Jurnal Manajemen Pelayanan Publik Vol. 09 No. 03, October 2025
http://dx.doi.org/10.24198/jmpp.v9i3.65900

Evaluation of Infrastructure and Cybersecurity in Supporting the Digital Transformation of Public Services in Tangerang City

[a] Achmad Kosasih; [b] Toddy Aditya; [c] Sukma Aditya Ramadhan

[a,b,c] Government Science Study Program, Faculty of Social and Political Sciences, University of Muhammadiyah Tangerang, Banten, Indonesia

ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi kesiapan infrastruktur digital dan keamanan siber dalam mendukung transformasi digital layanan publik di Tangerang, khususnya aplikasi Tangerang LIVE. Aplikasi ini dirancang untuk mengintegrasikan layanan publik ke dalam satu platform digital, namun data menunjukkan penurunan penggunaan fitur-fitur oleh publik. Penelitian ini menggunakan pendekatan kuantitatif dengan Structural Equation Modeling (SEM) untuk menyelidiki hubungan antara infrastruktur digital, keamanan siber, dan layanan publik digital. Hasil penelitian menunjukkan bahwa keamanan siber memiliki pengaruh yang lebih besar dalam membangun kepercayaan publik terhadap aplikasi layanan publik digital dibandingkan infrastruktur digital. Analisis deskriptif mengungkapkan bahwa mayoritas responden memberikan penilaian positif terhadap infrastruktur digital, keamanan siber, dan layanan publik digital. Temuan menunjukkan bahwa kedua faktor ini bersama-sama menjelaskan sebagian besar variasi dalam layanan publik digital. Oleh karena itu, penguatan kedua faktor tersebut sangat penting untuk keberhasilan transformasi digital layanan publik yang aman dan efisien. Penelitian ini berkontribusi pada pengembangan model tata kelola keamanan digital di sektor publik dan menekankan pentingnya meningkatkan kapasitas ketahanan siber di pemerintah daerah untuk menghadapi ancaman siber dan memastikan kelancaran pengoperasian layanan publik.

ABSTRACT

This study aims to evaluate the readiness of digital infrastructure and cybersecurity in supporting the digital transformation of public services in Tangerang, especially the Tangerang LIVE application. The app is designed to integrate public services into a single digital platform, but data shows a decline in the use of features by the public. This study uses a quantitative approach with Structural Equation Modeling (SEM) to investigate the relationship between digital infrastructure, cybersecurity, and digital public services. The results of the study show that cybersecurity has a greater influence in building public trust in digital public service applications than digital infrastructure. The descriptive analysis revealed that the majority of respondents gave positive assessments of digital infrastructure, cybersecurity, and digital public services. The findings suggest that these two factors together explain most of the variation in digital public services. Therefore, strengthening these two factors is critical for the successful digital transformation of public services that are safe and efficient. This research contributes to the development of digital security governance models in the public sector and emphasizes the importance of increasing cyber resilience capacity in local governments to deal with cyber threats and ensure the smooth operation of public services.

ARTICLE HISTORY
Submitted: 04 08 2025
Revised: 03 09 2025
Accepted: 11 09 2025
Published: 11 10 2025

KATA KUNCI
Keamanan Siber; Infrastruktur Digital; Tangerang LIVE; Transformasi Digital; Layanan Publik

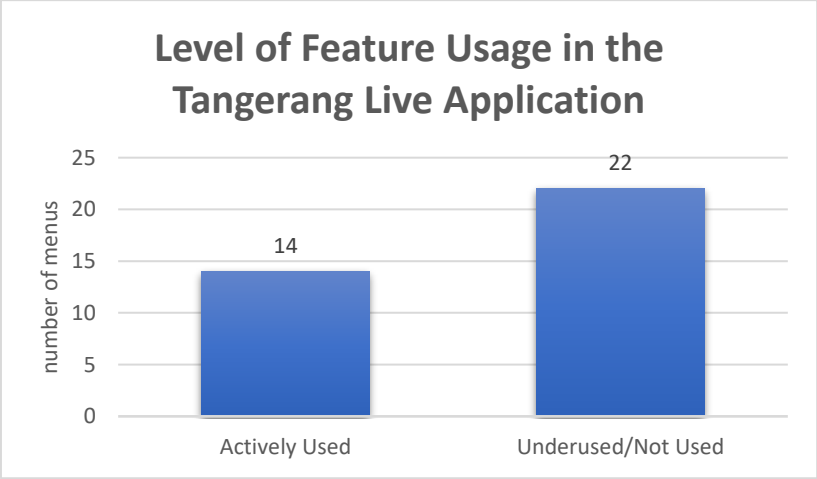
KEYWORDS
Cybersecurity; Digital Infrastructure; Tangerang LIVE; Digital Transformation; Public Services

Correspondence Achmad Kosasih Email : kosasih1957@gmail.com

INTRODUCTION

The *Tangerang LIVE application* refers to a Super App developed by the Tangerang (city) Regional Government to consolidate distinct public services in one digital platform (Dinas Komunikasi dan Informasi Kota Tangerang, 2022). Although it was launched in 2016 and has shown an increase in the number of users, data shows a decrease in downloaders since 2020 (Kosasih & Aditya, 2024). This decline in downloaders indicates that not all in-app features are being utilized optimally by the public (Tholok et al., 2019).

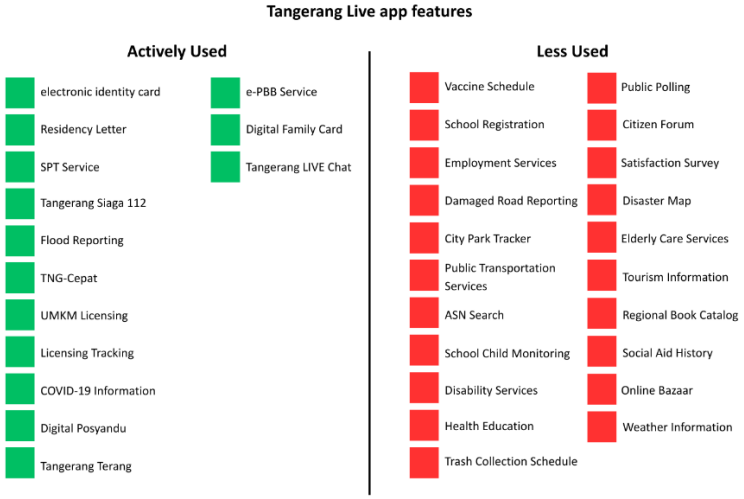
Figure 1.
Usage rate of the Tangerang LIVE Application Feature, 2025



Sources: Tangerang LIVE, 2025

As it is shown in Figure 1, the level of use of the Tangerang LIVE Application Feature, out of a total of 36 available service menus, only 14 are actively operated. The rest (22 menus) are classified as significantly underused (Tangerang, 2022). This inequality indicates potential problems both in terms of the suitability of features with the needs of the community, as well as in terms of the readiness of the digital infrastructure and the security guarantee of the underlying system of the application.

Figure 2.
Tangerang LIVE Application Features Active and Underused, 2025



Sources: Tangerang LIVE, 2025

Further in Figure 2 about Active and Underused Tangerang LIVE Application Features, when analyzed by service category, the administrative services menu has the highest usage rate. However, in other categories such as social services, public information, and health, most of the features are not utilized optimally (Aulia, 2019). The decline in the use of this feature shows the importance of an in-depth evaluation of the infrastructure and digital security dimensions as a prerequisite for the sustainability of application-based public services.

Meanwhile, the theoretical frameworks and empirical studies of governance are essential to comprehensively examine the security of digital systems in local government infrastructure (Schinagl et al., 2023). In discussing data management and security in public digital systems, it is important to evaluate resilience and trust in digital services. (Janssen et al., 2020) provided insights into digital rights, privacy, and internet governance principles, relevant in discussing legal frameworks and data protection in government applications (De Gregorio & Radu, 2022). Examining the digital governance transition and its relation to infrastructure readiness and mature governance (Erkut, 2020). It is relevant to evaluate the transparency, accessibility, and security of data in a digital public information system such as Tangerang LIVE (Setyawati & Fitriati, 2023). Explain how IT governance mechanisms impact the success of digital transformation and digital infrastructure security (Mulyana et al., 2021).

