International Conference on Social Science and Humanity
Homepage : https://proceeding.antispublisher.or.id/index.php/icossh
Email : admin@antispublisher.com

e-ISSN : 3063-9611
ICOSSH, Vol. 2, No. 2, 2025
Page 26-37

Cybersecurity and Public Trust in Digital Governance: Focusing on Citizen Trust

Jidapa Preecha
Burapha University, Thailand

DOI : https://doi.org/10.61796/icossh.v2i2.27

Sections Info

Article history:
Submitted: February 10, 2025
Final Revised: March 28, 2025
Accepted: April 14, 2025
Published: May 24, 2025

Keywords:
Cybersecurity
Digital governance
Citizen trust
E-government

ABSTRACT

Objective: *This study aims to investigate the critical role of cybersecurity in fostering public trust toward digital government services.* ***Method:*** *A survey was conducted involving 30 citizens to analyze their perceptions and trust levels in e-governance systems amidst increasing cyber threats.* ***Results:*** *Findings reveal that 86% of respondents who have engaged with government digital services express a lack of trust, primarily due to concerns over cyber disruptions and fraud. These vulnerabilities undermine the perceived security and reliability of digital governance platforms.* ***Novelty:*** *This research highlights the direct correlation between cybersecurity challenges and public trust in digital government services, emphasizing the urgent need for robust cybersecurity frameworks to safeguard personal data. By focusing on citizen attitudes, this study contributes empirical evidence that informs policymakers and practitioners about the social implications of cybersecurity weaknesses in e-governance, thereby guiding the development of more secure and trustworthy digital public service infrastructures.*

INTRODUCTION

In today's world, technology is advancing rapidly, and with it, the convenience of accessing information online has become easier and faster. This is made possible by connecting computer networks across the world, which is often referred to as "cyberspace" Cybersecurity refers to the measures individuals and organizations take to reduce the risk of cyberattacks. Its main purpose is to protect the devices and services we use both online and work from theft, damage, or any other harmful activities (National Cyber Security Centre, 2025, About the NCSC: What is cyber security?). With the rapid growth of digital technology, new threats have emerged, one of the most concerning being cyberattacks [1].

In Thailand, both the government and private sectors have increasingly adopted cloud computing, which functions like a large data warehouse on the internet, allowing organizations to store and access data without needing to buy additional hardware. Government agencies use private cloud systems designed to be secure for internal use (NIPA Cloud, 2024, Tech Knowledge). However, cloud systems that are connected to the internet still face significant risks, such as data theft, which has been on the rise [2]. According to the National Cyber Security Committee's annual report in 2023, the government sector most frequently targeted by cyberattacks was the education sector, which faced 632 attacks, followed by other government sectors with 145 incidents. In Thailand, cyberattacks related to online gambling have also increased, adding to the growing threats faced by government agencies [3].

As a result of these rising risks, Thailand must enhance its capabilities to protect against cyber threats and prepare for potential future scenarios, such as cyber warfare (Kanokkon Phohom, 2021, p.46) [4].

Despite the government's efforts to adopt technology and improve digital services, there are still weaknesses in the system. Security measures often fail to prevent major cyberattacks. Loopholes in the system and ineffective regulations for preventing data leaks have caused several large-scale data theft incidents, affecting many people. In one instance, personal information was leaked from government agencies in 9 separate events [5]. Of these, 4 involved the release of citizens' personal data, leading to serious consequences. Fraudsters who have access to this information have used it to deceive and steal from people, especially from older adults who may not be very familiar with technology. These scams have had severe effects, with victims sometimes losing their savings or, tragically, even taking their own lives due to overwhelming debt caused by fraud [6].

The issues don't just stem from vulnerabilities in government systems, but also from the negligence of authorities who have not taken enough action to address these problems. This lack of response contributes to further complications and delays in finding proper solutions.

As mentioned earlier, cybersecurity threats are a significant factor that affects the economy, people's quality of life, and even national security. These threats are also impacting government policies, especially those aimed at moving the country toward a digital economy or Thailand 4.0 (Kanokkon Phohom, 2021, p.46). The more news spreads about fraud and cybercrimes happening online, the more the public's trust in government digital services decreases. Frequent incidents of cyberattacks, such as data hacking, personal information theft, and online fraud, make citizens feel unsafe in the digital world. As a result, many are reluctant to use government digital services because they see them as risky [7].

