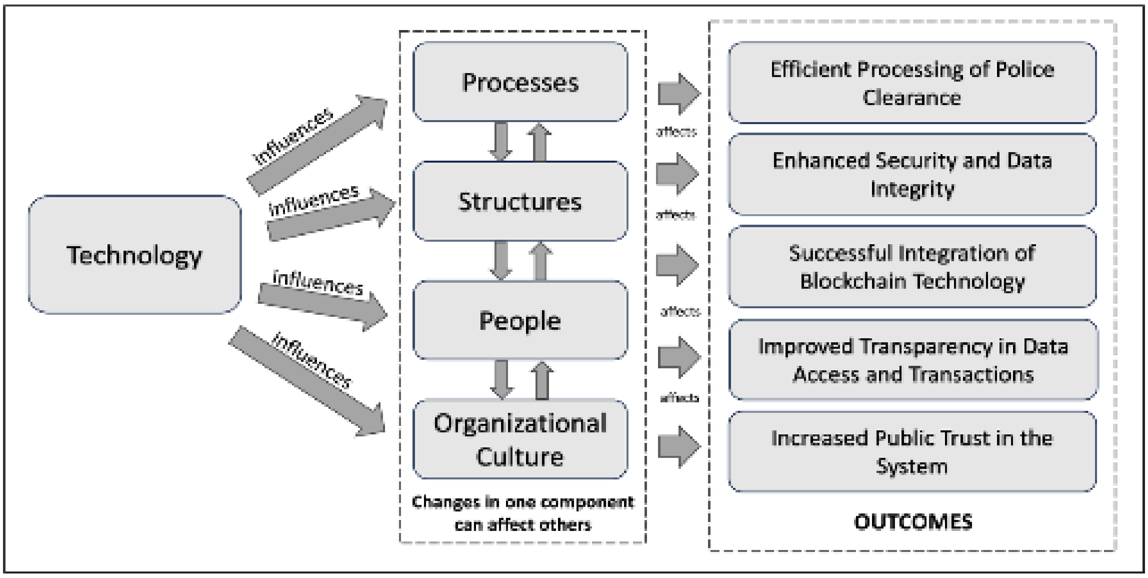

Technology
influences
influences
influences
influences
Processes
Structures
People
Organizational Culture
Changes in one component can affect others
affects
affects
affects
affects
Efficient Processing of Police Clearance
Enhanced Security and Data Integrity
Successful Integration of Blockchain Technology
Improved Transparency in Data Access and Transactions
Increased Public Trust in the System
OUTCOMES

*Figure 1. Conceptual Framework*

## Statement of the Problem

The PNP is currently facing issues related to its transactional system which may erode public trust. In particular, the NPCS is susceptible to various vulnerabilities, including hacking, data breaches, and potential tampering and manipulation of data, leading to concerns about bribery and falsification of records. These identified gaps may have hindered the effectiveness of law enforcement efforts and have placed the safety of citizens at risk.

This study seeks to address the following specific questions:

1. How do participants perceive public trust in the database management system of the PNP NPCS in terms of:
   a. Availability;
   b. Security;
   c. Immutability; and
   d. Transparency?

   From these variables, what issues and challenges are identified in the use of the PNP NPCS?
2. How do the participants perceive the proposal of integrating blockchain technology into the PNP NPCS to enhance public trust?
3. What action plan was formulated to address the issues and concerns identified in the study?

## Hypothesis

H1: There is no significant difference in the assessments of the respondents o the Relational Database Management System of the PNP National Police Clearance System as Securing Public Trust.

H2: There is no significant difference in the assessments of the respondents on the proposal of integrating blockchain technology into the PNP National Police Clearance System to enhance public trust.

H3: There is no significant difference in the assessments on the proposal of integrating blockchain technology into the PNP National Police Clearance System to enhance public trust when end-users are grouped according to profile.

H4: There is no significant difference in the assessments on the proposal of integrating blockchain technology into the PNP National Police Clearance System to enhance public trust when applicants are grouped according to profile.

H5: There is no significant correlation between the RDBMS system of the NCPS and the proposed integration of blockchain in the NCPS.

## Scope and Limitation of the Study

This study focused on assessing the Relational Database Management System (RDBMS) of the Philippine National Police (PNP) National Police Clearance System (NPCS). The evaluation was limited to four key variables: availability, security, immutability, and transparency. A major component of the study was the exploration of blockchain technology integration into the NPCS.

The respondents included applicants of the National Police Clearance and end-users within the National Capital Regional Police Office (NCRPO). In addition, interviews were conducted with system developers, database administrators, and PNP leaders to gather expert insights. The study also considered the experiences of government agencies and private companies that had adopted blockchain technology, as well as perspectives from local and international research and development laboratories and technology partners. The research was carried out in the National Capital Region in 2023.

One limitation of the study was its reliance on self- reported data from PNP personnel and subject matter experts, which may be subject to social desirability bias. Another limitation was the evolving state of blockchain technology, which may require further development and investment before full integration into the NPCS can be realized. Finally, the study's

scope was confined to the PNP, and therefore its findings may not be generalizable to other law enforcement agencies in the Philippines or abroad.

## Research Methodology

This study employs an action research approach, utilizing the explanatory sequential method to investigate "Securing Public Trust through Blockchain Integration: The Case of the National Police Clearance System in the Philippines." The study aimed to analyze both quantitative and qualitative data, focusing on four criteria— availability, security, immutability, and transparency—to understand how blockchain technology could enhance public trust in the National Police Clearance Operations (NPCS).

## Research Design

Quantitative data were analyzed using mean analysis, tests of difference, regression analysis, and correlation analysis. To enrich and contextualize these findings, qualitative data from key informant interviews, observations, and secondary data analysis were integrated. This multifaceted approach allowed a comprehensive assessment of blockchain's potential impact on public trust in NPCS.

Triangulation was employed to ensure the reliability and validity of the findings by cross-verifying data from multiple sources and methods. This approach provided a more holistic and accurate understanding of the research problem.

Data were obtained from both primary and secondary sources to ensure depth and integrity of the study.

## Primary Sources

Surveys: Quantitative data were collected through surveys administered to applicants and end-users across the five districts of the NCRPO. Respondents were asked about their perceptions of the current RDBMS and their expectations regarding blockchain integration. Surveys were conducted online and in- person.

Direct Insights: Firsthand perspectives were gathered from NPCS applicants and end-users to identify specific areas where blockchain could improve system performance, with particular focus on availability, security, immutability, and transparency.

## Secondary Sources

**Interviews:** Qualitative data were obtained through interviews with PNP personnel involved in NPCS operations, exploring experiences with the current RDBMS and expectations for blockchain integration. Additional interviews with experts from government, private sector, and academia provided insights into best practices and innovative approaches for blockchain adoption.

**Observations:** On-site observations of NPCS operations were conducted to understand system workflows and identify areas for potential blockchain enhancement.

**Document and Literature Review:** Secondary data included academic research, policy documents, and reports related to blockchain technology, public trust, and NPCS operations. These resources provided a contextual foundation for interpreting the study's findings.

## Respondents of the Study

The participants of this study were divided into six categories and were selected based on their predetermined roles in the development, successful implementation, and administration of NPCS. Table 1 provided the selection criteria for the participants and respondents to ensure that they had at least comprehension on the topic at hand.

*Table 1. Target Participants with Selection Criteria*

| | | |
|---|---|---|
| Leaders | Decide or influence on the IT direction of their unit or the PNP | Leaders from the DICTM or ITMS or NCRPO |
| Detailed IT Project Officers or<br>IT PNCOs or<br>IT NUPs as End-users | He/she is task to administer and maintain the NPCS | Deployed IT personnel to DIDM whether PCO, PNCO, or NUP |
| Programmer/s<br>Database Administrator/s | He/she is task to develop the system and ensure all needed requirements prior to the implementation and deployment of the system | Programmer/s and Database Administrator/s of the NPCS and other PNP Transactional System related to application of clearances |
| Subject Matter Experts | He/she is an IT expert from government agency, private sector, academe | IT experts in blockchain technology |
| End-users | PNP personnel who uses the NPCS, they directly interact with the system | End-users from the five (5) Districts of NCRPO |
| Applicants | Individuals who use the NPCS to apply for police clearance | Their feedbacks and experiences are important for improving the system and |

## Samples and Sampling Technique

The sampling method that was used in the study was the quota non-probability sampling. The researcher used this method to ensure that the sample represented the diversity of key players in the PNP NPCS with the following sample sizes for each category.

The actual respondents for the survey which used Google forms was 950 applicants and 175 end-users. Their profiles are shown on Appendix G and H, respectively.

It shows that there were more males than female end- user respondents. Most of the respondents were police non-commissioned officers, majority of whom were police corporals.

Majority were processors at 44.75%. Most of the respondents (55) were from Southern Police District of the National Police Region Police Office (NCRPO).

Most had worked in the NCPS from 1 to 3 years. Sixty-four percent (64%) were not familiar or have no prior knowledge about blockchain being used in the PNP.

The profiles of the applicants show that majority were males, aged 35 to 44, had college degrees, had occupations categorized as "others", purpose of application categorized as "others", applied in Manila Police District, and answered "no" if respondent had prior knowledge of blockchain.

Table 2 provided the sampling plan for the study.

*Table 2. Sample Sizes for Each Approaches*

| Data Gathering Approach | Participants | Sample Size | Remarks |
|---|---|---|---|
| Survey Questionnaire | Applicants | 950 | Minimum 100 per District (5 Districts) |
| | End-users | 175 | Minimum 20 per District (5 Districts) |
| Key Informant Interview | Leaders | 7 | Assigned in DICTM/ITMS/NCRPO |
| | End-users | 5 | Assigned/Detailed in DIDM/ITMS/NCRPO |
| | Programmers and Database Administrators | 2 | ITMS Personnel |

## Statistical Tools Used

The following were the statistical tools used in the study:

1. **Mean**. This was employed to get the average of the responses on the perception on the public trust in the database management system of the PNP and the perception on the proposal of integrating blockchain technology in the PNP NPCS.

   The formula for mean is:

$$Xw= \frac{\Sigma Wx}{N}$$

where:

| | | |
|---|---|---|
| Xw | - | weighted mean |
| ΣWx | - | sum of all quantities that follow W |
| | - | weight factor |
| x | - | any score in the distribution N - |
| | | number of cases |

2. **Anova**. The analysis of variance (ANOVA) is a method dividing the variation observed in data into different parts; each part assignable to a known source, cause, or factor. The analysis of variance is used to determine the significance of the difference between the means of a number of different populations. In this study, this was used to test the significant difference in the perceptions of the groups of respondents on the current RDBMS and the proposed blockchain technology for the PNP NPCS. A significant difference means that the groups have different interpretation on each database management system.

   The implication is that, especially for the applicants, the system used in the NPCS must be fully explained to them. This was also used mostly in analysis in the significant differences of respondents in multi-group settings such as rank, district, length of service in NPCS, role in NPCS, education, occupation, and purpose in application of police clearance.

   The formula for ANOVA is:

**SS$_t$** (sums of squares for total variability)

$$SS_t = \Sigma(x_t^2) - \frac{(\Sigma x_t)^2}{N_t}$$

Where:

Σ (x t2) – is the sum of the squares of each group

(Σx t) – is the sum of the scores of each group

Nt – Total Number of cases

**SS$_b$** (sums of squares for between groups variability)

$$SS_b = \frac{(\sum X_1)^2}{N_1} + \frac{(\sum X_2)^2}{N_2} + \frac{(\sum X_3)^2}{N_3} - \frac{(\sum X)^2}{N_t}$$

**SS$_w$** (sums of squares for within group variability)

$$SS_w = SS_t - SS_b$$

**Degrees of Freedom** :

$$Df_b = k\text{-}1 \qquad Df_w = N\text{-} k$$

Where:
K = number of group

Mean Squares

$$MSb = \frac{SSb}{Dfb} \qquad MSw = \frac{SSw}{Dfw}$$

Where:
MSb = mean square between groups
MSw = mean square within groups
Dfb = degree of freedom between
Dfw = degree of freedom within

F - Test

$$F = \frac{MSb}{MSw}$$

F - F-test
MSb - Mean Square Between groups
MSw - Mean Square Within groups

3. **T-test** was used to find out significant differences in the observations of the two sets of respondents. In the study, this was used to test the differences in the perceptions between genders, and whether respondents had knowledge on blockchain or none.

   The formula is:

$$t = X1 - X2$$

Where:
T = t - value
X1 = mean of the first group
X2 = mean of the second group
s1 = standard deviation of the first group
s2 = standard deviation of the second group
n1 = sample size of the first group
n2 = sample size of the second group

4. **Regression and Correlation Analysis**. Regression was used to determine the relationship between one dependent variable and one or more independent variables. A model of relationship is hypothesized and estimated. The parameter values are used to develop an estimated regression equation. Various tests are then employed to see if the model is satisfactory. If the model is satisfactory than regression estimation can be used to determine value of dependent variable through values of independent variables. In the study, regression analysis was used in order to check whether blockchain technology (dependent variable) was dependent on the current relational database management system. Correlation and regression analysis are related to each other as both deal with the estimations of variables values and relationship.

The formula is

Where:
n = sample size
xi, yi = responses from individual sample points
x = sample mean

Correlation coefficient is estimation of linear relationship between two variables. This was used to check whether perception on RDBMS has the same correlate or movement to the perception on blockchain. Values of correlation are always between +1 to -1. +1 value indicates the two values are perfectly relative in positive sense and -1 value means both are perfectly negatively related. And a value of 0 means there is no linear relationship between variables.

The following are the Coefficient of Correlation values and verbal interpretation:

| | |
|---|---|
| 0.01 - 0.20 | Negligible Correlation |
| 0.21 - 0.39 | Low Correlation |
| 0.40 - 0.59 | Moderate Correlation |
| 0.60 - 0.79 | Substantial Correlation |
| 0.80 - 0.89 | High Correlation |
| 0.90 - 0.99 | Very High Correlation |
| 1.00 | Perfect Correlation |

### *Modal Adjectival/Verbal Interpretation*

The techniques for data analysis in the study of the potential of blockchain technology in PNP NPCS includes: 1) descriptive statistics by summarizing and describing data which can help to identify patterns and trends in the data; and 2) content analysis by analyzing documents such as policies, regulations, journals, articles to identify issues and challenges related to the implementation of blockchain technology.

