information

MDPI

Article

Digital Transformation in Governmental Public Service Provision and Usable Security Perception in Saudi Arabia

Saqib Saeed

Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; sbsaed@iau.edu.sa

Abstract: Usable security and privacy in public services are critical considerations in today's digital age, where governments increasingly rely on technology to deliver services efficiently while safeguarding sensitive information. Successful usage of these electronic services depends on citizens' trust level in e-government channels. Therefore, the design of these public service organizations should consider the usability aspect of security controls. In this paper, we present the results of a quantitative study conducted in Saudi Arabia to understand end users' perceptions regarding usable security and privacy in their public service usage. Based on the findings, we present a model to further improve the usable security and privacy aspects, which will help policymakers and practitioners improve public service provision by electronic means. The model can be further refined in different geographical contexts to improve cybersecurity in e-government service provision through the integrated efforts of citizens, service-providing organizations and government cybersecurity agencies.

Keywords: digital transformation; e-government; usable security and privacy; sustainability; user-centered privacy; user security

check for updates

Academic Editors: Huseyin Dogan, Hossein Abroshan and Nader Sohrabi Safa

Received: 12 February 2025
Revised: 15 March 2025
Accepted: 18 March 2025
Published: 19 March 2025

Citation: Saeed, S. Digital Transformation in Governmental Public Service Provision and Usable Security Perception in Saudi Arabia. *Information* **2025**, *16*, 247. https://doi.org/10.3390/info16030247

Copyright: © 2025 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Digital technologies are critical for organizations to be efficient, gain competitive advantages, and increase their speed to market [1]. Digital technologies can enable organizations to manage the supply chain effectively by enhancing the stakeholders' experience and product value [2]. Customized interactions with customers, automated processes, and artificial intelligence-enabled applications can help in improving user experiences. Secondly, digital technologies help automate processes, improve decision making, and allow collaborative work for better productivity [3]. Furthermore, digital technologies help with making organizations agile and developing new business models for better scalability of their services. Digital transformation has gained enormous momentum in all business sectors in the post-COVID era. However, for smooth and sustainable adoption of digital technologies, considerable challenges need to be taken care of. Therefore, a strategic approach needs to be adopted to handle digital transformation initiatives [4,5].

Governmental organizations strive hard to optimally provide public services to their citizens [6]. Keeping in mind the benefits of digital transformation, governmental organizations also started adopting digital channels to provide public services. The adoption of digital services in governmental projects is affected by economic, social, technical, and cultural challenges. As a result, the adoption of digital infrastructure is not uniform across governments [7]. Governments require huge investments to build digital infrastructures and deliver public services efficiently and securely. To foster a sustainable digital

transformation, governments need to develop the trust of citizens that digital channels of government services are secure, efficient, and user-friendly. This way, governments can support citizens in rural and distant regions with the same quality level as that in cities. The adoption of user-centric approaches can help with designing technological systems aligned with user needs and practices [8]. Furthermore, governments may need to introduce new laws and regulations for digital data protection [9]. Digital transformation of government services also positively influences the environmental footprint of government operations and contributes to the sustainability efforts of governments. Its prime advantage includes limited paper-based forms, which reduces deforestation. This results in a cleaner environment and limited carbon emission, contributing to the United Nations' Sustainable Development Goals. However, there are certain environmental challenges also associated with digital transformation which require appropriate policies and planning from the government. This includes the adoption of green practices such as renewable energy, electronic waste disposal procedures, power management policies, data center optimization, and the adoption of energy-efficient hardware.

Security and privacy in software applications are critical considerations in the digital economy, where organizations are striving to use digital infrastructure to gain a competitive advantage and deliver services efficiently [10]. Alongside these benefits, digital technologies bring cybersecurity challenges for organizations in protecting technological systems and data. An extended number of devices, distributed work environments, and cloud infrastructure result in increased attacks on technological infrastructure. Similarly, the large volume of organizational digital data poses extensive data breach threats. Human errors, lack of training, and disgruntled employees are major insider threats to organizations, and they may also become victims of ransomware, phishing, and social engineering attacks. Therefore, organizations need to ensure that their technological infrastructure is secure so that end users can trust them. Software systems should be transparent in their data use and capable of securing stored data to foster the trust of end users [11]. This includes providing clear explanations of privacy policies and security measures, as well as giving users control over their data. Furthermore, software systems need to foster secure identity management and data storage mechanisms, which may include multi-factor authentication, password policies, behavioral analysis, access control policies, and data encryption [12]. Similarly, at the organizational level, the development of security audit mechanisms, robust cyber threat intelligence, and response mechanisms can contribute to enhancing the cybersecurity agility of organizations [13]. Continuous improvement in optimizing cybersecurity controls in organizations helps ensure that security measures remain effective over time and that user participation is enhanced [14,15].