Research on digital transformation at the regional level has been carried out extensively. Various studies highlight digital leadership and technology readiness as the key to digitalization success (AlNuaimi et al., 2022; Borah et al., 2022; De Araujo et al., 2021; Khaw et al., 2022; Schiuma et al., 2022; Topcuoglu et al., 2023; Verma et al., 2022). However, as people's reliance on public service applications increases, aspects of cybersecurity and digital infrastructure are becoming increasingly critical(Klappe et al., 2020; Naranjo et al., 2019; Nurunnisa et al., 2023; Smyrnova et al., 2021; Tyagi, 2024). Studies such as Schinagl et al. (2023) and Janssen et al. (2020) emphasize the importance of applying strong data security and governance principles (Janssen et al., 2020; Janssen & van der Voort, 2020; Obaid et al., 2022; Schinagl et al., 2023; Srebalová & Peráček, 2022; Thompson et al., 2020). On the other hand, research in Indonesia such as Aditya, (2023) dan Rosyidah, (2017) emphasized more on application user behavior, there has not been much exploration of the infrastructure and security of digital systems as a whole (Aditya, 2023; Aditya et al., 2023; R. Ramadhan et al., 2019; Rosyidah, 2017).

The existing research gap is the lack of studies that simultaneously model the readiness of digital infrastructure including the network level, uptime, and cybersecurity interoperability and governance that includes awareness, readiness, and resilience, as predictors of digital public service quality at the city level, which has not been widely discussed in the context of local government. This research makes a theoretical contribution to the development of digital governance models and provides policy implications that emphasize the importance of integrating strengthening digital infrastructure and cyber resilience in improving the quality of digital public services at the city level.

This research is proposed to find out how the readiness of digital infrastructure and cybersecurity systems supports the digital transformation of public services in Tangerang City. The urgency of conducting this research is that the digital transformation of public services requires reliable infrastructure and cybersecurity. In Tangerang City, the low utilization of the Tangerang LIVE application feature indicates a fundamental problem. Evaluation of the readiness of digital infrastructure and information security systems is very important to ensure the sustainability, public trust, and effectiveness of technology-based public services.

Literature Review

Cybersecurity Theory

Cybersecurity, or cybersecurity, is an area that focuses on protecting computer systems, networks, devices, and data from threats, damage, or unauthorized access (Henriques de Gusmão et al., 2018). Along with the increasing dependence on information and communication technology in various sectors, both private and public, threats to digital systems are becoming increasingly complex and diverse. Cybersecurity aims to maintain the integrity, confidentiality, and availability of data and systems, known as the CIA Triad (Confidentiality, Integrity, Availability) (Lahcen et al., 2020). Cybersecurity Theory is a theory that examines the application of policies, techniques, and strategies to protect information systems from potential cyber threats (Savaş & Karataş, 2022). In Cybersecurity Theory, these threats can be external or internal, including hacker attacks, viruses, malware, and threats from internal system failures or human error (Kianpour et al., 2022). This theory also highlights the importance of risk management aspects in dealing with cyber threats. Risk management includes identifying, assessing, and mitigating potential threats to the system. This theory focuses on the creation of systems that are not only capable of detecting threats but also able to deal with them proactively and responsively, keeping the system running despite disruptions (Gale et al., 2022; Yusif & Hafeez-Baig, 2021).

One of the main foundations in Cybersecurity Theory in the study by Balozian et al. (2021) and Xu (2019) is the concept of the CIA Triad, which consists of three essential principles in cybersecurity. *Confidentiality* ensures that data can only be accessed by the authorities. In digital applications, maintaining the confidentiality of information is crucial, especially the user's data and other sensitive information. To ensure confidentiality, various encryption and access control techniques are applied to the system. Furthermore, *Integrity* refers to the validity and integrity of information. This principle ensures that the data is not altered or manipulated by unauthorized parties during transmission or storage. To maintain integrity, hashing and checksum mechanisms are used to detect unauthorized changes in the data. Finally, *Availability* ensures that information and systems are available to legitimate users when needed. Good system security depends not only on data protection, but also on the maintenance and management of infrastructure that ensures the availability of services 24/7, including recovery from disasters and attacks. These three principles work together to create a secure and reliable digital ecosystem, and they serve as a standard for assessing the effectiveness of a cybersecurity system.

In research (Chowdhury et al., 2022; Ebrahimi et al., 2025) ¸Cybersecurity Theory not only covers technical policies but also suggests various models for managing threats and building system resilience. One of the most well-known models is Defense in Depth, which involves applying multiple layers of protection throughout the system. Some of these layers include:

1. Firewall to block unauthorized access,
2. Intrusion detection systems (IDS) are used to monitor and detect suspicious activity,
3. Encryption to protect data in transit,
4. Multi-factor authentication is used to ensure that only authorized users can access the system.

The goal of this approach is to ensure that if one layer of defense fails, another layer can still protect the system. *Cyber Resilience* is a concept that develops in Cybersecurity Theory. Cyber resilience is more than just prevention, but it also includes the system's ability to survive and recover from attacks (Balozian et al., 2021; Xu, 2019). Resilient systems can quickly mitigate the impact of attacks, reduce recovery time, and ensure operational continuity, which is critical for technology-dependent services (Safitra et al., 2023). In addition to the technical aspects, Cybersecurity Theory also examines the importance of policies and compliance with regulatory standards in managing cybersecurity. Governments, organizations, and digital service providers must implement policies that ensure the protection of their data and technological infrastructure(Balozian et al., 2021; Mishra et al., 2022; Xu, 2019). Strict policy enforcement includes employee training, secure password management, regular software updates, and compliance with existing regulations, such as the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in the United States (Cazier, 2007; Nalley, 2022). Compliance with these regulations ensures that sensitive data is protected in a lawful manner and by recognized standards (Chung et al., 2021; L. Li et al., 2019).

Cybersecurity Theory is particularly relevant for this research because it provides a clear framework for evaluating how digital infrastructure and cybersecurity play a role in supporting the success of digital transformation in public services. In this study, this theory is used to analyze various important aspects of cybersecurity, such as risk management, data protection, and resilience to digital threats, which affect public adoption and trust in digital applications of public services. Good security can encourage people to trust and be more active in using digital public services, while threats or poor security policies can reduce participation rates and reduce the effectiveness of services. Therefore, Cybersecurity Theory is an important foundation in evaluating the readiness of digital systems and ensuring the sustainability and efficiency of technology-based public services in Tangerang City.

The *Demand Scale Effect* indicator relates to the ability of digital infrastructure to handle increasing demand without compromising the quality of services, taking into account the principles in *the CIA Triad* to maintain the confidentiality, integrity, and availability of data. The *Collaborative Effect indicator* measures the extent to which collaboration between the public and private sectors can strengthen cyber resilience by applying *a Defense-in-Depth* approach to improve protection against shared threats. The *Knowledge Spillover Effect* indicator assesses the extent to which knowledge and best practices in cybersecurity can be disseminated between institutions or sectors to improve resilience and readiness against cyber threats, based on *Cyber Resilience* theory that focuses on operational recovery and sustainability. The indicators used in this study, such as *the Demand Scale Effect*, *Collaborative Effect*, and *Knowledge Spillover Effect*, are linked to basic cybersecurity theories such as *CIA Triad*, *Defense-in-Depth*, and *Cyber Resilience*. Each of these indicators assesses the readiness and resilience of digital infrastructure as well as collaboration between sectors in supporting the sustainability of safe, efficient, and reliable digital public services.

Digital Infrastructure in Public Services

Digital infrastructure is the technological foundation that supports all electronic-based service systems in the context of government and public services (Finger & Montero, 2023). Basically, digital infrastructure includes communication networks, hardware,

software, data centers, and information management and storage systems that are interconnected to support the overall operation of digital systems (Zuckerman, 2020). The existence of adequate digital infrastructure is an absolute requirement for realizing effective digital transformation in the implementation of public services. Without a solid infrastructure, the digitization of public services risks facing technical failures, limited access, and threats to data integrity and public trust (Lafioune et al., 2023; Lindgren & van Veenstra, 2018).

The rapid development of information technology has prompted governments in various parts of the world to strengthen their digital infrastructure as an effort to improve the quality and efficiency of public services. The government is not only required to provide access to services digitally, but also to ensure that the system used is able to provide a fast, responsive, secure, and transparent service experience. Digital infrastructure allows governments to design services that can be accessed anytime and from anywhere by the public, thereby reducing reliance on physical services and expanding the reach of public services to areas that were previously difficult to reach (Serrano, 2018). A strong digital infrastructure not only speeds up administrative processes in government but also plays a crucial role in driving internal efficiency and accountability. Digital system-based services allow the automation of various service processes, such as permit applications, levy payments, public reporting, and access to government information. All of these processes become more efficient with the support of a well-integrated network and software system. In addition, data management has become more structured so that it facilitates the process of reporting, monitoring, and evaluating service performance by government agencies (Deokryong Yoon, Yaewon Hyun, 2022; Lafioune et al., 2023; Paiva et al., 2019; Yan & Li, 2022).