With these data analysis, the result will be able to contribute to the success or failure of blockchain implementation in PNP NPCS.

## Results and Discussions

Public Trust in the Relational Database Management System of the PNP National Police Clearance System.

### *Availability*

Table 3 shows the assessment of the respondents on the RDBMS of the NPCS as securing public trust in terms of availability.

*Table 3 Assessment of the Respondents on the RDBMS of the NPCS as Securing Public Trust in terms of Availability*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | I trust the system to be | 3.26 | SA | 3.34 | SA | **3.30** | **SA** |
| 2 | The NPCS's quick response | 3.29 | SA | 3.35 | SA | **3.32** | **SA** |
| 3 | Downtime of NPCS is rare, | 3.17 | A | 3.02 | A | **3.09** | **A** |
| 4 | I trust the NPCS to keep data | 3.26 | SA | 3.26 | SA | **3.26** | **SA** |
| 5 | Effective NPCS backups make me trust the system's data availability. | 3.32 | SA | 3.27 | SA | **3.29** | **SA** |
| | **Overall Weighted Mean** | **3.26** | **SA** | **3.25** | **A** | **3.25** | **A** |

**Legend:**

| | |
|---|---|
| 3.26 – 4.00 | Strongly Agree (SA) |
| 2.51 – 3.25 | Agree (A) |
| 1.76 – 2.50 | Disagree (D) |
| 1.00 – 1.75 | Strongly Disagree (SD) |

The applicants “strongly agreed” that the RDBMS of the NPCS secures public trust in terms of availability, with an overall weighted mean of 3.26. The highest-rated indicator was “Effective NPCS backups make me trust the system’s data availability” (M=3.32), showing that applicants’ trust is largely influenced by the perceived reliability of the backup system. The lowest-rated indicator was “Downtime of NPCS is rare, which boosts my trust” (M=3.17), indicating that system downtime remains a key concern for applicants when applying for clearance.

For the end-users, the RDBMS was rated as “agree” for enhancing public trust in availability, with an overall mean of 3.25. The highest-rated aspect for end-users was quick response, which received a mean of 3.35, reflecting the importance of system responsiveness in their workflow. Similar to applicants, end-users noted downtime as the main factor reducing public trust, with a mean of 3.02.

Overall, respondents “agreed” that the RDBMS secures public trust in availability, with a grand mean of 3.25. The indicator “the NPCS's quick response makes me more confident” had the highest weighted mean (M=3.32), emphasizing that timely processing and clearance issuance are crucial for trust. Conversely, downtime of the NPCS remained a concern, with the lowest mean of 3.09, highlighting that availability issues could erode public confidence.

The NPCS manages voluminous data that must be readily available for retrieval. Bhoyar (2022) notes that “proper data organization and administration are required for a company to work efficiently. A database management system is simply the storage and management of data in a computer information system. Any organization requires accurate and trustworthy data for better decision-making, data privacy protection, and effective data management" (p. 1). These insights underscore the critical importance of database availability for both operational efficiency and public trust in the NPCS.

### *Interview Results-Availability*

Table 4 shows the interview results and themes pertaining to the aspect of availability in the RDBMS in the NPCS.

The data indicate that the current RDBMS of the PNP is generally accessible, even without blockchain integration. However, two key themes highlighted that the system is not always fully available. First, access is not universal, meaning that only authorized personnel can retrieve data. Second, there are occasional system downtimes, typically occurring once or twice per month. These findings suggest that, while the system is largely operational, its availability is limited both by access controls and periodic technical interruptions.

*Table 4 Interview Results and Themes Pertaining to the Aspect of Availability in the RDBMS in the NPCS*

| Participant No. | Answers | Themes |
|---|---|---|
| 4 | All stations are enabled/ have access to NPCS system | • Accessible system<br>• Not available or accessible to all<br>• Can be available even if not in blockchain<br>• Sometimes the system is down |
| 6 | Di basta-basta pwedeng buksan yan kasi baka ma-violate yung Data | |
| 8 | Importance ng security ng records… Syempre dahil dun tayo kumukuha ng data ng criminal records<br>Pag nagdowntime tayo, kunwari nakaroon ng national disaster, meron tayong makukuha na data | |
| 10 | There are implementations of distributed ledgers that doesn't have necessarily have to be blockchain. | |
| 18 | Regular monitoring of web services to ensure continuous uptime;<br>Implementation of Standard Operating Procedures for ITMS Database Backup and Retrieval Procedure to ensure data is available when needed; and | |

In database management, availability refers not only to the ease of accessing data when needed but also to who is permitted to access it. Shay et. al. (2018) argued that "the enforcer must view the query, the records, or both in traditional view-based database access control. This may be challenging if the enforcer is not permitted to access the database contents or the query itself. Query control is also a suitable fit for implementing rules and regulations that view-based access control does not adequately handle." In the NPCS, this means that while applicant data is available, only personnel with proper access rights can view it.

Blockchain, however, introduces a distinct advantage: each transaction generates a unique block, making it easier to track who accesses specific data. This feature enhances accountability and transparency while maintaining controlled access, addressing one of the limitations observed in the current RDBMS.

### *Analysis*

The quantitative and qualitative findings for availability were consistent. Both approaches indicated that applicant data are generally available when needed for police clearance applications. Quantitative results showed that respondents strongly agreed on the system's availability, while qualitative analysis identified system accessibility as the primary theme. However, downtime emerged as a concern in both datasets: it recorded the lowest mean in the survey and was also highlighted as a negative theme in the qualitative findings.

### *Security*

Table 5 shows the assessment of the respondents on the RDBMS of the NPCS as securing public trust in terms of security.

*Table 5 Assessment of the Respondents on the RDBMS of the NPCS as Securing Public Trust in terms of Security*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | Only authorized persons can | 3.30 | SA | 3.41 | SA | **3.35** | **SA** |
| 2 | Strong passwords and | 3.33 | SA | 3.41 | SA | **3.37** | **SA** |
| 3 | Multi-factor authentication adds security to NPCS login mechanism. | 3.31 | SA | 3.38 | SA | **3.34** | **SA** |
| 4 | I am confident that NPCS data is protected from cyber threats. | 3.28 | SA | 3.31 | SA | **3.30** | **SA** |
| 5 | Data storage of NPCS is ready | 3.25 | A | 3.22 | A | **3.23** | **A** |
| | **Overall Weighted Mean** | **3.29** | **SA** | **3.35** | **SA** | **3.32** | **SA** |

***Legend:***

| | |
|---|---|
| *3.26 – 4.00* | *Strongly Agree (SA)* |
| *2.51 – 3.25* | *Agree (A)* |
| *1.76 – 2.50* | *Disagree (D)* |
| *1.00 – 1.75* | *Strongly Disagree (SD)* |

The applicants strongly agreed that the NPCS is secure, with an overall weighted mean of 3.29. Their trust was primarily driven by the indicator "Strong passwords and encryption keep the data safe" (M=3.33), reflecting confidence in the system's security features. The lowest-rated indicator was "Data storage of NPCS is ready for natural disasters" (M=3.25), indicating some concern about the system's resilience in the event of disasters.

Similarly, end-users strongly agreed on the system's reliability, with an overall mean of 3.35. The highest-rated indicators were "Only authorized persons can access the database" and "Strong passwords and encryption keep the data safe" (both M=3.41). End-users recognized that authentication protocols and password controls restrict access, ensuring system security. Like applicants, end-users gave the lowest rating to disaster preparedness.

Overall, respondents strongly agreed that the RDBMS secures public trust in terms of security, with a grand mean of 3.32. Security was anchored on encryption and access controls, with the indicator "Strong passwords and encryption keep the data safe" scoring the highest (M=3.37). Although there have been attempts to compromise the system, current security measures are perceived as robust. However, both applicants and end-users suggested that simulating the effects of natural disasters on the database infrastructure could further strengthen security, as this indicator received the lowest mean (M=3.23).

Zeb (2018) recommends optimizing encryption by categorizing data as sensitive or insensitive, applying strong encryption to sensitive data while allowing faster access to less critical information. Given that all NPCS data are sensitive, investing in robust encryption is essential. Public confidence in the system can decline if data are perceived as vulnerable to attacks or denial-of-service incidents.

### *Interview Results-Security*

Table 6 shows the interview results and themes pertaining to the aspect of security in the RDBMS in the NPCS.

*Table 6 Interview Results and Themes Pertaining to the Aspect of Security in the RDBMS in the NPCS*

| Participant No. | Answers | Themes |
|---|---|---|
| 2 | The technology will serve it safe and secured, and of course, it is being protected by mechanism | • Presence of security system<br>• Access control |
| 3 | Presence of security features | |
| 8 | External hard drive located in fire-proof cabinet | |
| 19 | The systems has many security measure implemented, one of this is the access control. Only the authorized user has access to the system. A user has also a specific role to the system so he/she has selected module to view depends on his/her role. The system also implemented audit logging. All activity inside the system is logged to track all the user's action. | |
| 20 | Security features are present. | |

Interviews with PNP personnel revealed appreciation for the security features of the current RDBMS. Four participants noted that the system includes essential security measures, and the practice of maintaining backup systems ensures data availability during natural disasters.

While the RDBMS provides security for files and data, it is not without limitations. Encryption in RDBMS is applied invisibly, with data encrypted upon insertion and decrypted upon retrieval. However, this process introduces processing overhead and may reduce system performance (Zeb, 2018). This highlights the need for the PNP to explore more secure and efficient alternatives.

### *Analysis*

Quantitative results corroborated the qualitative findings. Applicants and end-users "strongly agreed"that the system's security is reliable, particularly due to strong passwords and multi-factor authentication, as well as strict access control protocols. Both methods consistently highlighted these aspects as central to trust in the NPCS. A key weakness, however, was system preparedness for natural disasters, which was emphasized in the quantitative results but not as strongly in interviews. This indicates that disaster resilience is an area requiring further attention.

### *Immutability of the RDBMS in the NPC*S

Immutability refers to the assurance that data, once entered into the system, cannot be altered or tampered with, and that any modifications are logged to maintain a clear chain of changes. Both applicants and system administrators expressed confidence in the immutability of the NPCS database. Applicants "strongly agreed" with a grand mean of 3.25 that data integrity is maintained. The highest-rated indicator was "The NPCS prevents unauthorized changes to data" (M=3.30), reflecting trust that unauthorized alterations are unlikely.

The lowest-rated indicator among applicants was "Security measures of NPCS protect data from potential threats" (M=3.26), suggesting that while they trust the system, they are aware that potential external threats exist. Overall, these results indicate that the current RDBMS provides a reasonable level of data integrity, but continued attention to threat prevention is necessary to sustain public trust.

*Table 7 Assessment of the Respondents on the RDBMS of the NPCS as Securing Public Trust in terms of Immutability*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | I trust that NPCS data remains unchanged. | 3.29 | SA | 3.29 | SA | **3.29** | **SA** |
| 2 | The NPCS maintains data integrity and | 3.29 | SA | 3.31 | SA | **3.30** | **SA** |
| 3 | The NPCS prevents immutability | 3.30 | SA | 3.27 | SA | **3.29** | **SA** |
| 4 | The NPCS protects data from unauthorized | 3.27 | SA | 3.30 | SA | **3.28** | **SA** |
| 5 | Security measures of NPCS protect data from potential threats changes to | 3.26 | SA | 3.27 | SA | **3.27** | **SA** |
| | **Overall Weighted Mean** data, malware | **3.28** | **SA** | **3.29** | **SA** | **3.29** | **SA** |

and viruses.

***Legend:***

| | |
|---|---|
| *3.26 – 4.00* | *Strongly Agree (SA)* |
| *2.51 – 3.25* | *Agree (A)* |
| *1.76 – 2.50* | *Disagree (D)* |
| *1.00 – 1.75* | *Strongly Disagree (SD)* |

### *Immutability of the RDBMS in the NPCS*

End-users "strongly agreed" that the immutability of the RDBMS enhances public trust in the NPCS, with an overall weighted mean (OWM) of 3.29. The highest-rated indicator was "The NPCS maintains data integrity and immutability" (M=3.31), highlighting confidence in the system's ability to preserve accurate and unchanged data. The lowest-rated indicators were "The NPCS prevents unauthorized changes to data" and "Security measures of NPCS protect data from potential threats" (both M=3.27), reflecting awareness that the system is not entirely immune to attacks or hacking attempts.

Overall, respondents "strongly agreed" that the RDBMS secures public trust in terms of immutability, with a grand mean of 3.29. Both applicants and end- users trust the system primarily because it maintains data integrity and immutability (M=3.30). While there have been numerous attempts to compromise database systems both locally and internationally, the perception remains that the PNP adequately defends applicant data. However, security measures are not foolproof, as indicated by the lower rating for protection against potential threats (M=3.27).

Rovnyagin et al. (2021) noted that traditional database management systems (DBMS) may experience performance deterioration when storing frequently modified data.

This is relevant to the NPCS, where applicant data may be updated, particularly when a positive "hit" occurs. In contrast, blockchain technology offers true immutability, ensuring that data cannot be altered while avoiding performance degradation, thus providing a potential advantage over the current RDBMS.

### *Interview Findings – Immutability*

Table 8 presents the interview results and emerging themes related to immutability in the RDBMS of the NPCS. The interviews reinforced that end-users value the integrity of the system, emphasizing that data changes are closely monitored and unauthorized modifications are prevented as much as possible.

*Table 8 Interview Results and Themes Pertaining to the Aspect of Immutability in the RDBMS in the NPCS.*

| Participant No. | Answers | Themes |
|---|---|---|
| 8 | "Binaback-up-pan namin even NPCS" | • Data back-up to preserve original data state<br>• Limited changing of external data |
| | "SOP nung back-up ng system. Back-up and retrieval" | |
| 10 | Assured that data is authentic. | |
| 19 | External change pero for specific information lang po for example the birthdate and the name. | |
| | The system only accepts and save data from the user and cannot delete data once saved. We also have a group of people to apply regular back up at least once a week. For its integrity, all actions of all the users | |

### *Immutability of the RDBMS in the NPCS*

The PNP has established systems to protect and back up data, ensuring that changes made by applicants are limited to basic personal information, without affecting criminal record status. Such critical updates are handled exclusively by end-users. Despite these measures, the RDBMS still faces issues related to reversibility or modification of data. For example, an unauthorized change from "cleared" to "with hit" could distort an applicant's record, undermining trust in both the system and the organization. Kulkarni and Sharma (2022) highlighted potential vulnerabilities in non-immutable systems, noting that administrators may grant unnecessary user rights, creating opportunities for misuse or malicious attacks.