Moreover, some citizens believe that once their personal data is leaked, they cannot do anything to change or recover it. This belief leads them to ignore the issue and not pay much attention to the risks. They might think that since the damage has already occurred, there's no point in trying to fix it or prevent it from happening again.

Because of these issues, this article focuses on conducting a survey to understand the public's trust and attitudes toward government digital services in Thailand. The main questions in the survey will focus on the factors that influence the public's trust in digital government systems, the risks they see in using digital services (such as cyberattacks or privacy violations), and whether they believe their personal information is at risk [8]. The surveyors explore citizens' experiences with using government digital services, such as online banking, submitting government documents through websites, or using other digital services. This will help understand how incidents like data leaks have impacted citizens' behavior [9].

The results of this survey will give us a clear picture of how the public views and experiences government digital services. It will also help identify the reasons why many citizens feel insecure or avoid using these services. This information is crucial for

improving government digital systems, making them more secure and reliable, so that citizens can use them without fearing for their privacy or data security [10].

By addressing these concerns and finding solutions, the government can rebuild trust in its digital services. This will allow citizens to feel safe when using online government services without worrying about their personal data being compromised or misused.

RESEARCH METHOD

Research design

This article employs survey research design, collecting quantitative data through questionnaires to study public trends, attitudes, and behaviors regarding trust and experiences with the government's digital systems. Collecting data through questionnaires enables us to understand the thoughts and feelings of respondents about the following questions:

1. Have you ever used online services provided by the government, such as registering for benefits or government applications?
2. Do you think new technologies, such as digital systems and applications, make interacting with the government more convenient?
3. Do you feel that the government's digital systems adequately protect the privacy of your personal information?
4. When using online government services, do you feel secure when providing personal information, such as your national ID number or address?
5. Have you ever been concerned about the government storing your personal information online? Why?
6. Do you think the government should provide more public education on online security?
7. If a cyberattack occurred and your data were leaked, how would you want the government to respond?
8. Do you think you would continue to trust the government's digital system if your personal data were stolen from a government website? Why?

Each question in this survey is carefully designed to analyze and understand the perspectives and experiences of the public across multiple dimensions related to the use of government digital systems. These dimensions include behavioral insights, perceptions of security, and policy-related expectations. These questions help gather essential data to analyze public opinion trends and identify factors influencing the use of government digital systems more clearly.

Population and sample

The target population for this research consists of the general public in Thailand who have had experience using government digital services. These experiences may include submitting documents via online platforms, paying government service fees, or

accessing information through official government agency websites. Sample size: 30 general public people

The sample group was selected using purposive sampling, focusing on individuals aged 18 and above who have direct experience with or have used government-designed websites or applications and are able to complete an online questionnaire. While the sample size may not fully represent the entire population, collecting preliminary data from individuals with direct experience can effectively reflect relevant opinion trends.

Research instruments

Questionnaire

The primary research tool for this study is an online questionnaire designed to collect in-depth information from respondents, divided into three main sections:

General information of the respondents:

Personal information, divided into three questions

1. Gender (female 63.3%, male 30%, preferred not to specify their gender 6.7%)
2. Age (18-25 years 68%, 26-30 years 18%, 31-40 years 7%, 41-60 years 7%)
3. Occupation students 62%, civil servants 21%, other 17%)

Opinions on Cybersecurity and Trust in Digital Governance

Question 1 "Do you think new technologies, such as digital systems and applications, make interacting with the government more convenient?"