However, the advancement of digital infrastructure in the public sector is closely tied to significant challenges. One of the primary obstacles is ensuring the availability and equitable distribution of internet connectivity, which serves as the foundation for digital service operations (Brunetti et al., 2020). In many areas, especially remote or densely populated low-income areas, access to stable and fast internet networks remains a significant obstacle. This condition creates a digital divide that directly affects public participation in the digital public service system(Aminah & Saksono, 2021; M. Li et al., 2025). Another critical challenge is the availability of human resources with the technical expertise required to manage and maintain digital infrastructure. Many government agencies continue to struggle with a shortage of IT personnel, both in terms of numbers and technical skills (Singh & Pankaj, 2022). In addition to the technical and human aspects, the institutional aspect is also an important factor. The government needs strategic and measurable policies to support the development of digital infrastructure sustainably. Budget allocation, long-term planning, and partnerships with the private sector are part of the institutional strategies needed to ensure that infrastructure development does not run sporadically or intermittently (Abdussamad, 2024; Giest & Samuels, 2023). In addition, the need for a strong security system is also a major concern in the development of digital infrastructure. Weak infrastructure in terms of security will be vulnerable to cyberattacks, data manipulation, and leakage of sensitive information belonging to citizens (Priscilla et al., 2024).

In a global context, various studies show that countries or regions with mature digital infrastructure tend to have more efficient, inclusive, and trusted public service systems. Research conducted by Shah et al., 2025) on the implementation of e-governance found that improving digital infrastructure directly increases public trust in government services,

which in turn accelerates efficiency in the delivery of public services. On the other hand, limited infrastructure is often the main obstacle in optimizing the use of information technology for public services. Research by Desai & Manoharan (2024), states that countries with underdeveloped digital infrastructure face difficulties in digitizing efficient public services, which affects transparency, accountability, and the government's ability to deliver quality services. With suboptimal infrastructure, it is difficult for the government to meet people's demands for fast, safe, and accessible services throughout the region, especially in rural areas or areas with limited internet access (Desai & Manoharan, 2024).

This research offers novelty with a focus on evaluating the readiness of digital infrastructure and cybersecurity systems in Tangerang City, especially in the Tangerang LIVE application. Advantages: This research assesses the actual conditions and gaps against the ideal standard (gap analysis), as well as prepares strategic recommendations for system strengthening. The expected results will enrich the literature on *cyber-resilience* and provide a policy framework for strengthening the digital system in the Tangerang City Regional Government.

RESEARCH METHODS

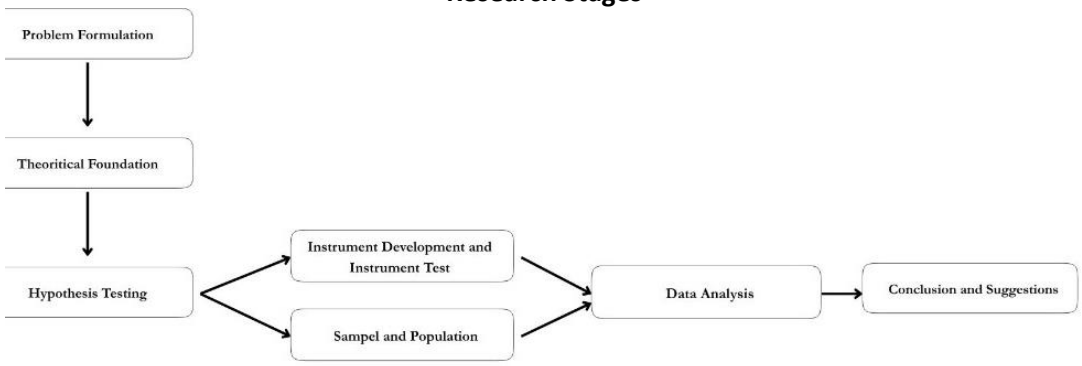
Research Design

This study employs a quantitative design with a Structural Equation Modeling (SEM) approach, which is implemented using SmartPLS. This study uses Partial Least Squares Structural Equation Modeling (PLS-SEM) for several reasons. PLS-SEM was chosen because this method is well suited for both exploratory and predictive models, making it possible to analyze relationships between complex latent variables and predict their effects. In addition, PLS-SEM is more flexible in handling the complexity of models involving many different latent variables and indicators. This method is also more appropriate for smaller sample sizes, and although the study involved 400 respondents, PLS-SEM was still effective in providing robust estimates. In addition, PLS-SEM does not assume a normal distribution, so it can be used on data that is not normally distributed, as found in this survey. Based on the inverse square root and gamma-exponential formulas to determine the minimum sample size, this study ensures that the sample size used is sufficient to achieve the statistical strength required to detect the relationships between variables significantly. The SEM method is applied to assess the relationship between predefined variables, which are:

1. Digital infrastructure.
2. Cyber Security
3. Digital Public Services.

Figure 3 shows the stages of research used in this study. The research process begins with Problem Formulation, followed by Theoretical Foundations, and Hypothesis Testing. After that, the next stage involves Instrument Development and Instrument Testing, followed by the Sample and Population stage, as well as Data Analysis. Finally, this study closes with Conclusions and Suggestions.

Figure 3.
Research Stages



Sources: (Cresswell, 2018)

Population and Sample

1. Population: Residents of Tangerang City who have downloaded the Tangerang LIVE application.
2. Sample: This study uses stratified random sampling with samples from 13 sub-districts in Tangerang City. The sampling frame is an active user of the Tangerang LIVE application whose data is obtained from the Communication and Information Service. Respondents were randomly selected from each sub-district, with a proportional allocation based on the number of active users. The inclusion criteria include active users within the last three months who are willing to participate and provide written consent.
3. Sample Size: Based on data from the Communication and Information Service, this population amounts to 1,006,289 users
4. Slovin Formula: The Slovin formula is used to determine the number of samples needed in a study from a limited or known population. Based on the results of the Slovin formulation with a margin of error of 5%, the result is 399.55 because the number of samples must be an integer, so n is rounded to 400.

Data Collection

Data is collected through:

1. This study uses a data collection procedure that combines online and offline channels. The questionnaire was distributed through online platforms (social media) to ensure wide access and efficiency, as well as through offline collection in several strategic locations in each sub-district to reach participants who were more difficult to reach online. The expected response rate is 80%, with reminder and follow-up measures to ensure a high participation rate. To overcome non-response bias, the control strategy used includes sending periodic reminders to respondents who have not responded and ensuring that the participation of various strata (based on sub-district and demographic characteristics) is recorded proportionally, in accordance with the stratified random sampling technique used.

2. Measurement Scale: Likert is on a 5-point scale, from "strongly disagree" to "strongly agree".

3. Ethics and Approval: This research has been approved by the Institutional Review Board (IRB) which ensures that this research complies with applicable ethical standards. Before participating, each respondent who receives a questionnaire through Google Form

(online channels) or offline collection is given informed consent explaining the purpose of the research, the procedures carried out, and their rights, including the right to resign at any time without consequences. Written consent is also taken electronically through Google Form before the respondent fills out the questionnaire. For the protection of personal data, a mechanism in accordance with the Personal Data Protection Law (PDP Law) is applied, where all respondents' data will be kept confidential and only used for the purpose of this research. The data collected will be anonymized to protect the identity of the respondent and will not be shared with third parties without the explicit permission of the respondent.

Research Instruments

The instrument implemented in this study was a survey to determine the level of readiness of digital infrastructure and cybersecurity to support the digital transformation of public services in Tangerang City. Based on Figure 4, it can be concluded that this questionnaire consists of several sections, including Digital Infrastructure, Cybersecurity, and Digital Public Services. This can be seen in Table 1 regarding the research instruments:

Table 1.
Research Instruments

No.	Variable		Indicator	Number of Questions
1	Digital Infrastructure (X1)	1.	Network Coverage	3
		2.	Service Level Agreement	3
		3.	Cloud	3
2	Cyber Security (X2)	1.	Cybersecurity Awareness	3
		2.	Cybersecurity Behavior	3
		3.	Cybersecurity Readiness	3
		4.	Cyber Resilience	3
3	Digital Public Service (Y)	1.	Digital Accessibility	3
		2.	Digital Efficiency	3
		3.	Transparency and Trust	3
		4.	Citizen Engagement	3

Sources:(Chowdhury et al., 2022; Finger & Montero, 2023; Priyanto, 2024; S. A. Ramadhan & Pribadi, 2024)

Additionally, Table 2 presents the design of the questions used in the questionnaire for this study:

Table 2.
Questionnaire Design

No	Variable	Question
1	Digital Infrastructure (X1)	1. Measure how extensive a digital infrastructure network covers an entire area, including remote areas. 2. Assess the strength and stability of the signal available for digital public service applications in various locations. 3. Measure the network's ability to provide services in areas with risks or challenges of suburban access. 1. Measure the percentage of time that a digital public service application operates without interruption.