Additionally, operating system or software vulnerabilities can give intruders access to sensitive data.

### *Analysis*

The themes of data backup and limited changes were reflected in the highest-rated indicator on immutability— "integrity, immutability, and prevention of unauthorized changes". These findings are closely linked to the security dimension of the NPCS database. However, recent cyberattacks and system breaches have underscored that immutability remains a critical concern that must be addressed. As a result, blockchain technology is being considered to enhance data integrity, prevent unauthorized modifications, and strengthen public trust in the NPCS.

### *Transparency*

Table 9 shows the assessment of the respondents on the RDBMS of the NPCS as securing public trust in terms of transparency.

*Table 9 Assessment of the Respondents on the RDBMS of NPCS as Securing Public Trust in terms of Transparency*

| | Indicators | Appli cants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | I know who access data | 3.16 | A | 3.20 | A | **3.18** | **A** |
| 2 | I understand data access | 3.25 | A | 3.24 | A | **3.25** | **A** |
| 3 | NPCS provides notification about minor “hits” for the applicant. | 3.21 | A | 3.29 | SA | **3.25** | **A** |
| 4 | NPCS provides explanations about minor “hits” for the applicants. | 3.19 | A | 3.29 | SA | **3.24** | **A** |
| 5 | Clearing minor “hits” is | 3.21 | A | 3.17 | A | **3.19** | **A** |
| | **Overall Weighted Mean** | **3.20** | **A** | **3.24** | **A** | **3.22** | **A** |

***Legend:***

| | |
|---|---|
| *3.26 – 4.00* | *Strongly Agree (SA)* |
| *2.51 – 3.25* | *Agree (A)* |
| *1.76 – 2.50* | *Disagree (D)* |
| *1.00 – 1.75* | *Strongly Disagree (SD)* |

### *Transparency of the RDBMS in the NPCS*

Transparency in the NPCS is reflected through data access and the handling of “hits” in applicants’ records. Among the variables, transparency received the lowest overall weighted mean from applicants, 3.20 (“agree”). Applicants recognized the importance of data access controls (M=3.25) but expressed concern over the indicator “I know who accesses data through logs” (M=3.16). This concern arises because inaccurate “hits”—such as records from blotters, warrants of arrest, or security threat classifications— could appear on their profiles, causing undue stress when the hit is not valid.

End-users agreed that the NPCS database system is transparent, with an overall mean of 3.24. The highest- rated indicators were “NPCS provides notification about minor hits for the applicant” and “NPCS provides explanations about minor hits for the applicant” (both M=3.29). End-users ensure that applicants are informed and clarified regarding minor hits. The lowest-rated indicator was “Clearing minor hits is straightforward for applicants” (M=3.17), reflecting the challenge of managing applicant complaints and guiding them through the resolution process.

Overall, respondents “agreed” that the RDBMS secures public trust in terms of transparency, with a grand mean of 3.22. The highest-rated indicators were “I understand data access controls” and “NPCS provides notification about minor hits for the applicant” (both M=3.25). Transparency in the system ensures applicants are aware of their data status and access rules. The main concern remained tracking who accessed the data, as reflected in the lowest-rated indicator “I know who accesses data through logs” (M=3.18). Without comprehensive logging, it is difficult to determine whether applicant data has been compromised or misused by end-users.

Brusca et al. (2018) emphasize that transparency is closely linked to accountability and the fight against corruption. Their study demonstrates that transparent processes can reduce inefficiencies, curb hidden costs, and improve public trust by decreasing opportunities for corruption. In the NPCS, clear access controls and timely communication regarding “hits” contribute to enhanced transparency, reinforcing accountability and public confidence in the system.

### *Interview Results-Transparency*

Table 10 shows the interview results and themes pertaining to the aspect of transparency in the RDBMS in the NPCS.

*Table 10 Interview Results and Themes Pertaining to the Aspect of Transparency in the RDBMS in the NPCS*

| Participant No. | Answers | Themes |
|---|---|---|
| 4 | No feedback if person would have to be arrested | • Police clearance leading to several arrests.<br>• Right information is provided to applicants<br>• Audit trail for data changes |
| 6 | "Yung kumukuha sila ng Police Clearance, marami din tayong makukuha dyan na may warrant" | |
| 8 | To provide them reliable, secured, right information system na dapat nakikita nila | |
| 19 | May audit trail po na ginagamit and visible naman po yung mga transaction na yun only for the others. | |
| | The system gives all the information available clearly for the users. It also has a status monitoring for ever clearance and transaction made by the user. Statistical data or reports are also available for better | |

### *Transparency – Interview Findings*

Participants highlighted that transparency in the clearance system has practical implications beyond information access. For instance, it has enabled law enforcement to act on applicants who appear as suspects. Participant 8 emphasized that applicants are provided with accurate information, and all changes to data are logged through audit trails, ensuring traceability.

The police clearance process is inherently a two-way system. Applicants require the clearance for jobs, education, travel, or other official transactions, while law enforcement benefits from the system in identifying individuals wanted by authorities. Brusca et al. (2018) argue that transparent units generate and share more information than less transparent counterparts, thereby improving operational efficiency.

### *Analysis*

Quantitative findings emphasized notification of "hits" as the main transparency indicator. However, interviews highlighted the law enforcement function, including the potential for arrests based on pending warrants. While applicants have access to certain information, transparency is not an absolute privilege for them; it is also a mechanism for operational effectiveness within the PNP. This underscores that transparency in the NPCS serves both public information purposes and law enforcement objectives, which may occasionally limit applicant awareness of certain actions.

### *Test of Significant Difference in the Assessments of the Respondents on the RDBMS of the NPCS as Securing Public Trust*

Table 11 shows the test of significant difference in the assessments of the respondents on the RDBMS of the NPCS as Securing Public Trust

*Table 11 Test of Significant Difference in the Assessments on the RDBMS of the NPCS as Securing Public Trust between Groups of Respondents.*

| Group | Mean | F-value | F-critical | Decision | Conclusion |
|---|---|---|---|---|---|
| Applicants | 3.26 | 0.15 | 3.85 | Accept Ho. | No significant difference |
| End-Users | 3.28 | | | | |

The hypothesis states that there is no significant difference in how respondents assess the RDBMS of the NPCS in terms of securing public trust.

For all variables combined, the mean score for applicants was 3.26, while for end-users it was 3.28. An ANOVA test yielded an F-value of 0.15, which is lower than the F-critical value of 3.85. This led to the acceptance of the null hypothesis, indicating that there is no significant difference between the assessments of applicants and end-users.

These results suggest that both groups have a similarly high level of agreement regarding the features of the current RDBMS, which is understandable since it is the system currently in use. Dhanbe et al. (2020) noted that electronic systems like the E-Crime Management System can further enhance the functionality of RDBMS by providing efficient online complaint filing and tracking, demonstrating the benefits of well- managed database systems.

## Issues and Challenges Identified in the Use of RDBMS of the NPCS that Affect Public Trust

### *Availability*

Table 12 shows the assessment of the respondents on the issues and challenges identified in the use of the RDBMS of the NPCS that affect public trust in terms of availability.

*Table 12 Assessment of the Respondents on the Issues and Challenges Identified in the Use of the RDBMS of the NPCS that Affect Public Trust in terms of Availability*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | NPCS is not easily accessible. | 3.16 | S | 3.29 | S | **3.22** | **S** |
| 2 | Downtime disrupts my use of | 3.09 | S | 3.00 | S | **3.04** | **S** |
| 3 | Slow data retrieval in NPCS delays processing of application of applicants | 3.06 | S | 3.07 | S | **3.07** | **S** |
| 4 | NPCS is not available during | 2.90 | S | 2.33 | LS | **2.62** | **S** |
| 5 | NPCS backup availability | 2.95 | S | 2.61 | S | **2.78** | **S** |
| | **Overall Weighted Mean** | **3.03** | **S** | **2.86** | **S** | **2.95** | **S** |

***Legend:***

| | |
|---|---|
| *3.26 – 4.00* | *Very Serious* |
| *2.51 – 3.25* | *Serious* |
| *1.76 – 2.50* | *Less Serious* |
| *1.00 – 1.75* | *Not Serious* |

### *Availability Issues in the NPCS RDBMS*

The assessment of the RDBMS of the NPCS revealed notable concerns regarding availability that may affect public trust. Applicants rated the availability of the system as serious, with an overall weighted mean of 3.22. Their primary concern was the difficulty in accessing the NPCS website during the application process, which was reflected in the highest-rated indicator (M=3.16).

Other issues related to availability, such as slow data retrieval, system downtime, and backup readiness, were also rated as serious.

End-users similarly perceived availability issues as significant, with an overall weighted mean of 2.86. They emphasized that the system is not easily accessible (M=3.29), while limited availability during peak hours received a comparatively lower concern (M=2.62). Across both groups, the grand mean of 2.95 indicated a general consensus that access to the system could be improved.

Difficulties in accessing the RDBMS were seen as a source of inefficiency, potentially delaying the processing of applications and affecting public trust. Sharma & Sharma (2019) have highlighted that relational databases often struggle to manage very large datasets, or "big data," which is relevant to the NPCS given the volume of applicant records.

This underscores the need to enhance storage capacity and data retrieval efficiency to ensure uninterrupted availability.

Overall, the findings suggest that while the current RDBMS of the NPCS provides basic levels of availability and security, several challenges persist that may compromise public trust. Addressing these challenges—through system upgrades, enhanced access management, and stronger security measures— would improve the reliability and integrity of the clearance system, ultimately reinforcing confidence in the PNP's operations.

### *Security*

Table 13 shows the assessment of the respondents on the issues and challenges identified in the use of the RDBMS of the NPCS that affect public trust in terms of security.

*Table 13 Assessment of the Respondents on the Issues and Challenges Identified in the Use of the RDBMS of the NPCS that Affect Public Trust in terms of Security*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | Unclear data access rules of | 2.85 | S | 2.34 | LS | **2.60** | **S** |
| 2 | Concerns about password security and data theft in NPCS | 3.09 | S | 2.98 | S | **3.03** | **S** |
| 3 | Lack of higher security measures in NPCS like multi-factor authentication. | 2.97 | S | 2.58 | S | **2.78** | **S** |
| 4 | Data vulnerability to hacking | 3.00 | S | 2.63 | S | **2.81** | **S** |
| 5 | System readiness during | 3.04 | S | 2.85 | S | **2.95** | **S** |
| | **Overall Weighted Mean** | **2.99** | **S** | **2.68** | **S** | **2.83** | **S** |

***Legend:***

| | |
|---|---|
| *3.26 – 4.00* | *Very Serious* |
| *2.51 – 3.25* | *Serious* |
| *1.76 – 2.50* | *Less Serious* |
| *1.00 – 1.75* | *Not Serious* |

### *Security Issues in the NPCS RDBMS*

Applicants expressed serious concerns regarding the security of the RDBMS in the NPCS, with an overall weighted mean of 2.99. Among the indicators, the highest concern was related to password security and potential data theft (M=3.09). Other aspects of security were also viewed as serious issues, indicating that applicants recognize the importance of protecting their personal information.

End-users shared similar concerns, rating security issues with an overall weighted mean of 2.68. They, too, identified password security and data theft as the primary challenge (M=2.98), reflecting the critical role that secure access plays in processing police clearances and maintaining data integrity.

Across all respondents, the grand mean for security issues was 2.83, confirming that security is a serious concern affecting public trust. Key issues identified included:

Password security and potential data theft (M=3.03)

System readiness during natural disasters (M=2.95)

Vulnerability to hacking attempts (M=2.81)

Lack of advanced security measures such as multi-factor authentication (M=2.78)

Unclear rules for data access (M=2.60)

Passwords are a central point of vulnerability since they allow access to individual applicant files and the processing of clearances. Breaches could compromise sensitive data, leading to a loss of public trust. Oesch & Ruoti (2020) note that residual vulnerabilities in password management—such as automated insertion into compromised domains or user-enabled weaknesses—remain a critical challenge.

Overall, while the RDBMS provides basic security measures, these findings indicate a need for stronger protections, better access controls, and enhanced disaster preparedness to safeguard data and maintain public confidence in the NPCS.

### *Immutability*

Table 14 presents the respondents' assessment of issues and challenges in the NPCS RDBMS related to immutability. Applicants rated these issues as serious, with an overall weighted mean of 3.08. Among the concerns, data integrity stood out, as any threat to the accuracy or correctness of applicants' data was considered particularly serious.

*Table 14 Assessment of the Respondents on the Issues and Challenges Identified in the use of the RDBMS of the PNP NPCS that Affect Public Trust in terms of Immutability*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | Data are lost or stolen. | 2.98 | S | 2.38 | LS | **2.68** | **S** |
| 2 | Data are changed and altered | 3.00 | S | 2.51 | S | **2.76** | **S** |
| 3 | Unauthorized data | 2.99 | S | 2.57 | S | **2.78** | **S** |
| 4 | Inadequate security measures | 2.97 | S | 2.53 | S | **2.75** | **S** |
| 5 | Data integrity challenges | 3.08 | S | 2.91 | S | **3.00** | **S** |
| | **Overall Weighted Mean** | **3.01** | **S** | **2.58** | **S** | **2.79** | **S** |

***Legend:***

| | |
|---|---|
| *3.26 – 4.00* | *Very Serious* |
| *2.51 – 3.25* | *Serious* |
| *1.76 – 2.50* | *Less Serious* |
| *1.00 – 1.75* | *Not Serious* |

### *Immutability*

End-users rated the issues in the RDBMS related to immutability lower than the applicants, with an overall weighted mean of 2.58, but still considered them serious.

Like the applicants, their main concern was data integrity, which received a mean of 2.91. The operations of the NPCS rely heavily on accurate data, as any manipulation—such as false "hits" appearing on a clearance—can undermine trust in the system.