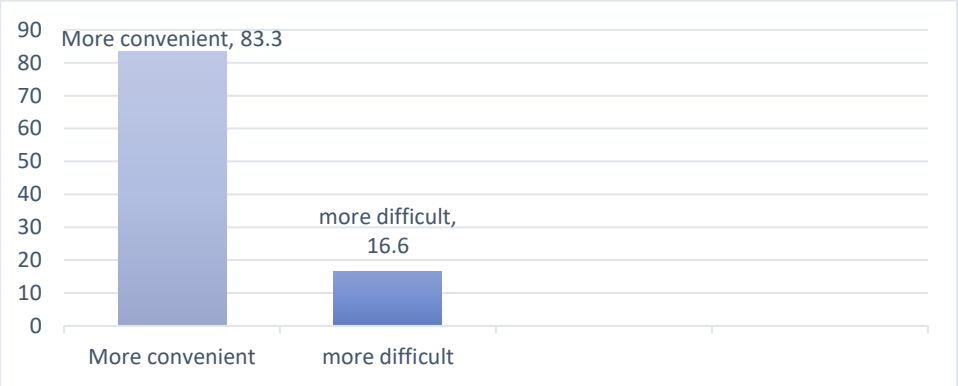

Figure 1. Question 1 Result Diagram

From the survey, 83% of respondents agreed that modern technology has made it easier for people to communicate with the government. However, 17% of respondents, aged 50-60 years, felt that these advancements have not made it easier for them. This may be because they are less familiar with digital tools, have limited IT skills, or find the systems too complicated. This shows the importance of creating simple, user-friendly systems and providing support to help older people use digital government services more easily.

Question 3 "Do you feel that the government's digital systems adequately protect the privacy of your personal information?"

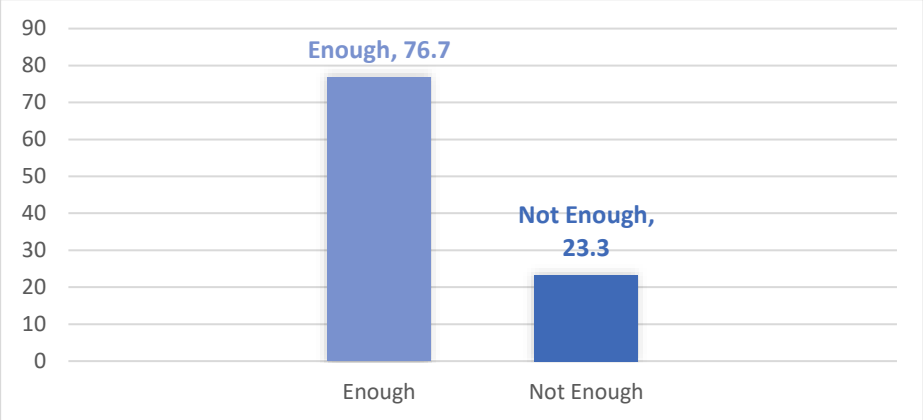

Figure 2. Question 3 Result Diagram

From the chart, it can be observed that 76.6% of respondents believe that the protection of citizens' privacy is insufficient due to frequent data breaches that often lead to online scams. Meanwhile, 23.3% think that the government is doing enough to protect people's data, as major data breaches are rare and do not significantly impact them.

Question 5 "Have you ever been concerned about the government storing your personal information online? why?"

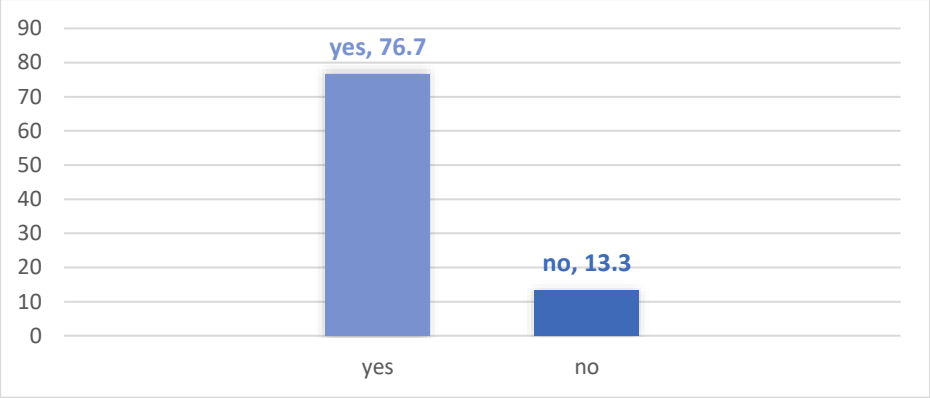

Figure 3. Question 5 Result Diagram

85% of respondents expressed concerns about the government's handling of personal data. Their worries primarily stem from a perception that the government lacks sufficient reliability in managing secure database systems. Many noted that data breaches occur frequently, especially in cases where sensitive information is exposed to the public or misused.