Security of digital infrastructure has become a key challenge for governments [16]. Cybersecurity is a broad area which is divided into data security, software security, component security, connection security, system security, human security, organizational security, and societal security knowledge [17]. In the user-centric design paradigm [18–20], the user is at the forefront of system design. Similarly, user-centric security focuses on users' behavior and cognitive limitations in designing security controls. As a result, the concept of usable security and privacy has emerged, which focuses on human factors' implications on the security and privacy of digital artifacts [21]. Usable security and privacy focus on a user-centered design approach to align the design of security controls with the cognitive abilities of end users and work practices [22]. As a result, the design of security controls in digital systems is not an afterthought in designing digital systems; rather, it is integrated into the design process. End user behavior and practices influence the system design choices, resulting in improving the trust of end users. Furthermore, data transparency of systems is enhanced to make the user aware of their choices in security controls and enable

them to control their privacy settings easily. Aligning the security of digital technologies with human factors enhances the user acceptance of security controls and thus results in sustainable digital transformation initiatives. Adopting and modifying security settings in technological systems is often complex. It requires extensive technical knowledge, negatively affecting users' capability to optimally use security features. Furthermore, unclear data handling policies for digital platforms also affect users' ability to protect themselves from cybersecurity attacks. A balance in security measures and usability can increase a user's adoption of digital systems. Therefore, user perception of security is highly critical and forms the backbone of the success of digital systems. Cybersecurity awareness plays a critical role in end users' resilience against cyber threats and security. If users are more aware of cybersecurity challenges, then their behavior can lead them to cautious decisions in information security, and vice versa. This paper explores citizens' perceptions of usable security and privacy in using e-government services in Saudi Arabia and presents a model for improving cybersecurity. This model will help governments foster sustainable digital transformation in e-government projects.

The rest of the paper is structured as follows. Section 2 provides a review of the related literature and is followed by empirical data in Section 3. Section 4 outlines a detailed discussion and our proposed model for improving usable security and privacy. A brief conclusion is provided in Section 5.

2. Related Work

Secure digital transformation initiatives not only contribute to improving trust but also help governments reduce operational cybersecurity costs. An IBM study [23] reported USD 3.58 million in average savings for each data breach in organizations with fully deployed security automation. Similarly, Forbes [24] projected huge savings for the US government by adopting secure digital solutions, which resulted in transparency, limited administrative costs, and minimized redundancies. Furthermore, secure digital transformation artifacts (such as chatbots and virtual assistants) can improve operational efficiency, productivity, and business continuity. Compliance with security regulations such as the GDPR [25] enhances user trust in electronic channels. Estonia is one of the models for the provision of public services via digital channels, where 99% of public services are available through electronic channels. The government in Estonia has adopted blockchain-based security to secure its digital infrastructure [26]. Despite these robust security mechanisms, an increase in cyber-attacks was reported in the 2023 annual report, resulting in billions of euros in losses [27]. Such digital initiatives modernize government service provision, but privacy protection should also be a key consideration. Dixon [28] highlighted similar concerns in the case of India's Aadhaar biometric ID program. As per the data from the national fraud initiative of the UK [29], the government has been able to save more than GBP 2 billion in the UK and GBP 49.4 million in Wales since 1996 through digital verification.