Overall, the respondents assessed the immutability issues in the RDBMS as serious, with a grand mean of 2.79. The primary concern remained data integrity challenges, with a mean of 3.00. Other issues were also rated serious: data loss or theft (M=2.68), data being changed or altered over time (M=2.76), unauthorized data modification (M=2.78), and inadequate security measures to prevent data alteration (M=2.75). These findings highlight the risk of data being hacked or manipulated.

Huang et al. (2023) emphasized that database-backed applications handle large volumes of critical data and require high integrity.

To protect data from errors or unauthorized changes, RDBMS often allow developers to enforce integrity constraints. These observations reflect the key immutability challenges in the current NPCS RDBMS.

### *Transparency*

Table 15 shows the assessment of the respondents on the issues and challenges identified in the use of the RDBMS of the NPCS that affect public trust in terms of transparency.

The applicants have as much concern as anyone on who has access on their data in the storage. Asked on the issues and challenges on transparency, they answered that these were serious with an overall weighted mean of 2.99.

They were worried most on "No controls to determine who can access specific data in the system" with a mean of 3.03. If applicants would not know who were accessing their files, chances were that the information of each applicant could be manipulated.

*Table 15 Assessment of the Respondents on the Issues and Challenges Identified in the Use of the RDBMS of the NPCS that Affect Public Trust in terms of Transparency.*

| | **Indicators** | **Appli cants** | | **End-Users** | | **Grand Mean** | |
|---|---|---|---|---|---|---|---|
| | | **WM** | **VI** | **WM** | **VI** | **AWM** | **VI** |
| 1 | No histories to determine who accessed the system | 2.99 | S | 2.77 | S | **2.88** | **S** |
| 2 | No control to determine who can access specific data in the system | 3.03 | S | 2.73 | S | **2.88** | **S** |
| 3 | No mechanism to inform in advance the applicants for minor "hits" | 3.00 | S | 2.70 | S | **2.85** | **S** |
| 4 | No information are given | 2.96 | S | 2.66 | S | **2.81** | **S** |
| 5 | No mechanism available to | 2.98 | S | 2.60 | S | **2.79** | **S** |
| | **Overall Weighted Mean** | **2.99** | **S** | **2.69** | **S** | **2.84** | **S** |

***Legend:***

| | |
|---|---|
| *3.26 – 4.00* | *Very Serious* |
| *2.51 – 3.25* | *Serious* |
| *1.76 – 2.50* | *Less Serious* |
| *1.00 – 1.75* | *Not Serious* |

### *Transparency*

End-users, who have direct access to the NPCS data, rated the issues in transparency lower than applicants, with an overall weighted mean of 2.69, but still considered them serious. Their main concern was "no histories to determine who accessed the system" (M=2.77), as this lack of audit trails could allow unauthorized alterations without accountability. All other transparency-related indicators were also rated as serious.

Overall, the respondents assessed transparency issues in the RDBMS as serious, with a grand mean of 2.84. The top concerns were "no histories to determine who accessed the system" and "no controls to determine who can access specific data", both with a mean of 2.88. These gaps in access history and controls imply potential risks of data being altered or deleted by unauthorized personnel.

Qiu et al. (2020) highlighted that, especially with the increasing use of IoT, ineffective access control can lead to security breaches. Proper access control mechanisms are essential to monitor resource activity and ensure that only authorized users access sensitive information under legal conditions.

### Test of Significant Difference on the Assessments of the Respondents on the Issues and Challenges Identified in the Use of the RDBMS of the NPCS that Affect Public Trust

Table 16 shows the test of significant difference in the assessments of the respondents on the issues and challenges Identified in the use of the RDBMS of the NPCS as securing public trust.

*Table 16 Test of Significant Difference in the Assessments of the Respondents on the Issues and Challenges Identified in the Use of the RDBMS of the NPCS that Affect Public Trust.*

| Group | Mean | F-value | F-critical | Decision | Conclusion |
|---|---|---|---|---|---|
| Applicants | 3.00 | 30.64 | | Reject Ho. | With |
| End-Users | 2.70 | 3.85 | | | significant difference |

The data indicates that applicants rated the issues and challenges in using the RDBMS of the NPCS at 3.00, while end-users rated them lower at 2.70. The F-value of 30.64, which exceeds the F-critical value of 3.85, led to the rejection of the hypothesis. This shows that there is a significant difference in how applicants and end-users perceive the issues and challenges affecting public trust in the system.

These results suggest that applicants experience more serious challenges when applying for police clearance, particularly regarding availability, security, immutability, and transparency. In contrast, end-users, who operate the system rather than receive the output, are less affected by these issues.

This significant difference aligns with the observations of Stonebraker et al. (2018), who argued that contemporary RDBMSs, often based on decades-old legacy code, are not optimized for modern demands. Applicants' trust issues may reflect the limitations of these traditional systems, highlighting the need for specialized, updated solutions to address current challenges.

### Perception of the Respondents on the Proposal of Integrating Blockchain Technology into the NPCS to Enhance Public Trust

#### *Availability*

Table 17 shows the perception of the respondents on the proposal of integrating blockchain technology into the NPCS to enhance public trust in terms of availability.

*Table 17 Perception of the Respondents on the Proposal of Integrating Blockchain Technology into the NPCS to Enhance Public Trust in terms of Availability*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | Data can be accessed from | 2.98 | R | 2.76 | R | **2.87** | **R** |
| 2 | One can monitor the changes in the status of data processing. | 3.20 | R | 3.10 | R | **3.15** | **R** |
| 3 | Has a back-up system that when one peer goes down, the other still works. | 3.27 | HR | 3.21 | R | **3.24** | **R** |
| 4 | Protects the accuracy and | 3.32 | HR | 3.33 | HR | **3.32** | **HR** |
| 5 | Correcting data errors is safe | 3.32 | HR | 3.33 | HR | **3.32** | **HR** |
| | **Overall Weighted Mean** | **3.22** | **R** | **3.15** | **R** | **3.18** | **R** |

***Legend:***

| | | |
|---|---|---|
| *3.26 – 4.00* | *Highly Recommended* | *(HR)* |
| *2.51 – 3.25* | *Recommended* | *(R)* |
| *1.76 – 2.50* | *Less Recommended* | *(LR)* |
| *1.00 – 1.75* | *Not Recommended* | *(NR)* |

The respondents recommended the integration of blockchain technology into the National Police Clearance System (NPCS) to enhance availability. The applicants rated it highly, with an overall weighted mean of 3.22, and identified the most important benefits as protecting the accuracy and completeness of data and ensuring that correcting data errors is safe and secure (both with means of 3.32). They also highlighted blockchain's ability to maintain continuous service through a peer backup system, where if one node fails, others continue to operate (mean = 3.32).

End-users provided similar responses, with an overall weighted mean of 3.15. Like the applicants, they highly recommended blockchain for its ability to protect data integrity and securely correct errors (means = 3.33).

Overall, the respondents rated the adoption of blockchain for availability as recommended, with a grand mean of 3.18. The key advantages noted were data accuracy, secure error correction, and monitoring of data processing changes (mean = 3.15–3.32). Blockchain's decentralized structure also allows data to be stored across multiple nodes, ensuring continuity even if one node fails (mean = 3.24).

However, the indicator "data can be accessed from different decentralized nodes" received the lowest score, with an average weighted mean of 2.87. End-users rated this aspect lowest at 2.76, while applicants rated it 2.98.

This may reflect unfamiliarity with blockchain features, or concerns about allowing access outside the designated office, since the current system only allows access within the NPCS office.

Blockchain's capability to correct errors and maintain secure data is supported by Liu et al. (2022), who proposed a secure distributed storage method using bilinear pairing and BLS-HLA (BLS-Homomorphic Linear Authenticator).

This system allows clients to verify uploaded data, locate errors, and manage data dynamics efficiently, with a low false-positive rate, demonstrating blockchain's reliability and security.

### *Interview Results- Blockchain Availability*

Table 18 shows the interview results and themes pertaining to the aspect of availability in the Integration of Blockchain Technology in the NPCS.

Blockchain is welcomed by police officers as this technology can improve police operations. However, questions arise on the fitness of the system and need for the system in the NPCS.

Moreover, there is that question of learning for the personnel to use and adopt the system.

Participant 18, however, provided the merits of using blockchain making data easy to retrieve. As explained in Liu, et. al. (2022), upon receiving the checking request, the edge server retrieves the corresponding data tag and verify its validity using the public key of the signature.

This aspect is one of the major reasons why this study pushes for the use of blockchain in the National Police Clearance System.

*Table 18 Interview Results and Themes Pertaining to the Aspect of Availability in the Integration of Blockchain Technology for the NPCS*

| Participant No. | Answers | Themes |
|---|---|---|
| 3 | Technology makes our work faster | • Work improvement |
| 7 | Technology must fit with the organization | |
| 9 | You bring technology sa implementation ng everything para umunlad ang process ng bawat opisina. | • Fitness and need |
| | Since this technology is not yet adopted by the PNP, though already used widely in different industries and private sectors, our programmers will need to undergo training to learn how to utilize blockchain effectively. | • Expertise of personnel<br>• Ease of access of files |
| 10 | You need to ask yourself to really identify whether your scenario is fit for blockchain. | |
| 12 | If you want to improve the storage of your drive | |

| | |
|---|---|
| 13 | In availability since, it is running in Cloud, usually like yung samin it's running on Azure sa cloud-based. Kapag cloud po kase, mas available sya kasi hindi sya mag-accumulate ng computing power. Para kang may Google drive. Actually pag may kailangan kang file, huhugutin mo lang ida-download mo lang. Whereas kapag nasa laptop mo, bubuksan mo pa laptop mo, diba ganun, so mas ano mas matagal. So sa availability yun. |
| 14 | It goes without saying that it is more conveniently available in geographical terms in contrast to on-premise databases. Ang tanong talaga palagi is what its difference to cloud storage is. Blockchain is a distributed ledger technology which means decentralized. |

### Analysis

The quantitative results highlighted the benefit of blockchain in protecting the data, and the process of correcting errors in data. The qualitative themes exhibited that blockchain can contribute to work improvement, ease of file access, it fits the need of the organization, and requirement of expertise of personnel. The resulting data were complementary in explaining how blockchain can make data available not only to the end users but also to the applicants.

Hence, all the positive points provided in the quantitative and qualitative results are complementary.

### Security

Table 19 shows the perception of the respondents on the proposal of integrating blockchain technology into the NPCS to enhance public trust in terms of security.

The security aspect of the blockchain system for the NPCS was "recommended" by the applicants as the overall weighted mean is 3.24. What they appreciated most were the indicators on "the blockchains themselves are strong features for data security" and "multi-factor authentication is highly used" both with means of 3.27 or highly recommended. All other indicators were assessed as "recommended." One of the issues of the applicants in clearance application has been the security of their information stored by the current database system of the PNP. The applicants, based on the data, showed a high level of understanding of blockchain's security.

*Table 19 Perception of the Respondents on the Proposal of Integrating Blockchain Technology into the NPCS to Enhance Public Trust in terms of Security*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | Unauthorized access can be | 3.25 | R | 3.20 | R | **3.22** | **R** |
| 2 | The blockchains themselves are strong features for data security. | 3.27 | HR | 3.26 | HR | **3.27** | **HR** |
| 3 | Multi-factor authentication is | 3.27 | HR | 3.29 | HR | **3.28** | **HR** |
| 4 | Even if the data storage is breached, the other peers can blockchains. | 3.22 | R | 3.19 | R | **3.21** | **R** |
| 5 | Blockchain technology can | 3.21 | R | 3.15 | R | **3.18** | **R** |
| | **Overall Weighted Mean** | **3.24** | **R** | **3.22** | **R** | **3.23** | **R** |

| | | | |
|---|---|---|---|
| ***Legend:*** | *3.26 – 4.00* | *Highly Recommended* | *(HR)* |
| | *2.51 – 3.25* | *Recommended* | *(R)* |
| | *1.76 – 2.50* | *Less Recommended* | *(LR)* |
| | *1.00 – 1.75* | *Not Recommended* | *(NR)* |

The respondents also recommended the integration of blockchain technology into the NPCS to enhance security. The applicants gave it an overall weighted mean of 3.22, highlighting multi-factor authentication as the most valued feature (mean = 3.29, highly recommended). Another highly recommended aspect was that the blockchain itself is a strong feature for data security (mean = 3.26).

End-users, responsible for safeguarding client data, shared similar views, emphasizing the importance of any feature that strengthens security. Overall, the respondents rated blockchain security as recommended, with a grand mean of 3.23.

The most appreciated security feature was multi-factor authentication (mean = 3.28), which makes it difficult for hackers to infiltrate the system, as multiple authentication steps—including hash codes—are required before access is granted. The inherent strength of blockchains was also valued (mean = 3.27), as breaking the chain is extremely difficult, and multiple authentication layers further reinforce security.

Additional advantages of blockchain security included:
Detection of unauthorized access (mean = 3.22)
Data accessibility even if one node is breached (mean = 3.21)
Resilience against natural risks (mean = 3.18)

These features allow data to remain secure and accessible even if part of the system is compromised.

The findings align with Zhang et al. (2022), who emphasized that multi-factor authentication protocols—combining PINs, passwords, hardware tokens, and biometrics—provide strong security, particularly for IoT and other systems that require both device independence and human-device interaction.

### *Interview Results- Blockchain Security*

Table 20 shows the interview results and themes pertaining to the aspect of security in the Integration of Blockchain Technology in the NPCS.

*Table 20 Interview Results and Themes Pertaining to the Aspect of Security in the Integration of Blockchain Technology for the NPCS*

| Participant No. | Answers | Themes |
|---|---|---|
| 5 | Ayaw naman natin na malaman ng iba pa ang personal data | • Objective to secure personal data<br>• Makes changes secured due to further documentation in other nodes<br>• Use of data through permission<br>• Super vault system |
| 7 | Strengthened security by adding one more layer | |
| 9 | Think of blockchain as a super-secure vault for our citizens' personal data. It keeps everything locked away from prying eyes, so we can assure everyone that their information is safe from any unauthorized access or hacking attempts. | |
| 12 | You add another block for the correction. So sinong makapagtago nyan kasi ang mangyayari nyan pati yung mali nya nakarecord na so madali mong mahuli talaga. | |

The main objective of blockchain technology is to provide an additional layer of security for protecting applicants' personal data. According to the qualitative data, making changes in the system is difficult because blockchain nodes record every input, including mistakes. Since security is a key concern in the PNP, blockchain offers a more secure solution for data protection.