On the other hand, 15% of respondents indicated that they were not worried about the government's data storage practices. They believed that the government was trustworthy enough and that their personal information would not be easily compromised.

All respondents agreed that the government should provide more education to the public regarding data security. One respondent pointed out that, in addition to

educating citizens about protecting their data, the government must take responsibility for ensuring the security of personal information. They argued that even if individuals are well-informed about data security, such knowledge becomes meaningless if their information is leaked or compromised.

Respondents expressed a desire for the government to design and implement a more efficient and secure system to safeguard personal data. They acknowledged that cyber-attacks could target any organization or individual, making it essential for the government to address these issues with urgency and seriousness. The government must act swiftly to prevent data breaches and minimize harm to the public, ensuring that citizens are not left to face the consequences alone.

Additionally, some respondents called for stricter legal action against those who commit data theft. They emphasized the importance of enforcing laws rigorously and imposing severe penalties on offenders to deter similar incidents in the future. By taking these measures, the government could help prevent data breaches and restore public confidence in its ability to protect personal information effectively.

Question 7 “Do you think you would continue to trust the government’s digital system if your personal data were stolen from a government website? Why?”

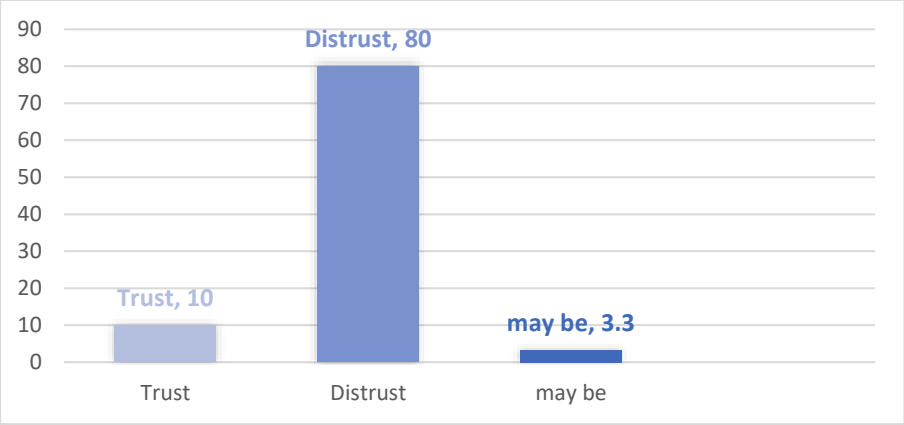

Figure 4. Question 7 Result Diagram

From the question, "Would you still trust the government’s digital system if your personal data were stolen from a government website?" 86% of respondents stated that they would lose trust in the government in such a scenario. Most expressed concerns over the government’s inability to protect personal data effectively and the lack of robust measures to combat cybersecurity threats. Many believe frequent data breaches stem from outdated security systems and negligence by officials, which has significantly damaged public confidence.

Some respondents also pointed out the government’s lack of transparency in disclosing data breaches and the absence of a clear crisis management plan, making it harder to rebuild trust in the long run. Another common issue raised was the inefficiency of responsible officials, which left people feeling their concerns were not addressed properly or on time.

On the other hand, 11% of respondents who still trusted the government's digital system explained that they believed the government had the capability and intention to resolve issues and protect their data. They trusted that the government would stand by its citizens during crises. Another 3% of respondents said they might trust the government if it could demonstrate strong action to solve the problem effectively and introduce clear policies to prevent future incidents.

This survey reflects the opinions of a specific group of respondents and cannot fully represent the views of the entire population.