No	Variable	Question
		2. Assess whether the service provider is meeting SLA promises regarding response time and recovery after an outage. 3. Measure how quickly and effectively the system can recover from failures or technical glitches in accordance with the terms of the SLA. 1. Data center or cloud capacity to handle large volumes of data and support digital public service applications. 2. Security measures and backup systems in place to ensure data is protected and available at all times. 3. The ability of the data center or cloud to manage the scalability of resources according to the operational needs of public applications.
2	Cyber Security (X2)	1. Knowledge of the types of cyber threats (phishing, malware, ransomware) 2. Awareness of the importance of using strong, unique passwords. 3. Knowledge about secure online behaviors and practices. 1. The habit of changing passwords regularly 2. Regular software updates to ensure security 3. Awareness and participation in cybersecurity training programs. 1. There is a regular data backup system 2. Staff are adequately trained to respond to cyber threats. 3. The existence of incident response protocols in case of a breach. 1. System recovery time after a cyberattack 2. The capacity of the system to operate during cyberattacks. 3. Availability of redundancy measures in the event of a security failure.
3	Digital Public Service (Y)	1. Ease of access to government services online 2. Availability of 24/7 access to online government services. 3. Accessibility of services for individuals with disabilities. 1. Automation of public service procedures (e-form, online tracking, e-payment) 2. The efficiency of digital services in reducing paperwork. 3. Response times for processing digital service requests. 1. Public access to service process information 2. Availability of clear terms and conditions for using digital services. 3. Public confidence in the fairness and transparency of online services. 1. Ease of providing input/suggestions through digital channels 2. Participation of citizens in online surveys and consultations. 3. Opportunities for real-time feedback on public services through digital platforms.

Sources: processed by researchers from various sources

Theoretical Framework

Digital Infrastructure (X1)

Digital infrastructure includes various elements that enable digital public services to be delivered efficiently and effectively (Finger & Montero, 2023). This variable consists of three main indicators: Network Coverage, Service Level Agreement, and Cloud.

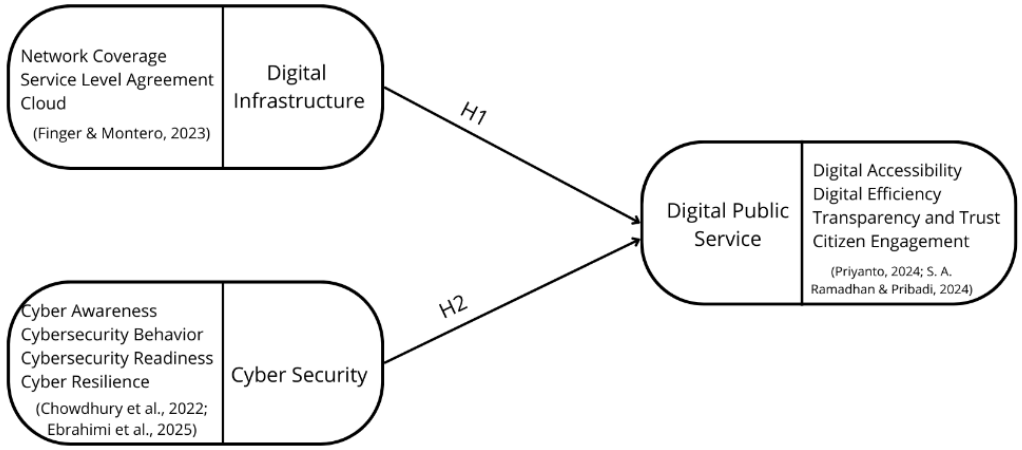
Cyber Security (X2)

Cybersecurity plays a crucial role in ensuring that data and information managed in digital public service systems remain safe and secure (Chowdhury et al., 2022; Ebrahimi et al., 2025). This variable is measured by four indicators: Cybersecurity Awareness, Cybersecurity Behavior, Cybersecurity Readiness, and Cyber Resilience.

Digital Public Service (Y)

Digital public services are a dependent variable in this study, which includes the effectiveness, inclusivity, and public trust in digital systems (Priyanto, 2024; S. A. Ramadhan & Pribadi, 2024). These variables are measured by four main indicators: Digital Accessibility, Digital Efficiency, Transparency and Trust, and Citizen Engagement.

Figure 4.
Digital Infrastructure, Cyber Security, and Digital Public Service Dimension



Sources: (Finger & Montero, 2023) (Chowdhury et al., 2022; Ebrahimi et al., 2025) (Priyanto, 2024; S. A. Ramadhan & Pribadi, 2024)

Based on Figure 4. The dimensions between variables can be hypothesized as follows:

H1: Digital Infrastructure has a significant impact on Digital Public Service
H2: Cyber Security has a significant effect on Digital Public Service

Data analysis

In this study, we analyzed the data using the Structural Equation Modeling (SEM) method with a Partial Least Squares (PLS) approach, utilizing SmartPLS software version 4. The SEM-PLS model was chosen for its capability to test complex relationships between latent variables, which in this case include Digital Infrastructure, Cybersecurity, and Digital Public Services.

Analysis Steps

1. **Validity and Reliability Testing**

Before proceeding with further analysis, the first step is to test the validity and reliability of the measurement model. This is done to ensure that each indicator used to measure the variables in the model is of good quality.

1. Convergent Validity: Using the Average Variance Extracted (AVE), which must be greater than 0.5 to indicate that the indicators measure the variable in question.
2. Reliability: Measured using Composite Reliability (CR) and Cronbach's Alpha. CR and Cronbach's Alpha values greater than 0.7 indicate good reliability of the measured construct.

2. **R-Square Testing (R^2)**

Once validity and reliability are confirmed, the next step is to calculate the R-square value to determine the proportion of variance in the dependent variable that can be explained by the independent variable in the model. Chin (1998), stated that a higher R^2 value indicates that the model can better explain the variance of the data. Interpretation of the R^2 value:

1. R^2 low: 0,19
2. R^2 medium: 0,33
3. R^2 tall: 0,67

3. **Hypothesis Test**

To test the hypothesis in this study, we conducted a hypothesis test using the bootstrapping technique available in SmartPLS. Bootstrapping is used to obtain t-statistics and p-values that allow us to test the significance of relationships between variables in the model.

1. If the t-statistic is greater than 1.96 and the p-value is less than 0.05, then the relationship between the variables is considered significant.

Hypothesis tests were carried out to test the influence of Digital Infrastructure and Cybersecurity on Digital Public Services, as well as to confirm whether these relationships are in accordance with the hypotheses proposed in this study.

RESULTS AND DISCUSSIONS

Respondent's demographic profile

Table 3 displays the demographic profile of the respondents, namely the users of the Tangerang Live application. In terms of gender, the majority of respondents were men, with a total of 249 people (62.25%), while women recorded 151 people (37.75%). In terms of age, most of the respondents were in the age range of 20-30 years, which was 193 people (48.25%), followed by the age group of 31-40 years, which included 118 people (29.50%). The age of 41-50 years was recorded for as many as 88 people (22.00%), with only one respondent being in the age of 51-60 years (0.25%). In terms of age, most of the respondents were in the age range of 20-30 years, which was 193 people (48.25%), followed by the age group of 31-40 years, which included 118 people (29.50%). The age of 41-50 years was recorded for as many as 88 people (22.00%), with only one respondent being in the age of 51-60 years (0.25%). For the last education category, most of the respondents had Diploma/Bachelor (D3/S1) education, as many as 193 people (48.25%), while Senior High School (SMA) was recorded as many as 118 people (29.50%), and Graduate (Postgraduate) 88 people (22.00%). Only one respondent had a final education in

Junior High School (SMP), which recorded a very small percentage (0.25%). In terms of jobs, most of the respondents were Students, who numbered 193 people (48.25%), followed by Self-employed, as many as 88 people (22.00%), and Private Employees, as many as 67 people (16.75%). PNS/TNI/POLRI recorded as many as 50 people (12.5%). Regarding the length of use of the application, most respondents have used the application for 1-2 years and 3-4 years (44.75%), while 21 people (5.25%) admitted to having used the application for 5-6 years.