Stephen & Alex (2020) explain that blockchain is decentralized and can address various operational challenges. Each transaction is encrypted and linked to previous records, while algorithms on the nodes validate transactions, preventing a single entity from initiating changes. Blockchain also supports transparency, allowing participants to view transactions in real time. Additionally, smart contracts provide secure, automated transactions, reducing the risk of third-party interference. Platforms like Ethereum enable the execution of these smart contracts in a decentralized environment

### *Analysis*

Strong security and high authentication level were the keywords for blockchain technology in the quantitative part. The themes were security and super vault system. All of these aspects are part of the CIA triad of computer security or the confidentiality, integrity and availability. The security feature of the “super-vault” like blockchain technology highly influences the next factor which is immutability.

### *Immutability*

Table 21 shows the perception of the respondents on the proposal of integrating blockchain technology into the NPCS to enhance public trust in terms of immutability.

The applicants highly recommended the use of blockchain for immutability, giving it an overall weighted mean of 3.27. They rated the feature “data integrity and reliability are maintained” the highest at 3.31, showing that blockchain can address concerns about data being destroyed or altered. Another highly recommended feature was “data are kept accurate” with a mean of 3.30.

The end-users also highly recommended blockchain integration for immutability, with the same overall mean of 3.27. They particularly valued “data are kept accurate” (3.31) and “if one peer is infected by virus or malware, the other peers remain unaffected” (3.29).

Overall, blockchain was highly recommended for immutability with a grand mean of 3.27, the highest among all four variables assessed. Both applicants and end-users emphasized the need for a system that protects data from changes or corruption. Other notable features, interpreted as “recommended” but still highly rated, included “it is highly improbable to hack the data in the blockchain” and “denial of service in one peer does not affect the other peers”, both with a mean above 3.23.

Blockchain provides strong guarantees of immutability. Landerreche & Stevens (2018) highlighted that Bitcoin’s proof-of-work consensus makes rewriting prior blocks nearly impossible unless an attacker controls the majority of the network’s hashing power, giving an exponentially small chance of success the deeper the block. This demonstrates how blockchain can preserve data integrity and reliability for the NPCS.

*Table 21 Perception of the Respondents on the Proposal of Integrating Blockchain Technology into the NPCS to Enhance Public Trust in terms of Immutability*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | Data are kept accurate. | 3.30 | HR | 3.31 | HR | **3.30** | **HR** |
| 2 | Data integrity and reliability | 3.31 | HR | 3.32 | HR | **3.31** | **HR** |
| 3 | It is highly improbable to hack the data in the blockchain. | 3.24 | R | 3.25 | R | **3.24** | **R** |
| 4 | If one peer is infected by virus or malware, the other peers remain unaffected. | 3.25 | R | 3.29 | HR | **3.27** | **HR** |
| 5 | Denial of service in one peer does not necessarily affect the other peers. | 3.25 | R | 3.20 | R | **3.23** | **R** |
| | **Overall Weighted Mean** | **3.27** | **HR** | **3.27** | **HR** | **3.27** | **HR** |

***Legend:***

| | | |
|---|---|---|
| *3.26 – 4.00* | *Highly Recommended* | *(HR)* |
| *2.51 – 3.25* | *Recommended* | *(R)* |
| *1.76 – 2.50* | *Less Recommended* | *(LR)* |
| *1.00 – 1.75* | *Not Recommended* | *(NR)* |

***Interview Results-Blockchain Immutability***

Table 22 shows the interview results and themes pertaining to the aspect of immutability in the Integration of Blockchain Technology in the NPCS.

One of the main reasons for the push in adopting blockchain technology is in the immutability of data or data cannot be easily changed without multiple node updates. As expressed in the interviews, the tokens are unique which means that it is hard to fake the police clearances. Moreover, the token system requires less space which can ease the problem of storage.

One of the features of blockchain is multiple validation before changes can be made on data. Blockchain is a distributed ledger technology that is immutable and encrypted. While it was designed for and is most usually associated with cryptocurrency, there are a growing variety of applications, McBee & Wilcox (2020).

*Table 22 Interview Results and Themes Pertaining to the Aspect of Immutability in the Integration of Blockchain Technology for the NPCS*

| Participants | Answers | Themes |
|---|---|---|
| 9 | Once something goes into the blockchain, it's like carving it in stone. No one can sneak in and change or erase anything. This means the records we keep are rock-solid, reducing the chances of any funny business happening with our clearance records. | **• Unique token issued/ generated to applicants.**<br>**• Creates better storage security**<br>**• Decentralization**<br>**• Multiple areas of validation** |
| 10 | Promote government transparency and enhance accountability due to its immutable ledger. For example, it can be used for transparent tracking of government spending. It may also address fraudulent transactions. | |
| 11 | Blockchains, may identification siya for saan ba siyang storage and what kind of files. | |
| 12 | It really takes a lot of maturity bago ka mag decentralized, kaya sabi ko we can start the storage the moment pag okay na sila sa storage system | |
| 13 | When you are in the chain, it is really immutable kasi it takes a village to…di ba? Ang blockchain kailangan lahat informed. Certain information is really valid about you. It’s a big issue, so immutable yun kasi lahat na nagsabi na ikaw yun e diba? Otherwise, it will not push through. | |
| 14 | Immutability is part and parcel of blockchain technology. Block data cannot be changed. It can be buried under clutter by adding transactions on top of each other, but the trail remains. | |
| 15 | Decentralization and immutability | |
| 16 | We are not trusting single source of truth we are the whole system kasi each of the govt agencies in this example yung tatlo would have copy of their own and can validate each. | |

| | |
|---|---|
| 20 | Decentralization and immutability<br>The integration of blockchain technology into the National Police Clearance System ay importante, especially in preserving the integrity of data. Hindi lang nya pinapalakas yun security lalo pa it ensures the availability of crucial information, maintains the immutability of records, enhances transparency, and ultimately fosters public trust sa PNP. |

### *Analysis*

Accuracy, integrity, and reliability were the keywords for blockchain technology in the quantitative part. Themes were uniqueness, security, decentralization and multiple areas of validation. All of these aspects are part of the CIA triad of computer security or the confidentiality, integrity and availability. The immutability feature of blockchain technology highly influences the proposal for its adoption. In blockchain, "confidentiality ensures that information is kept confidential. For example, confidentiality is important in the PNP, where only officers with clearance can access classified information. Integrity is making sure that no one tampers with an information system. In blockchain technology, data are hardly changed", Sadiku, et. al. (2017).

### *Transparency*

Table 23 shows the perception of the respondents on the proposal of integrating blockchain technology into the NPCS to enhance public trust in terms of transparency.

*Table 23 Perception of the Respondents on the Proposal of Integrating Blockchain Technology into the NPCS to Enhance Public Trust in terms of Transparency*

| | Indicators | Applicants | | End-Users | | Grand Mean | |
|---|---|---|---|---|---|---|---|
| | | WM | VI | WM | VI | AWM | VI |
| 1 | Public ledger allows all participants to access and transactional records. | 3.21 | R | 3.16 | R | **3.18** | **R** |
| 2 | Once data is added, it cannot | 3.23 | R | 3.17 | R | **3.20** | **R** |
| 3 | Lack of reliance on a central authority which reduces the risk of manipulation. | 3.25 | R | 3.17 | R | **3.21** | **R** |
| 4 | Users can track the complete | 3.25 | R | 3.30 | HR | **3.28** | **HR** |
| 5 | Consensus mechanisms to validate transactions collectively. | 3.28 | HR | 3.30 | HR | **3.29** | **HR** |
| | **Overall Weighted Mean** | **3.24** | **R** | **3.22** | **R** | **3.23** | **R** |

***Legend:***

| | | |
|---|---|---|
| *3.26 – 4.00* | *Highly Recommended* | *(HR)* |
| *2.51 – 3.25* | *Recommended* | *(R)* |
| *1.76 – 2.50* | *Less Recommended* | *(LR)* |
| *1.00 – 1.75* | *Not Recommended* | *(NR)* |

The applicants recommended blockchain technology for enhancing transparency in the NPCS, with an overall weighted mean of 3.24. The top-rated feature was "consensus mechanisms to validate transactions collectively" (3.28), showing their appreciation for the collective validation process.

Similarly, the end-users also recommended blockchain for transparency, with an overall mean of 3.22. They highlighted "users can track the complete history of transactions" and "consensus mechanisms to validate transactions collectively" as highly recommended features, both rated 3.30.

Overall, blockchain was recommended for transparency with a grand mean of 3.23. The highest-rated indicator was "consensus mechanisms to validate transactions collectively" (3.29), followed closely by "complete history of transactions" (3.28). These features ensure that any data changes require multiple validations, unlike the current RDBMS, and that all transaction records are traceable.

Other highly rated features include "lack of reliance on a central authority, reducing the risk of manipulation" (3.21), "once data is added, it cannot be easily changed or deleted" (3.20), and "public ledger allows all participants to access transaction records" (3.18).

However, participants noted that blockchain may not suit data that must remain private. Hellani et al. (2021) explained that while blockchain offers full transparency across systems, some users avoid it due to confidentiality concerns.

### *Interview Results-Blockchain Transparency*

Table 24 shows the interview results and themes pertaining to the aspect of immutability in the Integration of Blockchain Technology in the NPCS.

Blockchain technology is meant to make transactions with the PNP, specifically on police clearance, more transparent. These are enhanced by blockchain as it can make others change data and verify the changes through the nodes. However, one of the issues is making blockchain known and acceptable to the public. In the government, blockchain can help in the drive for transparency.

Batubara, et. al. (2019) identified key issues where accountability and transparency can be had such as in digital ID, privacy, interoperability, connectivity and technology aware population, computational efficiency and storage size, acceptability, check and control mechanism, data validity, digital signature, algorithm transparency, law and regulation support, and dispute resolution, that must be considered in developing a transparent and accountable blockchain-based e-Government system.

### *Analysis*

Transparency in the quantitative aspects was highlighted on complete changes history in the documents and consensus for changes. Transparency, validation and accountability were the main themes on the qualitative aspect. Hence, the results for both methods were consistent.

*Table 24 Interview Results and Themes Pertaining to the Aspect of Transparency in the Integration of Blockchain Technology for the NPCS*

| Participant No. | Answers | Themes |
|---|---|---|
| 4 | Informs the person on the "hits" | • Transparency on police records<br>• Access by third party or applicant<br>• Validation by anyone in the nodes.<br>• Public knowledge on what blockchain is<br>• Providing accountability |
| 7 | Transaction sa users and system is yung third party. | |
| 9 | Blockchain is often compared to a glass house, allowing authorized users to see what's happening inside. This transparency is a great way to build trust because people can double-check their records and understand how everything works behind the scenes. In the rare instance when the integrity of the system is being questioned, the blockchain's unchangeable nature can serve as a record of truth and provide a clear audit trail to address such concerns. | |
| 10 | If you think about evidence management system you have the police you have the department of justice, you have the supreme court so several institutions are sharing or using the data probably updating the data so that maybe a candidate for blockchain. | |
| 13 | But if you're dealing with public finance like let's | |

| | |
|---|---|
| | say in my end, this is where it differentiate my used case to yours. Kasi in my used case we're on the transparency kasi we want the people to know how the public funds are being spent. And this is precisely the reason why we are doing the blockchain projects because it's not just for the Courts to see but also for public to use this information na they're immutable, we can rely on these documents to provide. |
| 14 | Aside from every change to data being logged and unchangeable, blockchain as a DLT means that all authorized users have synchronous access to the same data across different locations, making it easier to monitor as opposed to manual reconciliation and providing greater transparency. |
| 15 | Blockchain is to meant to create a system that can be validated by everyone that can be publicly available, |
| 16 | Most people don't know what blockchain is for them it's just word that means bitcoin or Ethereum or |

## Test of Significant Difference on the Perception of the Respondents on the Proposal of Integrating Blockchain Technology into the NPCS to Enhance Public Trust

Table 25 shows the analysis of variance of the assessments of the respondents on the proposal of integrating blockchain technology into the NPCS to enhance public trust.

*Table 25 Test of Significant Difference in the Assessments of the Respondents on the Proposal of Integrating Blockchain Technology into the NPCS to Enhance Public Trust*

| Group | Mean | F-value | F-critical | Decision | Conclusion |
|---|---|---|---|---|---|
| Applicants | 3.24 | 0.98 | 3.85 | Accept Ho. | No significant difference |
| End-Users | 3.20 | | | | |

The null hypothesis is that there is no significant difference in the assessments of the respondents on the proposal of integrating blockchain technology into the NPCS to enhance public trust.

The endorsement of the applicants to the integration of the blockchain technology in the NCPS is at 3.24 or recommended. The end-users also recommended it at 3.20. The difference of the two means was not significant as the F-value was only 0.98, while the critical F-value was 3.85. This led to the acceptance of the null hypothesis and leading to the conclusion that there was no significant difference in the assessments of the respondents on the proposal of integrating blockchain technology into the NPCS to enhance public trust.

This result implies that the applicants, as well as the end-users, have understood and have trusted to endorse the integration of blockchain technology for the police clearance system in the PNP.

Bhawana, et. al. (2022) showed that the centralized system has drawbacks, such as single point of failure, trust, transparency, and data integrity. Therefore, the edge computing server and blockchain come into the picture to overcome such problems. The edge computing server resides close to the IoT devices to provide high bandwidth, fast computing, scalability, data storage, and efficiently manage numerous IoT devices.