Data collection

Data collection process

1. The questionnaire was distributed through online channels such as Google Forms or other convenient online platforms.
2. Data Collection Period: The data collection was conducted over a two-week period.
3. The questionnaire targeted respondents with direct experience using government digital services, and it was disseminated through social media platforms to reach the intended audience effectively.

Ethical considerations in data collection:

1. The purpose of the research and all relevant information were clearly communicated to the respondents before they participated in the survey.
2. Respondents were informed of their right to decline participation at any time without any consequences.
3. All collected data was treated as confidential and anonymized to ensure the protection of respondents' personal information.

Research limitations

The sample size is limited, which may constrain the generalizability of the findings to the entire population.

The use of online questionnaires might exclude individuals who lack access to or familiarity with digital technology, leading to potential sampling bias.

RESULTS AND DISCUSSION

Results

This research aims to study the perspectives, attitudes, and behaviors of citizens regarding the use of government digital systems, focusing on trust and data security. The findings reveal that most citizens are concerned about the risks associated with using government digital services, particularly regarding past incidents of data breaches, which have undermined confidence in the system. While citizens recognize that digital technology can enhance convenience in accessing government services, cybersecurity concerns remain a significant barrier to fully accepting digital services.

Moreover, citizens express expectations for the government to implement stricter measures to prevent cyberattacks and data breaches. These include improving cybersecurity systems, raising awareness about online safety, and effectively managing

data breach incidents when they occur. Citizens also emphasize the importance of educational initiatives to help them protect themselves from potential risks.

Overall, this study highlights that citizens have not fully entrusted government digital systems, primarily due to uncertainties surrounding data security, a lack of clarity in handling cybersecurity threats, and negative past experiences that have eroded trust.

Discussion

This research focuses on exploring the trust, attitudes, and behaviors of citizens towards the use of the government's digital systems. This issue is particularly critical in an era where technology plays a vital role across all sectors, especially in the public sector, which has been striving to integrate technology to enhance efficiency and transparency in public service delivery. However, findings indicate that trust in the government's digital systems remains low, despite efforts to improve security measures and encourage utilization.

Interpretation of research findings

The findings reveal that citizens remain concerned about various aspects of the government's digital systems, which can be categorized into the following key areas:

1. Personal Data Security

   A significant number of citizens expressed concerns regarding the security of their personal data required for submission or disclosure in the government's digital systems. Past incidents of data breaches have eroded trust in these systems and fostered negative attitudes. While efforts to improve security measures have been made, communication about the progress in this area remains insufficiently clear.

2. Cybersecurity Threat Management

   Cyberattacks have emerged as a critical risk in the digital era, particularly as government agencies have become prime targets for malicious actors. The research highlights that citizens perceive the government as inadequately equipped to handle such threats, including the development of advanced protective technologies, the establishment of secure networks, and swift responses to incidents.

3. Ambiguity in Measures and Policies

   Many citizens lack a clear understanding of the government's measures to protect data and address cybersecurity threats. This lack of clarity undermines confidence in the system and causes hesitation among some citizens to use digital services.

Concepts and theories

The analysis of these findings aligns with the **State-Citizen Relationship Theory**, which emphasizes the role of the state in building trust with its citizens through transparent and efficient governance. If citizens perceive that the government is unable to manage emerging issues or lacks transparency, this could negatively impact the state-citizen relationship.

Furthermore, the findings resonate with the concept of e-Governance, which underscores the integration of digital technologies to enhance efficiency and

transparency in public service delivery. While technology has the potential to improve convenience, the lack of trust in these systems remains a significant barrier to citizen acceptance.

Strategic issues and government efforts

Thailand has made strides in developing measures and infrastructure for cybersecurity, such as the enactment of the Cybersecurity Act B.E. 2019, which outlines guidelines for mitigating threats and reducing risks, as well as establishing dedicated agencies. However, the research indicates that citizens remain unaware of these measures in detail.

Initiatives such as the "Half-Half" project and the "10,000 Baht Digital Wallet Scheme" demonstrate the government's efforts to promote the use of digital services. At the same time, these initiatives highlight challenges when citizens are compelled to use digital services without confidence in the system. This necessity can create a sense of coercion and lead to resistance among certain demographic groups [11], [12], [13], [14], [15].