Table 3.
Respondent demographics

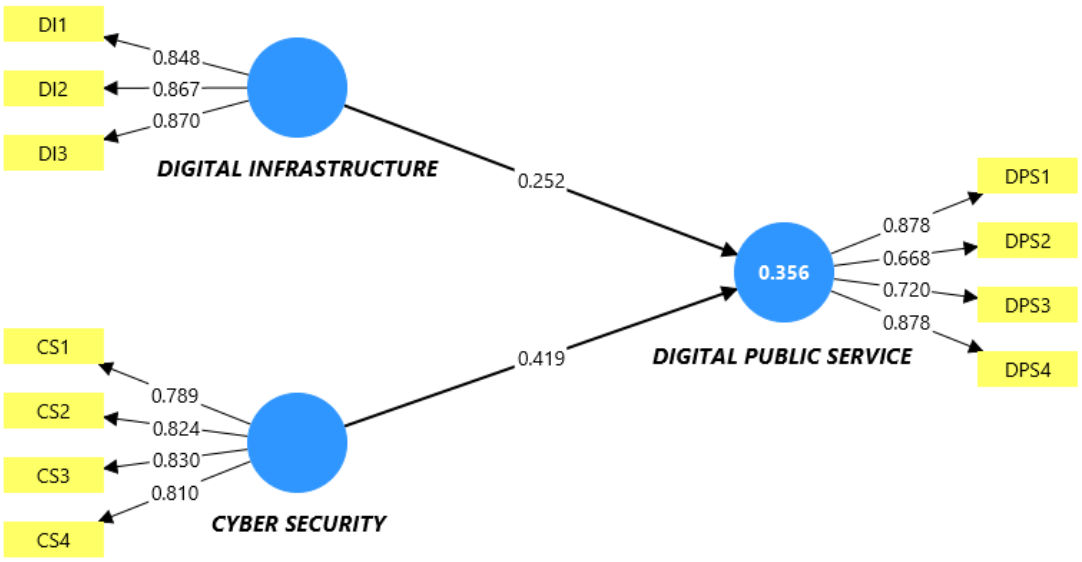
Characteristics of Respondents		
Gender	**Frequency**	**%**
Male	249	62.25%
Female	151	37.75%
Age		
20-30 Years	193	48.25%
31-40 Years	118	29.50%
41-50 Years	88	22.00%
51-60 Years	1	0.25%
Education Level		
Diploma/Bachelor	193	48.25%
Senior High School	118	29.50%
Graduate	88	22.00%
Junior High School	1	0.25%
Work		
Student/Student	193	48.25%
PNS/TNI/POLRI	50	12.5%
Self employed	88	22.00%
Private Employees	67	16.75%
long use of the application		
1-2 Years	179	44.75%
3-4 Years	179	44.75%
5-6 Years	21	5.25%

Sources: processed by researchers

The following section presents the findings of a study that analyzes the factors affecting digital infrastructure and cybersecurity systems in Tangerang City, especially related to digital public

services through the Tangerang LIVE application. These relationships are investigated using a *Structural Equation Modeling* (SEM) approach, as illustrated in the diagram below.

Figure 5.
Path coefficient graph



Source: Processed by the author using SmartPLS

Figure 5 indicates a coefficient path, structural equation modeling (SEM), that illustrates the relationship between Digital Infrastructure, Cyber Security, and Digital Public Service. Digital Infrastructure has a significant effect on Digital Public Service, with a path coefficient of 0.252, although the effect is lower than Cyber Security. Strong infrastructure supports accessibility and efficiency, but cybersecurity is more dominant in building public trust in digital service applications.

Cybersecurity shows a greater influence on Digital Public Service with a path coefficient of 0.419. Factors such as Cybersecurity Awareness, Cybersecurity Readiness, and Cyber Resilience play a major role in improving data protection and strengthening user trust in digital services. Digital Public Service is measured through indicators such as Efficiency, Accessibility, Transparency, Trust, and Citizen Engagement, all of which are influenced by cybersecurity and digital infrastructure.

The SEM model shows that cybersecurity has a greater influence on the quality of Digital Public Services than Digital Infrastructure. Strong security and adequate digital infrastructure are key to providing efficient, secure, and trustworthy digital public services.

Descriptive Statistics (n = Number of Respondents)

Table 4.
Descriptive Statistics

	n	Minimum	Median	Maximum	Mean	Standard Deviation
Digital Infrastruktur	400	1,000	4,000	5,000	3,806	0,739
Cyber Security	400	2,000	4,000	5,000	3,756	0,697

	n	Minimum	Median	Maximum	Mean	Standard Deviation
Digital Public Service	400	1,000	4,000	5,000	4,108	0,774

Source: Processed by the author using SmartPLS

Table 3 shows descriptive statistics for three main variables, namely Digital Infrastructure, Cybersecurity, and Digital Public Services, with each having n (number of samples) as many as 400 respondents. For Digital Infrastructure, an average score of 3,806 and a median of 4,000 indicate that most respondents rate digital infrastructure at a relatively high level. The range of Digital Infrastructure values is between 1,000 (minimum) and 5,000 (maximum), with a standard deviation of 0.739, which indicates a fairly low variation in respondents' answers. As for Cybersecurity, the average score was slightly lower, at 3,756, with a median of 4,000. The range of Cybersecurity values is also between 2,000 and 5,000, and has a standard deviation of 0.697, which indicates a relatively small variation. For Digital Public Services, the highest average score was recorded at 4,108, which shows the respondents' positive assessment of digital public services. The median value is also at 4,000, with the same value range between 1,000 (minimum) and 5,000 (maximum), and a standard deviation of 0.774, which indicates a slightly higher variation from the previous two variables. Based on the descriptive statistical table, the three variables show a relatively positive assessment of respondents, with small variations, showing the consistency of respondents' views on digital infrastructure, cybersecurity, and digital public services.

Results of reliability and validity measurements

Table 5.
Reliability and Validity

	Cronbach's Alpha	Composite Reliability (rho_A)	Composite Reliability (rho_C)	Average Variance Extracted (AVE)	
Digital Infrastructure	0.827	0.828	0.896	0.742	Valid
Cyber Security	0.830	0.833	0.886	0.661	Valid
Digital Public Service	0,794	0.793	0.869	0.627	Valid

Source: Processed by the author using SmartPLS

Table 4 shows excellent reliability measures for the three variables used in this study, namely Digital Infrastructure, Cybersecurity, and Digital Public Services. Cronbach's Alpha values for all three variables were above 0.7, with Digital Infrastructure reaching 0.827, Cyber Security 0.830, and Digital Public Service 0.794, indicating good internal reliability. The Composite Reliability (rho_A) and Composite Reliability (rho_C) for these three variables also showed high values, with values greater than 0.8, indicating excellent composite reliability. In addition, the Extracted Average Variance (AVE) for each variable shows values above 0.5, with Digital Infrastructure reaching 0.742, Cyber Security 0.661, and Digital Public Service 0.627, indicating adequate convergent validity. Hair et al. (2019) state that reliability and validity are said to be valid if the values of Alpha Cronbach, Composite Reliability, and AVE are above the accepted threshold, which is more than 0.7 for Alpha Cronbach and Composite Reliability, and more than 0.5 for AVE.

Table 6.
Fornell-Lacker Criterion

	Cyber Security	Digital Infrastructure	Digital Public
Cyber Security	0,813		
Digital Infrastructure	0,555	0,862	
Digital Public Service	0,556	0,485	0,792

Source: Processed by the author using SmartPLS

In this table, the values on the diagonal (0.813, 0.862, 0.792) represent the root of the Average Variance Extracted (AVE) for each construct: Cybersecurity, Digital Infrastructure, and Digital Public Services. A high AVE value indicates that each construction has a good level of explanation of the variables being measured. Meanwhile, the values on the off diagonal (0.555, 0.485, 0.556) show a correlation between different constructs. Fornell and Larcker (1981) in (Ab Hamid et al., 2017), states that in order to ensure the discriminative validity between constructs, the root of the Average Variance Extracted (AVE) of each construct must be greater than the correlation between constructs. In this case, the root of AVE is greater than the correlation between constructs, which means that the constructions are quite separate and have good discriminant validity. Thus, it can be concluded that Cybersecurity, Digital Infrastructure, and Digital Public Services have a valid relationship but remain well separated in this SEM model.

Table 7.
Heterotrait-monotrait Ratio (HTMT)

	Cyber Security	Digital Infrastructure	Digital Public
Cyber Security			
Digital Infrastructure	0,667		
Digital Public Service	0,680	0,592	

Source: Processed by the author using SmartPLS

The values in the table show the correlation between different constructs (heterotraits) and between the same constructs (monotraits). HTMT scores for Cybersecurity and Digital Infrastructure (0.667), Cybersecurity and Digital Public Services (0.680), and Digital Infrastructure and Digital Public Services (0.592). According to Henseler et al., (2015), HTMT values lower than commonly used thresholds (usually 0.85 or 0.90) indicate that the constructs are well separated and do not experience significant overlap. This suggests that the three constructs are fairly closely related but remain well separated, which supports the validity of the discriminators in the model. In other words, the Cybersecurity, Digital Infrastructure, and Digital Public Services constructs each measure different aspects and do not overlap significantly, indicating that they can be considered valid and separate constructs in this SEM model.

R-square

Table 8.
R-square

	R-square	
Digital Public Service	0.356	Moderat

Source: Processed by the author using SmartPLS

Table 5 shows the R-squared (R^2) value for the Digital Public Service variable, which has a value of 0.356. This R^2 value shows how much variability of Digital Public Service can be explained by a model involving Digital Infrastructure and Cyber Security as independent variables. In this case,

a value of 0.356 indicates that about 35.6% of the variation in Digital Public Service can be explained by both factors.