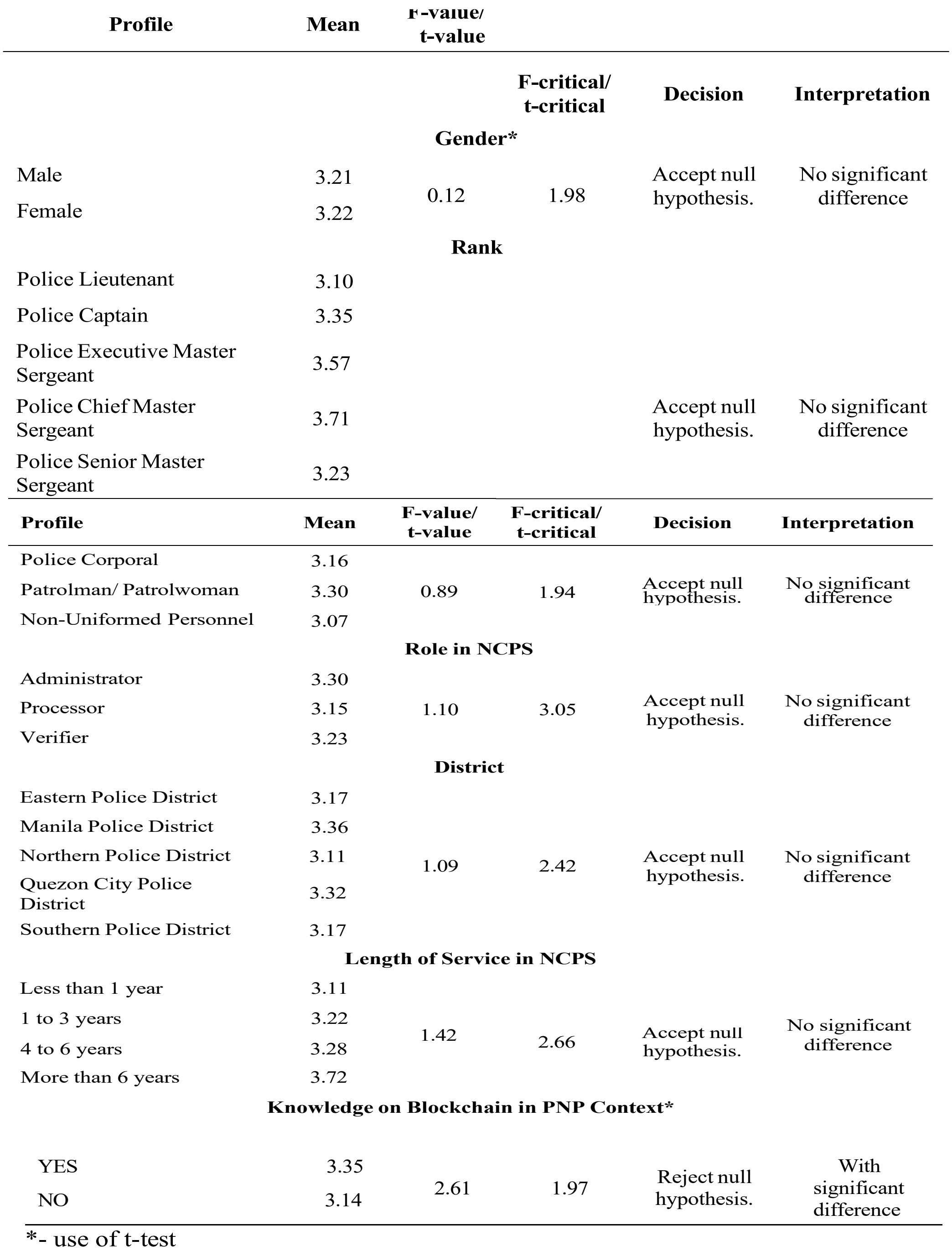
The blockchain adds distributed trust and transparency through a distributed ledger and consensus protocol.

### Test of Significant Difference in the Assessments on the Proposal of Integrating Blockchain Technology into the PNP NPCS to Enhance Public Trust when Grouped According to Profile

#### *End-Users*

Table 26 shows the test of significant difference in the assessments on the proposal of integrating blockchain technology into the NPCS to enhance public trust when end-users are grouped according to profile.

*Table 26 Test of Significant Difference in the Assessments of the Applicants on the Proposal of Integrating Blockchain Technology into the NPCS to Enhance Public Trust when End-Users are Grouped According to Profile*



| Profile | Mean | F-value/<br>t-value | F-critical/<br>t-critical | Decision | Interpretation |
|---|---|---|---|---|---|
| **Gender*** | | | | | |
| Male | 3.21 | 0.12 | 1.98 | Accept null hypothesis. | No significant difference |
| Female | 3.22 | | | | |
| **Rank** | | | | | |
| Police Lieutenant | 3.10 | | | | |
| Police Captain | 3.35 | | | | |
| Police Executive Master Sergeant | 3.57 | | | | |
| Police Chief Master Sergeant | 3.71 | | | Accept null hypothesis. | No significant difference |
| Police Senior Master Sergeant | 3.23 | | | | |
| Police Corporal | 3.16 | | | | |
| Patrolman/ Patrolwoman | 3.30 | 0.89 | 1.94 | Accept null hypothesis. | No significant difference |
| Non-Uniformed Personnel | 3.07 | | | | |
| **Role in NCPS** | | | | | |
| Administrator | 3.30 | | | | |
| Processor | 3.15 | 1.10 | 3.05 | Accept null hypothesis. | No significant difference |
| Verifier | 3.23 | | | | |
| **District** | | | | | |
| Eastern Police District | 3.17 | | | | |
| Manila Police District | 3.36 | | | | |
| Northern Police District | 3.11 | 1.09 | 2.42 | Accept null hypothesis. | No significant difference |
| Quezon City Police District | 3.32 | | | | |
| Southern Police District | 3.17 | | | | |
| **Length of Service in NCPS** | | | | | |
| Less than 1 year | 3.11 | | | | |
| 1 to 3 years | 3.22 | 1.42 | 2.66 | Accept null hypothesis. | No significant difference |
| 4 to 6 years | 3.28 | | | | |
| More than 6 years | 3.72 | | | | |
| **Knowledge on Blockchain in PNP Context*** | | | | | |
| YES | 3.35 | 2.61 | 1.97 | Reject null hypothesis. | With significant difference |
| NO | 3.14 | | | | |

*- use of t-test

The null hypothesis is that there is no significant difference in the assessments on the proposal of integrating blockchain technology into the NPCS to enhance public trust when end-users are grouped according to profile.

As shown on the data, differences in the means when end-users were categorized into gender, rank, role in the NCPS, district, and length of service in the NCPS yielded "no significant difference" as the F-values or t-values were lower than their critical values.

Therefore, there is no significant difference in the assessments on the proposal of integrating blockchain technology into the NPCS to enhance public trust when end-users are grouped according to gender, rank, role in the NCPS, district, and length of service in the NCPS.

However, when end-users were categorized on their knowledge on blockchain technology in the PNP context, the null hypothesis was rejected as the t-value of 2.61 was higher than the critical t-value of 1.97.

This led to the rejection of the null hypothesis. Therefore, there was a significant difference in the assessments on the proposal of integrating blockchain technology into the NPCS to enhance public trust when end-users are grouped according their knowledge on blockchain technology in the PNP context.

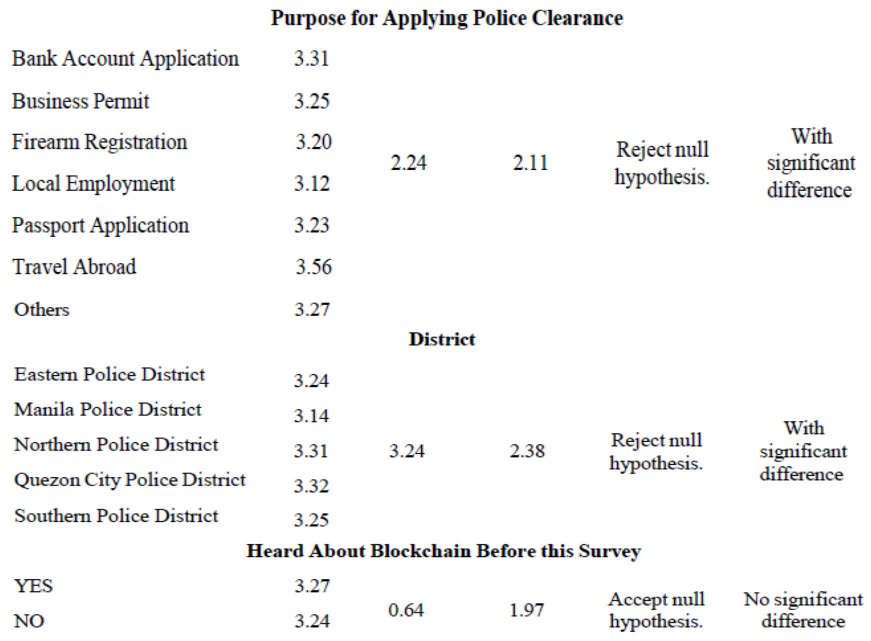
The impact of this finding is that before the blockchain will be introduced in PNP, the end-users unfamiliar with blockchain must be given orientation first. This is related to technological determinism as new technologies, in order to be effective in the society organization, must be learnt by the users.

There are also issues that must be overcome for blockchain to be fully accepted in the system. "Blockchain information and services are vulnerable to manipulation by hackers or foreign governments, and personal data are not always private.

As blockchain expands in multiple areas and domains, security challenges become critical considerations in deciding the viability of the blockchain economy" Pink, et. al. (2018).

*Table 27 Test of Significant Difference in the Assessments of the Applicants on the Proposal of Integrating Blockchain Technology into the NPCS to Enhance Public Trust when Applicants are Grouped According to Profile*

| Profile | Mean | F-value/ t-value | F-critical/ t-critical | Decision | Interpretation |
|---|---|---|---|---|---|
| | | **Gender** | | | |
| Male | 3.21 | 2.57 | 1.96 | Reject null hypothesis. | With significant difference |
| Female | 3.31 | | | | |
| | | **Age** | | | |
| 18 to 24 | 3.28 | 0.62 | 2.22 | Accept null hypothesis. | No significant difference |
| 25 to 34 | 3.26 | | | | |
| 35 to 44 | 3.23 | | | | |
| 45 to 54 | 3.17 | | | | |
| 55 to 64 | 3.36 | | | | |
| 65 and over | 3.18 | | | | |
| | | **Education** | | | |
| Elementary | 3.25 | 0.52 | 2.22 | Accept null hypothesis. | No significant difference |
| High School | 3.23 | | | | |
| College | 3.26 | | | | |
| Doctor's Degree | 3.00 | | | | |
| Master's Degree | 3.24 | | | | |
| Vocational | 3.13 | | | | |
| | | **Occupation** | | | |
| Businessmen | 3.44 | 4.82 | 2.22 | Reject null hypothesis. | With significant difference |
| Government Employees | 3.18 | | | | |
| Overseas Workers | 3.43 | | | | |
| Private Employees | 3.37 | | | | |
| Self-Employed | 3.06 | | | | |
| Others | 3.26 | | | | |



| | | | | | |
|---|---|---|---|---|---|
| **Purpose for Applying Police Clearance** | | | | | |
| Bank Account Application | 3.31 | 2.24 | 2.11 | Reject null hypothesis. | With significant difference |
| Business Permit | 3.25 | | | | |
| Firearm Registration | 3.20 | | | | |
| Local Employment | 3.12 | | | | |
| Passport Application | 3.23 | | | | |
| Travel Abroad | 3.56 | | | | |
| Others | 3.27 | | | | |
| **District** | | | | | |
| Eastern Police District | 3.24 | 3.24 | 2.38 | Reject null hypothesis. | With significant difference |
| Manila Police District | 3.14 | | | | |
| Northern Police District | 3.31 | | | | |
| Quezon City Police District | 3.32 | | | | |
| Southern Police District | 3.25 | | | | |
| **Heard About Blockchain Before this Survey** | | | | | |
| YES | 3.27 | 0.64 | 1.97 | Accept null hypothesis. | No significant difference |
| NO | 3.24 | | | | |

The test of significant difference revealed varying results when applicants were grouped according to profile. The profiles on age (t=0.62), education (F=0.52), and heard about blockchain before this survey (t=0.64) yielded lower t-values or F-values. Therefore, there was no significant difference in the assessments on the proposal of integrating blockchain technology into the NPCS to enhance public trust when applicants are grouped according to age, education, and heard about blockchain before this survey.

However, significant differences were found when respondents were grouped according to gender (t=2.57), occupation (F=4.82), purpose (F=2.24), and district (F=3.24). As the F-values were greater than the critical, the null hypotheses were rejected. Therefore, there was a significant difference in the assessments on the proposal of integrating blockchain technology into the NPCS to enhance public trust when applicants are grouped according to gender, profession, purpose, and district.

### Post-hoc analyses yielded the following:

For occupation, the government employees (M=3.18) and the self-employed (M=3.06) had means interpreted as "recommended" while the rest are "strongly recommended." Further t-test grouping the government and self-employed (M=3.16) and the other occupations (M=3.31) yielded a t-value of 4.01 (t-critical=1.96). This finding showed that there is some hesitancy on the government employees and the self- employed to use blockchain.

For purpose of application of police clearance, the groups with lower scores were those in "firearm registration" (M=3.20), and "local employment" (M=3.12). Grouping the two (M=3.14) against the grouping of the other "purposes" (M=3.28) yielded significant difference (t=2.96; t-critical= 1.97). This finding showed that those registering firearms and immediately looking for local employment might not have appreciated much the value of blockchain. In fact, blockchain expedites application for police clearance for local employment. However, those registering firearms might be hesitant with the technology, especially when they have violations like expired licenses or hiding from criminal records.

For the district, the lowest was Manila Police District (M=3.14 or recommended) while the rest of the Police Districts have "highly recommended" interpretations. The analysis is that proposing blockchain must take into consideration the technological capacities of each Police District. Some city governments have been investing more in technology than others.

These differences can be compared to the study of Shin (2019). “Blockchain is gaining traction in a variety of application cases across a wide range of sectors. Firms are boosting their blockchain investments in order to revolutionize how they deliver products and services, gain new insights for a competitive advantage, and improve their financial and operational performance. Because blockchain ledger records are secure, customer information, as well as company and transaction records, are becoming more secure as they become sequential and immutable. Ironically, such a trust-based method is blockchain's weakest link” (p. 2). The significant differences showed that some participants are not fully trusting yet to the benefits of blockchain technology, and may be more concerned on the security issues.