Recommendations

1. Enhancing Cybersecurity Measures
    a. Invest in modern technologies to prevent attacks, such as advanced cybersecurity systems, continuous monitoring, and rapid incident response mechanisms.
    b. Establish a Cybersecurity Emergency Response Team (CERT) to collaborate with various agencies for more effective threat management.
2. Communication and Transparency
    a. Increase communication with citizens regarding measures to protect personal data and manage data security. This could include publishing annual reports on system safety and explaining data collection and management processes.
3. Raising Awareness and Education
    a. Conduct training sessions or campaigns to raise awareness about cybersecurity among citizens, such as phishing prevention and secure password practices.
    b. Partner with schools and universities to promote education on cybersecurity.
4. Developing User-Friendly Systems
    a. Simplify the interface of digital systems to make them user-friendly, with clear guidance and reduced complexity in accessing services.
    b. Create support channels, such as online help centers or applications, to address citizen queries and resolve issues promptly.
5. Continuous Evaluation and Monitoring
    a. Establish independent agencies to regularly evaluate the security and efficiency of digital systems.

b. Develop evaluation reports to summarize problems and recommend solutions.

Future research directions

This research opens opportunities for future studies in the following areas:

1. Examining factors influencing trust in digital systems across different population groups, such as age, education, and income.
2. Analyzing case studies of countries that have successfully built trust in digital systems.
3. Investigating the psychological and social impacts of enforced digital policies on populations with varying levels of digital readiness.

This study provides valuable insights into the challenges the Thai government faces in developing digital systems for citizens. The low level of trust highlights structural issues that need to be addressed through better communication, system development, and public understanding. Building a trustworthy and user-friendly digital system can not only improve the quality of life for citizens but also strengthen trust and foster a positive relationship between the state and its citizens in the long term.

This research aimed to understand the perspectives, attitudes, and behaviors of the public toward the use of government digital systems, particularly concerning trust, security, and efficiency in the Thai context. The findings can be summarized across several key dimensions:

1. Trust in Government Digital Systems

   The study reveals that public trust in government digital systems remains low. Key factors influencing this trust include past experiences with data breaches and cyberattacks, which have created concerns and negative perceptions among citizens. Despite government efforts to improve security measures and system reliability, insufficient communication and lack of clarity in processes have left the public hesitant to fully engage with digital services.

2. Cybersecurity Challenges

   Cyber threats are a critical issue impacting public confidence in government digital systems. Many citizens perceive the government's measures as inadequate to address these risks, such as modern threat prevention, continuous security monitoring, and efficient responses to incidents. These concerns highlight doubts about the government's capacity to manage complex technical challenges effectively.

3. Public Awareness of Government Measures

   A significant portion of the population lacks a clear understanding of the government's efforts to protect personal data and mitigate cyber threats. The study found that unclear communication about policies, measures, and management strategies leaves citizens uncertain about engaging with digital services.

4. Impact of Digital Adoption Policies

   Government initiatives, such as the "Half-and-Half" program and the "10,000 Baht Digital Money" scheme, aim to encourage citizens to embrace

digital platforms. However, these initiatives reveal structural challenges, including a lack of trust in system security. As a result, some citizens feel compelled to participate, leading to resistance in certain groups.

CONCLUSION

Fundamental Finding : This study demonstrates that public trust in government digital systems in Thailand remains notably low, primarily due to past cybersecurity incidents, inadequate communication, and perceived insufficiencies in government cybersecurity capabilities. **Implication :** These findings underscore the critical need for governments to enhance transparent communication strategies, strengthen cybersecurity infrastructure, and foster public awareness to build trust and encourage meaningful engagement with digital services. Without addressing these trust deficits, digital adoption policies may face resistance or superficial compliance rather than genuine acceptance. **Limitation :** The research is limited by its focus on a specific national context, and findings may not be directly generalizable to other countries with differing socio-political and technological environments. Additionally, the study primarily relies on public perception data, which may be influenced by transient events or media coverage. **Future Research :** Further studies should investigate longitudinal changes in trust as government cybersecurity measures evolve, explore comparative analyses across diverse cultural contexts, and assess the effectiveness of targeted communication interventions designed to improve public confidence in digital government initiatives.