(Chin, 1998), stated that the R^2 value of 0.356 can be categorized as moderat, which means that there are other factors besides Digital Infrastructure and Cyber Security that play a role in determining the quality of Digital Public Service. This shows that although Digital Infrastructure and Cyber Security have a significant influence, there are still many other variables that need to be considered to fully understand Digital Public Service. However, to ensure consistency in the use of thresholds, the study can also refer to the guidelines of Hair et al., (2019), which classifies R^2 with a threshold of 0.25 for low, 0.50 for moderat, and 0.75 for high. Using the Hair guideline, an R^2 of 0.356 would fall into the low category, suggesting that this model still has the potential to explain more variation in Digital Public Service.

Hypothesis Test

Table 9.
Hypothesis Test

	Original Sample (O)	Average Sample (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Value	
Digital Infrastructure -> Digital Public Service	0.419	0.422	0.043	9.801	0.000	Accepted
Cyber Security -> Digital Public Service	0.252	0.253	0.043	5.198	0.000	Accepted

Source: Processed by the author using SmartPLS

Table 6 shows the results of the Hypothesis Test, which tests two main relationships, namely Digital Infrastructure to Digital Public Service and Cyber Security to Digital Public Service.

1. Digital Infrastructure to Digital Public Service shows a very high Statistical T value, which is 9,801, with a very low P Value (0.000), which means that this relationship is very statistically significant. The identical Original Sample (O) and Average Sample (M) values (0.419 and 0.422) indicate that this model is excellent at describing the relationship between digital infrastructure and digital public services. This indicates that improving the quality of digital infrastructure is closely related to improving the efficiency of digital public services.
2. Cyber Security on Digital Public Services, despite the lower T Statistics value (5,198) and the still significant P Value (0.000), shows a positive and significant influence, although it is smaller than Digital Infrastructure. Nonetheless, these results indicate that cybersecurity continues to have an important role to play in reducing the digital divide, especially in increasing public trust in the use of digital public service applications.

Table 10.
F-Square

	Digital Security	Digital Infrastructure	Digital Public Service
Cyber Security			0.189
Digital Infrastructure			0.068
Digital Public Service			

Source: Processed by the author using SmartPLS

In the F-Square table, it can be seen that the Cyber Security construct has an F^2 value of 0.189 for Digital Public Service, while Digital Infrastructure is only 0.068. The interpretation of this value refers to the guidelines of the Hair et al., (2019b), which states that the F^2 value of 0.02 is considered small, 0.15 as medium, and 0.35 as large. Therefore, it can be concluded that Cyber Security contributes that is being explained in explaining the variation in Digital Public Service, while the contribution of Digital Infrastructure is at a small level.

Table 11.
Q-Square

	Q^2Predict
Digital Public Service	0.211

Source: Processed by the author using SmartPLS

Based on the Q^2 Predict result of 0.211, it can be concluded that the model has moderate predictive ability in explaining variations in digital public services. This shows that variables such as digital infrastructure and cybersecurity are quite relevant as predictors, but do not include all factors that affect the quality of these services. Hair et al., (2019b), It falls into the moderate category as it is in the range of 0.15 – 0.34.

DISCUSSION

This discussion aims to analyze the results of research related to the influence of digital infrastructure and cybersecurity on digital public services in Tangerang City, especially in the Tangerang LIVE application. The results show that these two factors have a very significant role in influencing the quality of digital public services, but with different roles in their contribution to efficiency and public trust.

Digital infrastructure has proven to have a strong influence on digital public services. Good and adequate infrastructure, such as a stable communication network, advanced hardware, and an integrated data management system, contributes directly to the ease of access and speed in service delivery. This research is in line with the findings of Romanenkov (2021), who stated that digital infrastructure plays a key role in increasing the efficiency and public trust in government services by providing better and faster access to the public. Moreover, Yao et al. (2025) add that digital infrastructure can strengthen a region's innovation capabilities, which is key to advancing the public sector and improving the quality of services provided.

However, more interesting results suggest that cybersecurity has a greater influence on digital public services. Good security plays an important role in building public trust in digital public service applications. In an increasingly connected world, people are more likely to use digital services if they feel their data is well protected. Cybersecurity Awareness, Cybersecurity Readiness, and Cyber Resilience are key factors in maintaining the integrity and privacy of user data. This is supported by research of Mijwil et al. (2023), emphasizing the importance of governance in cybersecurity to support the digitization of public services and ensure the security of user data. With the right security policies, digital transformation can run effectively and safely. Moreover, Rudnev et al. (2024) added that the rapid development of cyber threats amid digital transformation requires greater investment in cybersecurity, which is a pillar to maintain the financial stability of companies and critical infrastructure. His research shows that attacks on critical infrastructure can cause enormous financial losses, which emphasizes the importance of adequate policies and technology in dealing with them. Sandhu (2021), also stated that cybersecurity is an integral part of secure digital transformation, especially in critical sectors such as energy, water, and telecommunications. The application of advanced technologies such as AI and blockchain can be a solution to deal with growing cyber threats. Effective cybersecurity

is essential to prevent hacks that can undermine the integrity of the system and undermine public trust in the government's digital service system.

In addition, one of the main challenges found is the digital divide, where areas with limited internet access or inadequate devices experience difficulties in accessing digital services. Brunetti et al. (2020) show that inequality in access to technology can hinder the equitable distribution of digital public services. Therefore, it is important for governments to focus on strengthening infrastructure in remote areas and providing inclusive solutions for all levels of society, so that digital transformation can run fairly and equitably. Shah et al. (2025) emphasize that equitable access to technology in underdeveloped regions is the key to creating social justice in the use of digital public services. In the field of cybersecurity, it includes a need to increase cyber resilience at the system level. Cyber Resilience, which focuses on the system's ability to recover from disruptions or threats, is critical to keeping applications running even in the event of a technological attack or disaster. Yusif & Hafeez-Baig (2021) emphasize that effective cybersecurity can help maintain the sustainability of application operations without being disrupted by external threats. Xu (2019). It also shows that the ability to recover systems after a digital attack or disaster is a decisive factor in ensuring the continuity of public services.

Policy Implications

Based on the findings that Cyber Security has a greater influence (F^2 = 0.189) than Digital Infrastructure (F^2 = 0.068) on Digital Public Services, policy recommendations are focused on increasing cybersecurity capacity in an operational and measurable manner.

The following are concrete recommendations prepared in the form of priority tables based on impact and feasibility.:

Table 12.
Prioritization Matrix (Impact vs. Feasibility)

No	Operational Recommendations	Impact	Feasibility	Priority
1	Security awareness improvement program for ASN and residents	High	High	1
2	Preparation and implementation of Incident Response Playbook for regional agencies	High	Moderat	2
3	Network redundancy for critical digital service systems	Moderat	Moderat	3
4	Implementation of information security audits based on ISO 27001 periodically	High	Low	4
5	Implementation of limited program bounty bugs in collaboration with the hacker ethical community	Moderat	Low	5

Source: Processed by the author

Based on the results of the study showing that the Cyber Security variable has a greater influence than Digital Infrastructure on Digital Public Services, the policy recommendations given are directed at concrete operational steps that have a direct impact. One of the most feasible and high-impact first steps is the implementation of a security awareness program aimed at state civil servants (ASN) and the public. This program can be implemented through online training, digital campaigns, and the integration of security materials in the new ASN onboarding process, to instill a basic understanding of threats and safe practices in the government's digital ecosystem. In addition, it is recommended that local governments compile and implement the Incident Response Playbook, which is a guide or operational SOP in dealing with various forms of security incidents such as phishing, DDoS attacks, or data leaks. The existence of this document will increase the readiness and speed of agencies in responding to incidents, as well as minimize the impact on public services. On the infrastructure side, it is necessary to

implement network redundancy, for example using failover systems and server backups to ensure the continuity of digital public services in emergency situations. Although the initial investment is considerable, this step is important to guarantee consistent service availability.

Furthermore, the regular implementation of security audits based on ISO 27001 standards is also recommended as part of efforts to build a credible and sustainable information security management system. However, this policy demands greater resource allocation as well as long-term commitment from top management. Finally, local governments can also consider implementing a limited bug bounty, which is an incentive program for system vulnerability reporters from the digital security community (ethical hackers). Although technically promising, the implementation of this policy still faces regulatory challenges and bureaucratic culture that is not fully prepared.

CONCLUSION

This study shows that both Digital Infrastructure and Cyber Security contribute significantly to the transformation of digital public services, with Cyber Security having a greater influence statistically ($F^2 = 0.189$) than Digital Infrastructure ($F^2 = 0.068$). The constructed structural model produced an R^2 value of 0.356, which is included in the moderate category according to the criteria of Hair et al., (2019b), as well as a Q^2 Predict value of 0.211 which indicates moderate predictive ability. These findings imply that while both exogenous variables are able to explain some of the variations in digital public services, there is still room to include other variables that have the potential to improve the model's cruising.