## Regression Analysis and Correlation Between the Use of the RDBMS in the NPCS and the Proposed Integration of the Blockchain Technology

### *Regression Analysis*

Table 28 shows the regression results between the use of the RDBMS in the NPCS and the proposed integration of the blockchain technology.

*Table 28 Regression Results between the Use of the RDBMS in the NPCS and the Proposed Integration of the Blockchain Technology*

| Factors | Mean | r2 | F-value | p-value |
|---|---|---|---|---|
| RDBMS | 3.26 | 0.27 | 413.96 | 0.001 |
| Blockchain | 3.24 | | | |

The test was done to check if blockchain technology (dependent variable) is dependent on the current database system. The results of the regression shows an r- square of 0.27 or low level of dependency. Therefore, the blockchain technology can proceed without much dependence on the previous system. The only significant issue is the migration of the current data from RDBMS to blockchain; hence, there is still that low level (0.27) of dependence of the new technology to the old one.

There are practical and theoretical implication of these results. The adoption of blockchain can render RDBMS technology passe. Technology acceptance theories and models were developed as a framework to investigate how users understand and accept new technologies, how they might use them, and what the consequences of continuing to use them are. The practical usage of any information system is implicitly dependent on the presence of a desire to use it. However, the continuing of utilizing the information system is contingent on two beliefs: First, the information system must be approved by the users. Then, after adoption, users' contentment with the system determines whether they continue to use the system. In the organizational context, this entails continuing to increase investment in information technology (Momani, 2020).

### *Correlation Analysis*

Table 29 shows the correlation results between the use of the RDMS in the NPCS and the proposed integration of the blockchain technology.

*Table 29 Correlation Results between the Use of the RDBMS in the NPCS and the Proposed Integration of the Blockchain Technology*

| Factors | Mean | Multiple r | t-value | Decision | Interpretation |
|---|---|---|---|---|---|
| RDBMS | 3.26 | 0.52 | 16.75 | Reject Ho. | Significant correlatio |
| Blockchain | 3.24 | | | | |

**Level of significance=0.05**

| | |
|---|---|
| 0.01 - 0.20 | Negligible Correlation |
| 0.21 - 0.39 | Low Correlation |
| 0.40 - 0.59 | Moderate Correlation |
| 0.60 - 0.79 | Substantial Correlation |
| 0.80 - 0.89 | High Correlation |
| 0.90- 0.99 | Very High Correlation |
| 1.00 | Perfect Correlation |

This test is done to check how does the perception of blockchain is correlated by the perception on RDBMS.

The results show that the correlation between RDBMS (M=3.26) and blockchain (M=3.24) is "moderate" as the correlation coefficient is 0.52. However, low the correlation is, they still pose significant correlation.

The interpretation is that the only moderate correlation meant that blockchain could prove to be much more different than the current RDBMS being used. Stated otherwise, the use of blockchain in the PNP will be a big leap away from the current RDBMS. If the correlation was high, it would be difficult to transition from RDBMS to blockchain because that would be having "substitute" systems. In that case, the incentive to change will be low because what the PNP will be getting will almost be the same.

Martin (2023) provided one of the best arguments for blockchain use. While both blockchains and relational databases are useful tools for storing information that supports critical business activities, they excel in different ways. When it comes to providing a robust, fault-tolerant mechanism to store critical data, blockchains have a clear edge.

### *Implications to the PNP Organization*

Whether the system for the NPCS was RDBMS or Blockchain Technology, what matters most is that the public trusts the transactions in the PNP. As bases for the implications, the following were the public trust ideas shared by the participants during the interview.

*Table 30 Interview Results and Themes Pertaining to Securing Public Trust in the NPCS*

| Participant No. | Answers | Themes |
|---|---|---|
| 1 | Yung public trust talaga, it's all about discipline. You cannot give them trust kung medyo may problema tayo sa kapulisan. | • Reliability of the system to protect data.<br>• Respecting privacy.<br>• Protecting police and civilians through technology.<br>• Trust on digital technology<br>• Authentic technology emanates trust. |
| 4 | Lesser corruption due to non-engagement (in clearance application) | |
| 5 | Individual privacy ng bawat tao ay maproteksyonan. | |
| 6 | Iniiwasan natin yung mga tinatawag na harassment on civilian side through technology.<br>Kaya din protektahan ng technology ang ating mga pulis | |
| 7 | Removing doubts from the public using technology that protects identity of individuals | |
| 9 | Kailangan pinagkakatiwalaan nila tayo dun sa kanilang binibigay na data. | |
| 10 | There should trust also in the digitalized public services, it's important because if the citizens cannot trust the platform the services of government they won't use it; so, it's counter-productive to the vision of digital transformation. | |

| | |
|---|---|
| 15 | Blockchain is meant to create a system that can be validated by everyone that can be publicly available. Yun mga tao will be able to or they can rely on the data that we are storin on the blockchain system. |
| 16 | It (blockchain) does promote trust and it is a system that helps each node to trust each other. |
| 17 | This is authentic, this is transparent diba? For me kasi pag nakita ng mga tao na authentic yun, kung she become person matatakot ka na e. Pero kung legitimate ka na ano, you really want to provide service to the public, mas ma-encourage ka pa e na magparticipate into the process of bidding or whatever diba. |

Based on the ideas provided, the option to integrate new technology in the digital services of the PNP must rely on certain criteria like: reliability on data protection, upholding privacy rights of the applicants, inclusion of the police as protected party in digitization, and overall trust to the system due to its authentic nature.

Yavaprabhas (2022) claimed that to solve trust concerns, the public has begun to embrace technology-based, trust-building solutions, such as blockchain technology. Blockchain is thought to have the promising potential to dramatically transform government transactions into a trustworthy ecosystem of exchange due to its ability to improve information authenticity and transparency.

### *Tactical/Operational*

The study's tactical enhancements for the NPCS focus on practical improvements derived from quantitative analysis and interview themes:

- Reliable Database Storage: Strengthening the system's foundation by ensuring dependable storage for data.
- Security Enhancement: Implementing measures to prevent data attacks and fortify the overall security framework of NPCS.
- Transparency on Data Access: Introducing measures for increased transparency in accessing and managing data.

### *Strategic/Managerial*

The strategic and managerial implications endorses the integration of blockchain technology in the NPCS, emphasizing key focal points:

- Increased Public Trust: Through blockchain integration, it will instill confidence in the public by ensuring transparency and accountability in police transactions.
- Enhanced Security and Data Integrity: By utilizing blockchain, we will be able to fortify the security of data, addressing vulnerabilities and ensuring the integrity of information.
- Improved Transparency: Leveraging blockchain's inherent transparency to enhance the visibility of data access and transaction processes.
- Efficient Processing of Police Clearances: Streamlining transaction processes, leveraging blockchain's efficiency to ensure quick and error-resistant processing of national police clearances.
- Successful Integration of Blockchain Technology: Advocate for the seamless integration of blockchain technology, positioning the NPCS as a pioneer in adopting innovative solutions in the PNP.

In summary, the tactical enhancements focus on immediate improvements, while the strategic recommendations advocate for a holistic adoption of blockchain technology, aligning with overarching goals of public trust, security, transparency, efficiency, and successful technological integration.

## Conclusions

1. The existing RDBMS used in the NPCS enjoys a certain level of public trust due to its data backup practices, robust password and en-

cryption standards, data integrity maintenance, and transparent data access controls. However, several vulnerabilities have surfaced, including system downtime, concerns about data safety during natural disasters, doubts regarding its ability to shield data from potential threats, and a lack of transparency regarding data access.

The utilization of the RDBMS in the NPCS is beset with significant issues and challenges. These encompass difficulties in system accessibility, worries regarding password security and data theft, struggles to maintain data integrity, the absence of historical logs on system access, and a lack of control mechanisms to monitor data access.

2. The endorsement of blockchain technology for integration into the NPCS is grounded in its ability to safeguard data accuracy and completeness, provide a secure mechanism for rectifying data errors, offer multi-factor authentication, uphold data integrity and reliability, and ensure a unanimous mechanism for validating transactions and their alterations.
   a. Safeguarding data accuracy and completeness: Blockchain's distributed ledger ensures that once data is recorded, it cannot be easily altered or deleted, enhancing the accuracy and completeness of stored information.
   b. Providing a secure mechanism for rectifying data errors: Blockchain allows for the secure correction of data errors through a consensus mechanism, ensuring that only authorized users can make changes and that changes are transparent and auditable.
   c. Offering multi-factor authentication: Blockchain systems can incorporate robust authentication methods, such as multi-factor authentication, to enhance security and verify the identity of users.
   d. Upholding data integrity and reliability: Blockchain's immutability and transparency mechanisms contribute to maintaining data integrity and reliability, as all transactions are recorded in a tamper-resistant manner.
   e. Ensuring a unanimous mechanism for validating transactions and their alterations: Blockchain relies on consensus algorithms to validate and agree on transactions, ensuring unanimity among network participants regarding the state of the data.
3. The proposed action plan to implement blockchain technology in NPCS, with the aim of bolstering public trust, is substantiated by its features that promise easy access, robust security through multi-factor authentication, data integrity mechanisms, and transparency in maintaining historical records, logs, and consensus mechanisms.

## Recommendations

This study recommends to pilot test the migration of SQL of the PNP NPCS to Blockchain Technology. The ITMS may consider piloting experimental setups for blockchain technology within its internal transactions. This will allow the organization to assess the feasibility and effectiveness of blockchain for public transactions and build confidence in its capabilities.

This study also recommends the following:

*Forge Partnership:* Collaborate with academic institutions and private companies experienced in blockchain technology. Partnering with academia will provide access to research and expertise, while private sector collaboration can offer practical guidance and potential pilot projects.

*Create a Blockchain Development Team:* Create a dedicated blockchain development team consisting of experts in system architecture, development, and security. Ensure the team receives adequate training, resources, and access to infrastructure for effective blockchain integration.

*Public Awareness Campaign:* Launch an information campaign to build and reinforce public trust. Educate the public about data protection, threat prevention, and transparent data access, emphasizing the PNP's commitment to safeguarding their information.

*Enhanced Data Protection:* Invest in a robust anti-virus and malware system to bolster data security measures, addressing concerns about data integrity and protection. Comprehensive Blockchain Adoption

*Proposal:* The PNP should justify and propose the adoption of blockchain technology for a significant portion of the entirety of its transactions. Emphasize the benefits of efficiency, effectiveness, and the enhancement of public trust as driving factors for this transition.

## THE ACTION PLAN

## *"Implementation Strategy: Building Trust through Blockchain in National Police Clearance Operations"*

### I. *Rationale and Inten*t

The current NPCS relies on traditional database system, which has been facing issues on data availability, security, immutability, and transparency that may have eroded public trust. These issues include occasional but prolonged system outages, problems with storing data, security concerns, and a lack of transparency in tracking who access public data.

These are called issues of trust in the technology and in the system. Technology is trusted when it provides the output required of it. The system (NPCS) is trusted if it provides accurate records for the applicants and more importantly to the PNP.

The adoption of blockchain is inherently based on the concept of trust. The degree to which people trust the services, transactions, and organizations underpinning blockchains becomes increasingly important as they evolve. When users interact with blockchains, they expect to obtain the items they paid for and to have their data protected. While it is evident that trust is important in digital environments, there is confusion about what trust is, how it works/can be built, and what genuinely defines digital trust.

In blockchain, digital trust is a type of user heuristic. Blockchain users are likely to cope with perceived danger, security, privacy, and overload by employing cognitive heuristics that reduce cognitive effort and time. As cognitive heuristics, digital trust constitutes information processing strategies for making conclusions more quickly and with less effort than more sophisticated ways, reducing cognitive load during security assessment (Shin, 2019).

To address these challenges and ensure trust, we propose adopting blockchain technology for PNP transactions, specifically, the NPCS. Blockchain is a new way of storing and managing data. It works by creating a chain of data blocks, where each block contains information, a timestamp, and a link to the previous block. When a transaction occurs in the system, a new block is created, and this transaction is verified by a network of computers (nodes) within the blockchain network. Once verified, the transaction is added to the blockchain as a secure and unchangeable record (IBM, n.d.).

While blockchain technology is relatively new, it offers several advantages over the traditional RDBMS, particularly, in terms of availability, security, immutability, and transparency. One of the practical implications of blockchain technology is that it removes some barriers to the application process.

The blockchain technology can use financial technology applications for the payment of fees. The process creates another block that will verify that the transaction had occurred. Although some of these processes may be observed in many database management system now, blockchain is more practical and secured especially in the verification of transactions or the concept of immutability where one cannot change the data without approval from different sources.

### *II. Action Plan*

This action plan presents a seven-month strategy to integrate blockchain into the National Police Clearance System (NPCS). It aims to strengthen public trust, improve security, ensure transparency, and streamline clearance processing. The plan details outcomes, strategies, actions, timelines, responsibilities, resources, and monitoring measures to guide effective implementation.