REFERENCES

[1] C. A. Londoño Londoño, "La seguridad humana, una perspectiva del poder terrestre en Colombia," *Revista Estado, Paz y Sistema Internacional*, vol. 3, no. 5, pp. 5–26, Jun. 2024, doi: 10.25062/2981-3034.4863.

[2] H. Chaoui and I. Makdoun, "A new secure model for the use of cloud computing in big data analytics," in *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*, in ICC '17. ACM, Mar. 2017, pp. 1–11. doi: 10.1145/3018896.3018913.

[3] E. Tekin (Delice) and N. Kartal, "Security of digital transformation in the healthcare sector: protection of medical data and solutions to cyber threats," in *Digital Transformation and Sustainable Development in Cities and Organizations*, IGI Global, 2024, pp. 212–229. doi: 10.4018/979-8-3693-3567-3.ch010.

[4] F. Z. Leccisotti, R. Chiesa, and D. De Nicolo, "Analysis of possible future global scenarios in the field of cyber warfare: national cyber defense and cyber attack capabilities," in *Cyber Security and Threats*, IGI Global, 2018, pp. 1584–1608. doi: 10.4018/978-1-5225-5634-3.ch077.

[5] N. E. Karpova and A. A. Babinova, "Ensuring the security of personal data in the enterprise information system," *Digital technology security*, no. 2, pp. 55–68, Jun. 2024, doi: 10.17212/2782-2230-2024-2-55-68.

[6] J. Manthorpe and J. Moriarty, "Working with older people from black and minority ethnic groups who have depression: From margin to mainstream," *Qual Ageing Older Adults*, vol. 10, no. 1, pp. 24–31, Mar. 2009, doi: 10.1108/14717794200900005.

[7] M. David, "Fraud, extortion and identity theft," in *Networked Crime*, Policy Press, 2023, pp. 143–158. doi: 10.1332/policypress/9781529218107.003.0008.

[8] S. Marsh and A. S. Patrick, "Social issues of trust and digital government," in *Encyclopedia of Digital Government*, IGI Global, 2007, pp. 1466–1471. doi: 10.4018/978-1-59140-789-8.ch224.

[9] X. Ye, X. Su, Z. Yao, L. Dong, Q. Lin, and S. Yu, "How do citizens view digital government services? study on digital government service quality based on citizen feedback," *Mathematics*, vol. 11, no. 14, p. 3122, Jul. 2023, doi: 10.3390/math11143122.

[10] T. S. Gesk and M. Leyer, "Artificial intelligence in public services: when and why citizens accept its usage," *Gov Inf Q*, vol. 39, no. 3, p. 101704, Jul. 2022, doi: 10.1016/j.giq.2022.101704.

[11] M. Alexander, "The british library initiatives for Access seminar: digital imaging," *Information Services & Use*, vol. 16, no. 3–4, pp. 165–173, Jul. 1996, doi: 10.3233/isu-1996-163-403.

[12] A. M. Alsalama and M. S. Alzahrani, "Cybersecurity in oil & gas 4.0: a systematic literature review of challenges, threats, and mitigating measures," in *ADIPEC*, in 24ADIP. SPE, Nov. 2024. doi: 10.2118/222581-ms.

[13] D. Lee, M. McGuire, and J.-H. Kim, "Collaboration, strategic plans, and government performance: the case of efforts to reduce homelessness," in *Toward a More Strategic View of Strategic Planning Research*, Routledge, 2022, pp. 51–67. doi: 10.4324/9781003295495-3.

[14] X. L. Lollar, "Assessing China's E-government and its impact on government and citizen relationship," in *Citizens and E-Government*, IGI Global, pp. 360–375. doi: 10.4018/978-1-61520-931-6.ch020.

[15] M. E. Milakovich, "Citizen-centric remote online digital governance," in *Digital Governance*, Routledge, 2021, pp. 88–117. doi: 10.4324/9781003215875-4.

* **Jidapa Preecha (Corresponding Author)**
Burapha University, Thailand
Email: 65140307@go.buu.ac.th