However, this study has methodological limitations. A moderate R^2 value indicates that this model has not been able to capture the overall factors that affect the effectiveness of public digital services. Therefore, further research is recommended to develop a more comprehensive model by considering mediation mechanisms, for example through construct trust (user trust), which can theoretically bridge the relationship between cybersecurity and the adoption of digital services. In addition, moderation analysis is also important to explore whether the relationships between variables are influenced by factors such as digital literacy, the age of the user, or the experience of using technology.

To reinforce the external validity and generalization of results, future research is also recommended using a longitudinal design approach, to capture changes in user perception and behavior over time. Furthermore, the application of multi-group analysis based on demographic dimensions (such as gender, education level, length of employment, or intensity of use of digital service applications) can provide sharper insights into the differences in influence patterns between population segments. With this approach, the results of the research are expected to be not only statistically relevant but also have a high practical utility in evidence-based public policy formulation.

REFERENCES

Ab Hamid, M. R., Sami, W., & Mohmad Sidek, M. H. (2017). Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion. *Journal of Physics: Conference Series*, *890*(1). https://doi.org/10.1088/1742-6596/890/1/012163

Abdussamad, Z. (2024). Enhancing Public Service Delivery through Digital Transformation: Challenges and Opportunities in the Era of E-Government. *Pakistan Journal of Life and Social Sciences (PJLSS)*, *22*(2), 22539–22551. https://doi.org/10.57239/pjlss-2024-22.2.001601

Aditya, T. (2023). Smart City Implementation: Analysis of Citizens' Behavior Through Utilization

of the “Tangerang-LIVE” Mobile Application to Improve Public Services during the Covid-19 Pandemic in Tangerang City. *Jurnal Pembangunan Kota Tangerang*, *1*(1), 44–66.

Aditya, T., Ningrum, S., Nurasa, H., & Irawati, I. (2023). Community needs for the digital divide on the smart city policy. *Heliyon*, *9*(8), e18932. https://doi.org/10.1016/j.heliyon.2023.e18932

AlNuaimi, B. K., Kumar Singh, S., Ren, S., Budhwar, P., & Vorobyev, D. (2022). Mastering digital transformation: The nexus between leadership, agility, and digital strategy. *Journal of Business Research*, *145*(September 2021), 636–648. https://doi.org/10.1016/j.jbusres.2022.03.038

Aminah, S., & Saksono, H. (2021). Digital transformation of the government: A case study in Indonesia. *Jurnal Komunikasi: Malaysian Journal of Communication*, *37*(2), 272–288. https://doi.org/10.17576/JKMJC-2021-3702-17

Aulia, R. (2019). Strategi Komunikasi Pemerintah Kota Tanggerang Via Aplikasi TAnggerang Live Dalam Menyampaikan Informasi Kepada Masyarakat Di Kota Tangerang. In *Universitas Sultan Ageng Tirtayasa*.

Balozian, P., Leidner, D., & Xue, B. (2021). Toward an intellectual capital cyber security theory: insights from Lebanon. *Journal of Intellectual Capital*, *23*(6), 1328–1347. https://doi.org/10.1108/JIC-05-2021-0123

Borah, P. S., Iqbal, S., & Akhtar, S. (2022). Linking social media usage and SME’s sustainable performance: The role of digital leadership and innovation capabilities. *Technology in Society*, *68*(October 2021), 101900. https://doi.org/10.1016/j.techsoc.2022.101900

Brunetti, F., Matt, D. T., Bonfanti, A., De Longhi, A., Pedrini, G., & Orzes, G. (2020). Digital transformation challenges: strategies emerging from a multi-stakeholder approach. *The TQM Journal*, *32*(4), 697–724. https://doi.org/10.1108/TQM-12-2019-0309

Cazier, J. (2007). An empirical investigation: health care employee passwords and their crack times in relationship to HIPAA security standards. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, *2*(3). https://doi.org/10.4018/jhisi.2007070104

Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, *113*, 102551. https://doi.org/https://doi.org/10.1016/j.cose.2021.102551

Chung, A., Dawda, S., Hussain, A., Shaikh, S. A., & Carr, M. (2021). *Cybersecurity: Policy BT - Encyclopedia of Security and Emergency Management* (L. R. Shapiro & M.-H. Maras (eds.); pp. 203–211). Springer International Publishing. https://doi.org/10.1007/978-3-319-70488-3_20

Cresswell, J. W. (2018). Research Design Qualitative, Quantitative, and Mixed Methods Approaches. In *Sage Publishing* (Fifth Edit). SAGE Publications Inc. https://doi.org/10.4324/9780429469237-3

De Araujo, L. M., Priadana, S., Paramarta, V., & Sunarsi, D. (2021). Digital leadership in business organizations: An overview. *Int. J. Educ. Adm. Manag. Leadersh*, *2*(1), 45–56.

De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology*, *30*(1), 68–87. https://doi.org/10.1093/ijlit/eaac004

Deokryong Yoon, Yaewon Hyun, S. K. (2022). Digitalization: A Government-Driven, Infrastructure-First Approach. *Global Solutions Journal*, *9*.

Desai, A., & Manoharan, A. P. (2024). Digital Transformation and Public Administration: The Impacts of India’s Digital Public Infrastructure. *International Journal of Public Administration*, *47*(9), 575–578. https://doi.org/10.1080/01900692.2024.2350762

Dinas Komunikasi dan Informasi Kota Tangerang. (2022). *Data Tangerang Live* (p. 5). Dinas Komunikasi dan Informasi Kota Tangerangg.

Ebrahimi, E., Pare, M., Stoker, G., & White, S. (2025). Cybersecurity Early Education: A Review of Current Cybersecurity Education for Young Children. *International Conference on Computer Supported Education, CSEDU - Proceedings*, *1*, 822–833. https://doi.org/10.5220/0013501000003932

Erkut, B. (2020). From digital government to digital governance: Are we there yet? *Sustainability (Switzerland)*, *12*(3), 1–13. https://doi.org/10.3390/su12030860

Finger, Matthias, & Montero, Juan. (2023). Digitalizing infrastructure, digital platforms and public services. *Competition and Regulation in Network Industries*, *24*(1), 40–53. https://doi.org/10.1177/17835917231156099

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840. https://doi.org/https://doi.org/10.1016/j.cose.2022.102840

Giest, S., & Samuels, A. (2023). Administrative burden in digital public service delivery: The social infrastructure of library programs for e-inclusion. *Review of Policy Research*, *40*(5), 626–645. https://doi.org/https://doi.org/10.1111/ropr.12516

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019a). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019b). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Henriques de Gusmão, A. P., Mendonça Silva, M., Poleto, T., Camara e Silva, L., & Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management*, *43*, 248–260. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.08.008

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*, *37*(3), 101493. https://doi.org/10.1016/j.giq.2020.101493

Janssen, M., & van der Voort, H. (2020). Agile and adaptive governance in crisis response: Lessons from the COVID-19 pandemic. *International Journal of Information Management*, *June*, 102180. https://doi.org/10.1016/j.ijinfomgt.2020.102180

Khaw, T. Y., Teoh, A. P., Abdul Khalid, S. N., & Letchmunan, S. (2022). The impact of digital leadership on sustainable performance: a systematic literature review. *Journal of Management Development*, *41*(9–10), 514–534. https://doi.org/10.1108/JMD-03-2022-0070

Kianpour, M., Kowalski, S. J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, *116*, 102493. https://doi.org/https://doi.org/10.1016/j.simpat.2022.102493

Klappe, E. S., De Keizer, N. F., & Cornet, R. (2020). Factors Influencing Problem List Use in Electronic Health Records-Application of the Unified Theory of Acceptance and Use of Technology. *Applied Clinical Informatics*, *11*(3), 415–426. https://doi.org/10.1055/s-0040-1712466

Kosasih, A., & Aditya, T. (2024). Digital Leadership dalam Digital Governance untuk Pelayanan Publik Digital di Kota Tangerang. *JIHHP: Jurnal Ilmu Hukum, HUmaniora Dan Politik*, *5*(1), 639–652.

Lafioune, N., Desmarest, A., Poirier, É. A., & St-Jacques, M. (2023). Digital transformation in municipalities for the planning, delivery, use and management of infrastructure assets:

Strategic and organizational framework. *Sustainable Futures*, *6*, 100119. https://doi.org/https://doi.org/10.1016/j.sftr.2023.100119

Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), 10. https://doi.org/10.1186/s42400-020-00050-w

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, M., Yu, G., & Pu, J. (2025). Digital rural construction enables synergistic development of agricultural economy and ecological environment: Based on the analysis of mediating effect and spatial spillover effect. *Journal of Chinese Agricultural Mechanization*, *46*(5), 322–333. https://doi.org/10.13733/j.jcam.issn.2095-5553.2025.05.042

Lindgren, I., & van Veenstra, A. F. (2018). Digital government transformation: a case illustrating public e-service development as part of public sector transformation. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. https://doi.org/10.1145/3209281.3209302

Mijwil, M. M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian Journal of CyberSecurity*, *2023*, 1–6. https://doi.org/10.58496/MJCS/2023/001

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. In *Sensors* (Vol. 22, Issue 2). https://doi.org/10.3390/s22020538

Mulyana, R., Rusu, L., & Perjons, E. (2021). IT governance mechanisms influence on digital transformation: A systematic literature review. *27th Annual Americas Conference on Information Systems, AMCIS 2021*, 0–10.