*Action Plan Summary*

| Outcomes | Strategies and Actions | Timeline | Responsibility | Resource Requirements | Monitoring Procedure |
|---|---|---|---|---|---|
| 1. Increased public trust in the system;<br>2. Enhanced security and data integrity in the National Police Clearance System;<br>3. Improved transparency in data access and transactions;<br>4. Efficient processing of police clearances; and<br>5. Successful integration of blockchain technology. | General Framework of the Migration of SQL to Blockchain Technology<br>- *9 Business Processes (Assessment and Planning, Data Modelling, Data Migration, Testing, Deployment and Integration, User Training and Adoption, Monitoring and Maintenance, Data Consistency and Synchronization, Gradual Transition)*<br>- Uses People, Process, Technology Model<br>Specific Framework of the Migration of SQL to Blockchain Technology<br>It will use Agile Programming | 7 Month Project<br>March 2024 to September 2024<br>Assumptions:<br>1. ITMS have already created an ITMS Blockchain Team prior to the project implementation<br>2. ITMS Blockchain team have already finished a 3-month training program<br>3. Forge Partnership with the Academe and Industry with Use Case<br>4. Have already finished procurement of the project | Project Sponsor (DICTM in collaboration with DIDM)<br>Steering Committee (senior executives of the PNP Directorates, other Unit involved)<br>Technical Working Group (ITMS, CES, DRD)<br>Project Management Team (ITMS)<br>Secretariat (DICTM, ITMS, CES)<br>Consultants (external from the academe, industry with use cases) | Proposed Budget: 35,000,000.00<br>Personnel<br>Equipment<br>Training and Education<br>Materials and Supplies<br>Physical Space<br>Consultants | Monitoring and Evaluation<br>Monitoring and Reporting (reviews)<br>Risk Management Plan (roles, registers, monitoring and review)<br>Evaluation Plan (progress) |

## References

Abrogar, S. (April 19, 2023). Over 1M records from NBI, PNP, other agencies leaked in massive data breach. Retrieved from https://newsinfo.inquirer.net/1758456/over-1-million-records-from-nbi-pnp-other-agencies-leaked-in-huge-data-breach

AWS. (n.d.). UnionBank & Consensys – Using blockchain to boost financial inclusivity across the Philippines. AWS Partner Network Blog. Retrieved September 3, 2023 from https://aws.amazon.com/partners/success/uniobank/#:~:text=The%20Intersection%20of%20Blockchain%20%26%20Banking,and%20inclusivity%20in%20the%20Philippines

ACG Report, (2023). Conference Meeting on January 25, 2023, Comments on the Recommendation of Re-Opening of CRMIS

APNIC (2021). Asia-Pacific internet registry APNIC says WHOIS admin passwords were mistakenly exposed for three months. Retrieved from https://portswigger.net/daily-swig/asia-pacific-internet-registry-apnic-says-whois-admin-passwords-were-mistakenly-exposed-for-three-months

Bannister, A. (2022, January 21). Was COMELEC hacked? Philippines Commission on Elections casts doubt on data breach claims. The Daily Swig. Retrieved from https://portswigger.net/daily-swig/was-comelec-hacked-philippines-commission-on-elections-casts-doubt-on-data-breach-claims

Batubara, F. R., Ubacht, J., & Janssen, M. (2019, June). Unraveling transparency and accountability in blockchain. In Y.-C. Chen, F. Salem, & A. Zuiderwjik (Eds.), Proceedings of the 20th Annual International Conference on Digital Government Research (pp. 204-213). ACM. https://doi.org/10.1145/3325112.3325262

Bhawana, Kumar, S., Rathore, R. S., Mahmud, M., Kaiwartya, O., & Lloret, J. (2022). BEST—Blockchain-Enabled Secure and Trusted Public Emergency Services for Smart Cities Environment. Sensors, 22(15), 5733. https://doi.org/10.3390/s155733

Bhoyar, N. G. (2022). A Case Study of RDBMS and OODBMS: Importance in Business. International Journal of Research in Engineering, Science and Management, 5(11), 1-6

Bluepoint Foundation (2023). Bluepoint Foundation, Retrieved August 15, 2023, from https://bluepoint.foundation/

Bongo, M. F., & Culaba, A. B. (2019, November). Blockchain technology in the Philippines:

Status, trends, and ways forward. In 2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM) (pp. 1-8). IEEE. https://doi.org/10.1109/HNICEM48295.2019.90703349

Brusca, I., Manes Rossi, F., & Aversano, N. (2018). Accountability and transparency to fight against corruption: An international comparative analysis. Journal of Comparative Policy Analysis: Research and Practice, 20(5), 486-504. https://doi.org/10.10.1080/13876988.2017.1393951

Cabugwang, K. A. F., Enriquez, R.C.K., Villabroza, E.E., & Pulmano, C.E. (2023). Towards the development of a blockchain system for Philippine government processes for enhanced transparency and verifiability. Procedia Computer Science (Vol. 219, pp 107-114). https://doi.org/10.1016/j.procs.2023.01.270

Dafoe, A. (2015). On technological determinism: A typology, scope conditions, and a mechanism. Science, Technology, & Human Values, 40(6), 1047-1076. https://doi.org/10.1177/0162243915579283

De Dios, E. S., & Ferrer, R. D. (2001). Corruption in the Philippines: Framework and context. Public Policy, 5(1), 1-42. University of the Philippines Center for Integrative and Development Studies. Retrieved from https:/cids.up.edu.ph/download/corruption-philippines-framework-context/July 23,2023

Dhande, M., Mehta, B., Panchal, M., & Trivedi, S. (2020). E-Crime Management for Trust Building. International Research Journal of Engineering and Technology (IRJET), 7(5)

El Khatib, M., Al Mulla, A., & Al Ketbi, W. (2022). The Role of Blockchain in E- Governance and Decision-Making in Project and Program Management. Advances in Internet of Things, 12(3), 88-109. https://doi.org/10.4236/ait.2022.123006

Gillis, A. S. & Brush, K. (2024). What is an RDBMS (Relational Database Management System)? Tech Target. Retrieved July 28, 2023 from https://www.techtarget.com/searchdatamangement/definition/rdbms-relational-database-management-system

Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the blockchain technology. In 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE) (pp. 1-6). IEEE. https://doi.org/10.1109/AIEEE.2018.8592253

Haworth-Elsayed, J. (2019, January 21). Filipino pawn shop breach leaks 900k clients' data. The Daily Swig (PortSwigger). Retrieved from https://portswigger.net/daily-swig/filipino-pawn-shop-breach-leaks-900k-clients-data

Heimdall (2023). Sobre a Heimdall. Retrieved September 5, 2023, from https://ph.linkedin.com/company/heimdall-digital?trk=public_profile_topcard-current-company

Hellani, H., Sliman, L., Samhat, A. E., & Exposito, E. (2021). On blockchain integration with supply chain: Overview on data transparency. Logistics, 5(3), 46. https://doi.org/10.3390/logistics5030046

Hingorani, I; Khara, R.; Pomendkar, D.; Raul, N. (2020). Police Complaint Management System using Blockchain Technology. In 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) (pp. 1214-1219). IEEE. https://doi.org/10.1109/ICISS49785.2020.9315884

Howcroft, D. & Taylor, P. (2022). Automation and the future of work: A social shaping of technology approach. New Technology, Work and Employment, 38(2), 351-370. https://doi.org/10.1111/ntwe.12240

Huang, H., Shen, B., Zhong, L., & Zhou, Y. (2023, January). Protecting data integrity of web applications with database constraints inferred from application code. In Proceedings of the 28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '23) (Vol. 2, pp. 632-645. Association for Computing Machinery. https://doi.org/10.1145/3575693.3575699

IBM (n.d.). What is blockchain technology? How blockchain works. IBM. Retrieved September 10, 2023 from https://ibm.com/topics/blockchain

Kaspersky (n.d.). What is smishing and how to defend it. Kaspersky Resource Center. Retrieved August 26, 2024 from https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how- to-defend-against-it/

Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H. N. (2022). Ethereum smart contract analysis tools: A systematic review. IEEE Access, 10, 57037-57062. https://doi.org/10.1109/ACCESS.2022.3169902

Landerreche, E., & Stevens, M. (2018, May). On immutability of blockchains. In W. Prinx & P. Hoschka (Eds.), Proceedings of the 1st ERCIM Blockchain Workshop. European Society for Socially Embedded Technologies. https://doi.org/10.18420/blockchain2018_04

Liu, D., Zhang, Y., Jia, D., Zhang, Q., Zhao, X., & Rong, H. (2022). Toward secure distributed data storage with error locating in blockchain enabled edge computing. Computer Standards & Interfaces, 79, 103560. https://doi.org/10.1016/j.csi.2021.103560

Martin, L. (2023). Blockchain vs. relational database: Which is right for your application? TechBeacon. Retrieved August 18, 2023 from https://techbeacon.com/security/blockchain-vs-relational-database-which-right-your-application

McBee, M. P., & Wilcox, C. (2020). Blockchain technology: Principles and applications in medical imaging. Journal of Digital Imaging, 33(3), 726-734. https://doi.org/10.1007/s10278-019-00310-3

McGregor, A., (2021, March 1). A journey through the ages. Retrieved from https://www.capita.com/our-thinking/evolution-of-data-policing

Mislos, M. (2023, September 21). Department of Budget and Management launches blockchain project with Bayanichain. BitPinas. Retrieved September 1, 2023 from https://bitpinas.com/business/budget-department-bayanichain-blockchain-project/

Momani, A. M. (2020). The unified theory of acceptance and use of technology: A new approach in technology acceptance. International Journal of Sociotechnology and Knowledge Development (IJSKD), 12(3), 79-98. https://doi.org/10.4018/IJSKD.2020070105

Nakamoto, S. (2008, October 31). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved August 16, 2023, from https://bitcoin.org/bitcoin.pdf

Oesch, S., & Ruoti, S. (2020, August). That was then, this is now: A security evaluation of password generation, storage, and autofill in browser-based password managers. In Proceedings of the 29th USENIX Conference on Security Symposium (pp. 2165-2182). USENIX Association. Retrieved July 20, 2023, from https://www.usenix.org/conference/usenixsecurity20/presentation/oesch

Philippine National Police (2019). PNP PATROL Plan 2030. Retrieved September 5, 2023, from https://www.pnp.gov.ph/images/Announcement/2019/PATROL_PLAN_2030.pdf

Philippine National Police. Directorate for Information and Communications Technology Management. (2018, November 5). Approved PNP ICT Master Plan (SMART Policing) for the period CY 2020 to CY 2025 [Memorandum]. Philippine National Police. Retrieved August 9, 2023, from https://www.scribd.com/document/837652755/Approved-PNP-ICT-Master-Plan-SMART-Policing-1

Philippine Statistics Authority (2022). Crime statistics. Retrieved from https://psa.gov.ph/content/crime-statistics-0

Pink, S., Lanzeni, D., Horst, H. 2018. Data anxieties: finding trust in everyday digital mess. Big Data Soc. 5 (1), 1–10.

https://doi.org/10.1177/2053951718756685

Philippine National Police. (2018, November 16). PNP ICT Master Plan (SMART Policing) [Memorandum]. Referenced in PNP Memorandum Circular No. 2022 – 135

Philippine National Police. (2022, April 18) Revised Guidelines and Procedures in the Implementation of the National Police Clearance System

Philippine National Police. (2021). Privacy Management Program, Guidelines and Procedures in Compliance with Data Privacy Act of 2012. (Memorandum Circular No. 2021-179). Retrieved from https://www.scribd.com/document/770719788/MC-2021-179-Privacy-Management-Program-Guidelines-and-Procedures-in-Compliance-with-Data-Privacy-Act-of-2012

Purdue Global (2018, April 9). Criminal Justice: The Growing Role of Technology in the Criminal Justice Field. Purdue Global. https://www.purdueglobal.edu/blog/criminal-justice/growing-role-technology- criminal-justice/

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of internet of things. IEEE Internet of Things Journal, 7(6), 4682-4696. https://doi.org/10.1109/JIOT.2020.2978707

Ronda, R. A. (2023, October 12). After PhilHealth, PSA suffers data breach. The Philippine Star. https://www.philstar.com/headlines/2023/10/12/2303082/after-philhealth-psa-suffers-data-breach

Rovnyagin, M. M., Dmitriev, S. O., Hrapov, A. S., Maksutov, A. A., & Turovskiy, I. A. (2021). Database Storage Format for High Performance Analytics of Immutable Data. In 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) (pp. 618-622). IEEE. https://doi.org/10.1109/EIConRus51938.2021.9396453

Sadiku, M. N. O.; Alam, S. & Musa, S. M. (2017). Information assurance benefits and challenges: An Introduction. Information and Security: An International Journal, (36). https://doi: 10.11610/isij.3604

Schuhknecht, F., & Jörz, S. (2022). The Easiest Way of Turning your Relational Database into a Blockchain — and the Cost of Doing So. Journal of Blockchain Technology. https://doi.org/10.48550/arXiv.2210.04484

Shang, Q. & Price, A. (2019). A blockchain-based land titling project in the Republic of Georgia: rebuilding public trust and lessons for future pilot projects. Innovations: Technology, Governance, Globalization, 12(3-4): 72–78. https://doi.org/10.1162/inov_a_00276

Sharma, Y., & Sharma, Y. (2019). Case study of traditional RDBMS and NoSQL database system. International Journal of Research Granthaalayah, 7, 351- 359. https://doi.org/10.29121/granthaalayah.v7.i7.2019.777

Shay, R., Blumenthal, U., Gadepally, V., Hamlin, A., Mitchell, J. D., & Cunningham, R. K. (2019). Don't even ask: Database access control through query control. ACM SIGMOD Record, 47(3), 17-22. https://doi.org/10.1145/3316416.3316420

Shin. D. D. H. (2019). Blockchain: The emerging technology of digital trust. Telematics and Informatics, 45, 101278. https://doi.org/10.1016/j.tele.2019.101278

Stephen, R., & Alex, A. (2018, August). A review on blockchain security. In IOP conference series: materials science and engineering (Vol. 396, No. 1, p. 012030). IOP Publishing. https://doi.org/10.1088/1757-899X/396/1/012030

Stonebraker, M., Madden, S., Abadi, D. J., Harizopoulos, S., Hachem, N., & Helland, P. (2018). The end of an architectural era: It's time for a complete rewrite. In M. Stonebraker & U. Cetintenel (Eds.), Making Databases Work: The Pragmatic Wisdom of Michael Stonebraker (pp. 463-489). ACM Books. https://doi.org/10.1145/3226595.3226637

The Asia Foundation (2022, March). Cybersecurity in the Philippines: Global Context and Local Challenges. https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf

White, S. K. (2021). What is CMMI? A model for optimizing development processes. CIO. Retrieved from https://www.cio.com/article/274530/process-improvement-capability-maturity-model-integration-cmmi-definition-and-solutions.html

Yavaprabhas, K., Pournader, M., & Seuring, S. (2023). Blockchain as the "trust-building machine" for supply chain management. Annals of operations research, 327(1), 49-88. https://doi.org/10.1007/s10479-022-04868-0

Zaeid, H. F. (2016). Technological determinism: A critique. Global Journal of Human-Social Science: G Linguistics & Education, 16(3), 7-13

Zeb, A. (2018). Security of Relational Database Management System: Threats and Security Techniques. Scribd. https://www.scribd.com/document/725019356/Security-of-Relational-Database-Management-System

Zhang, Y., Li, B., Wu, J., Liu, B., Chen, R., & Chang, J. (2022). Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT. IEEE Internet of Things Journal, 9(22), 22501-22515. https://doi.org/10.1109/JIOT.2022.3192488.