Nalley, C. (2022). Cybersecurity Best Practices for the Audiologist. *The Hearing Journal*, *75*(7). https://journals.lww.com/thehearingjournal/fulltext/2022/07000/cybersecurity_best_practices_for_the_audiologist.1.aspx

Naranjo, P. G. V., Pooranian, Z., Shojafar, M., Conti, M., & Buyya, R. (2019). FOCAN: A Fog-supported smart city network architecture for management of applications in the Internet of Everything environments. *Journal of Parallel and Distributed Computing*, *132*, 274–283. https://doi.org/10.1016/j.jpdc.2018.07.003

Nurunnisa, S., Girsang, E., & Lestari Ramadhani Nasution, S. (2023). Analysis Of The Effect Of The Process Of Issuing Health Personnel Licenses Using The Sipandu Medan Application On Health Worker Satisfaction In Dpmptsp Medan City. *International Journal of Health and Pharmaceutical (IJHP)*, *3*(4), 602–611. https://doi.org/10.51601/ijhp.v3i4.209

Obaid, T., Eneizan, B., Naser, S. S. A., Alsheikh, G., Ali, A. A. A., Abualrejal, H. M. E., & Gazem, N. A. (2022). Factors Contributing to an Effective E- Government Adoption in Palestine. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 127, pp. 663–676). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-98741-1_55

Paiva, L. H., Cotta, T. C., & Barrientos, A. (2019). "Great Policy Successes" Chapter 2: Brazil's Bolsa Família Programme. *Journal of Comparative Policy Analysis: Research and Practice*, 1–333.

Priscilla, I., Igbokwe-Ibeto, C. J., & Chris Nwafor, C. (2024). Challenges and Opportunities in Implementing Digital Transformation in Nigerian Public Service. *Journal of the Management Sciences*, *60*(3), 296–308. https://journals.unizik.edu.ng/jfms/article/view/3731

Priyanto, H. (2024). Public Service Quality in Banyuwangi District: A Study in Welfare Perspective. *Jurnal Manajemen Pelayanan Publik*, *8*(1), 77–94.

https://doi.org/10.24198/jmpp.v8i1.48657

Ramadhan, R., Arifianti, R., & Riswanda, R. (2019). Implementasi e-Government di Kota Tangerang menjadi Smart City (Studi Kasus Aplikasi Tangerang Live). *Responsive*, *2*(4), 140–156. https://doi.org/10.24198/responsive.v2i3.26083

Ramadhan, S. A., & Pribadi, U. (2024). Building Citizen Satisfaction with E-Government Services: A Case Study of the Population Administration Information System (SIAK). *Jurnal Manajemen Pelayanan Publik*, *8*(3), 972–988. https://doi.org/10.24198/jmpp.v8i3.55866

Romanenkov, A. M. (2021). Digital public administration infrastructure and its effectiveness. *Personality & Society*, *2*(3), 4–10. https://doi.org/10.46502/issn.2712-8024/2021.3.1

Rosyidah, I. N. (2017). *Efektivitas Kmunikasi Humas Pemkot Tangerang dalam Implementasi Aplikasi "Tangerang LIVE."* Universitas Islam Negeri Syarif Hidayatullah.

Rudnev, S., Zolkin, A., Artemyev, N., & Tychkov, A. (2024). THE ECONOMIC IMPORTANCE OF CYBERSECURITY FOR ENTERPRISES IN THE CONTEXT OF DIGITAL TRANSFORMATION. *EKONOMIKA I UPRAVLENIE: PROBLEMY, RESHENIYA*, *11/2*, 46–55. https://doi.org/10.36871/ek.up.p.r.2024.11.02.006

Safitra, M. F., Lubis, M., & Kurniawan, M. T. (2023). Cyber Resilience: Research Opportunities. *Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering*, 99–104. https://doi.org/10.1145/3592307.3592323

Sandhu, K. (2021). Advancing Cybersecurity for Digital Transformation. *Handbook of Research on Advancing Cybersecurity for Digital Transformation*. https://doi.org/10.4018/978-1-7998-6975-7.ch001

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4

Schinagl, S., Shahim, A., Khapova, S., & van den Hooff, B. (2023). Digital security governance: What can we learn from high reliability organizations? *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2023-Janua*, 5938–5948.

Schiuma, G., Schettini, E., Santarsiero, F., & Carlucci, D. (2022). The transformative leadership compass: six competencies for digital transformation entrepreneurship. *International Journal of Entrepreneurial Behaviour and Research*, *28*(5), 1273–1291. https://doi.org/10.1108/IJEBR-01-2021-0087

Serrano, W. (2018). Digital Systems in Smart City and Infrastructure: Digital as a Service. In *Smart Cities* (Vol. 1, Issue 1, pp. 134–154). https://doi.org/10.3390/smartcities1010008

Setyawati, D. N., & Fitriati, R. (2023). Digital Governance in Information Disclosure. *Jurnal Kebijakan Publik*, *14*(1), 48. https://doi.org/10.31258/jkp.v14i1.8217

Shah, F., Shah, A., Jadul, & Jabbar, A. (2025). The Impact of E-Governance Implementation on Public Trust and the Efficiency of Service Delivery. *Annual Methodological Archive Research Review*, *3*(3), 54–62. https://doi.org/10.63075/3yey1t51

Singh, C., & Pankaj, P. (2022). Digital Infrastructure Management-Challenges and Opportunities in Post Covid Era. *Cardiometry*, *23*, 593–596. https://doi.org/10.18137/cardiometry.2022.23.593596

Smyrnova, I., Akimov, O., Krasivskyy, O., Shykerynets, V., Kurovska, I., Hrusheva, A., & Babych, A. (2021). Analysis of The Application of Information and Innovation Experience in The Training of Public Administration Specialists. *IJCSNS International Journal of Computer Science and Network Security*, *21*(3), 120.

Srebalová, M., & Peráček, T. (2022). Effective Public Administration as a Tool for Building Smart Cities: The Experience of the Slovak Republic. *Laws*, *11*(5), 1–16. https://doi.org/10.3390/laws11050067

Tangerang, P. K. (2022). *Profile Kota Tangerang*.

Tholok, F. W., Santosa, S., & Janamarta, S. (2019). Studi Ketertarikan Masyarakat Terhadap

Penggunaan Aplikasi Tangerang Live (Pendekatan Pada Teori Skala SERVQUAL). *Primanomics: Jurnal Ekonomi & Bisnis*, *17*(2), 120–129.

Thompson, N., Mullins, A., & Chongsutakawewong, T. (2020). Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. *Government Information Quarterly*, *37*(1). https://doi.org/10.1016/j.giq.2019.101408

Topcuoglu, E., Oktaysoy, O., Erdogan, S. U., Kaygin, E., & Karafakioglu, E. (2023). The Mediating Role of Job Security in the Impact of Digital Leadership on Job Satisfaction and Life Satisfaction. *Marketing and Management of Innovations*, *4511*(1), 122–132.

Tyagi, S. (2024). Bibliometric analysis and scientific mapping of research trends on 'digital divide.' *Global Knowledge, Memory and Communication*, *ahead-of-p*(ahead-of-print). https://doi.org/10.1108/GKMC-10-2023-0376

Verma, R., Bharti, U., & Tripathi, U. (2022). Digital Era and Its Impact on Leadership Transformation. *Sachetas*, *1*(2), 36–41. https://doi.org/10.55955/120003

Xu, S. (2019). Cybersecurity Dynamics: A Foundation for the Science of Cybersecurity BT. In C. Wang & Z. Lu (Eds.), *Proactive and Dynamic Network Defense* (pp. 1–31). Springer International Publishing. https://doi.org/10.1007/978-3-030-10597-6_1

Yan, X., & Li, T. (2022). Construction and application of urban digital infrastructure—practice of "Urban Brain" in facing COVID-19 in Hangzhou, China. *Engineering, Construction and Architectural Management*, *30*(8), 3123–3141. https://doi.org/10.1108/ECAM-10-2021-0935

Yao, L., Li, A., & Yan, E. (2025). Research on digital infrastructure construction empowering new quality productivity. *Scientific Reports*, *15*(1), 6645. https://doi.org/10.1038/s41598-025-90811-9

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995

Zuckerman, E. (2020). *An essay, in the form of an FAQ, about the possibility of digital social spaces built with taxpayer dollars*. *November*, 1–20.