There has been a recent focus on a human-centric approach in the cybersecurity literature, which advocates considering user implications to achieve a balance in security and user privacy. Haney et al. [30] carried out an empirical study with cybersecurity practitioners and found a lack of awareness, organizational support, and resource constraints as the main obstacles. Kurdi et al. [31] highlighted that adopting secure design practices in the software development lifecycle improves software quality and security. It is highlighted that increased security awareness for software developers is required to design secure systems. Albarrak [32] highlighted that cybersecurity practices in energy management systems lack usability aspects, hindering end users' compliance. Therefore, it is necessary to adopt usability principles in cybersecurity practices to improve user compliance. Jastaniah et al. [33] developed a user-centric approach named "SAMA" by integrating homomorphic

encryption and attribute-based encryption approaches to achieve higher efficiency. In another study, Farzand et al. [34] highlighted that the interactions of end users with mobile devices may lead to security vulnerabilities, and therefore, integration of human factors in cybersecurity strategies is critical.

Zimmermann et al. [35] advocated for improving the usability of security applications and technologies to facilitate users in improving cybersecurity. Involving end users in developing cybersecurity controls and policies can result in a more resilient organization. A study by Frik et al. [36] highlighted that many mobile users are unaware of the ability to adjust a smartphone's security settings, resulting in cybersecurity risks. In another empirical study, Gull et al. [37] highlighted that end users emphasized the need for more robust security controls to enhance the trustworthiness of e-commerce portals. Similarly, Saeed [38] looked into the cybersecurity perception of Pakistani e-commerce customers and raised similar concerns. Vendors in e-commerce need to enhance the security of their IT infrastructure and enhance cybersecurity policies to build user trust. Another empirical study [39] highlighted that email and technological infrastructure management are perceived as major information security challenges by students. Another study [40] in Saudi Arabia highlighted a lack of information on security awareness among employees. Thus, there is a need to design security controls at organizational and individual levels to improve the cybersecurity of organizations. Another study [41] investigated the usability perception of security and privacy controls of mobile applications. The study highlighted that usable security and privacy are important in fostering trust in end users. Therefore, it is critical to enhance end users' cybersecurity awareness for their optimal protection in the cyber world.

Furthermore, there has been growing interest in understanding and enhancing the usable security and privacy of public services, particularly in the digital transformation of and increasing reliance on technology for service delivery. Trust in digital services is a prerequisite for fostering inclusive e-government services and strong cybersecurity awareness, and digital literacy positively contributes to trust. As in the case of Estonia, using secure e-government platforms across different government public services enhances transparency, citizen engagement, and efficiency [42]. Similar findings were also highlighted by Roots [43] based on the analysis of a government agency of Estonia named the "Estonian Road Administration (ERA)". In the design of Singapore's e-government portals, adoption of a user-centric design helped overcome challenges emanating from the multicultural context of citizens [44]. Lim et al. [45] highlighted the importance of trust and strategies from e-government authorities in Singapore by evaluating the electronic filing system. Larsen [46] compared the security challenges of data exchange in healthcare systems in Norway and Denmark and highlighted the need to foster a balance in data accessibility efficiency and security mechanisms. Kankam-Boateng et al. [47], based on their analysis of Danish small- and medium-scale enterprises, concluded that cybersecurity strategies need to be aligned with the local context for better adoption. Table 1 provides a summary of the related work.

Therefore, it is critical to enrich this body of knowledge by providing more studies in different geographical and cultural contexts to come up with challenges and best practices across different regions so that each region can benefit from each other's experiences. In this way, citizens are better served with secure e-government channels, which can especially benefit specialized user groups such as elderly, physically impaired, and low-income users, who are more vulnerable to cyber-attacks. By adopting a holistic approach which considers user perspectives, regulatory frameworks, and technological innovations, stakeholders can work toward enhancing the trustworthiness and effectiveness of public service delivery. Therefore, the presented study contributes to this discourse by investigating the

e-government service provision in Saudi Arabia, and this research specifically explored the following questions.

- What are the concerns of citizens in using e-government portals in Saudi Arabia?
- What is the trust level of citizens regarding the e-governmental portals in Saudi Arabia?
- What is the citizens' perception of usable security in e-government portals in Saudi Arabia?
- How do user intention, citizen concerns, and trust affect the citizens' perception of the usable security of e-government portals?

Table 1. Summary of related work.

Study	Core Finding
[30]	Cybersecurity specialists recognize the value of adopting a human-centered cybersecurity approach, but its application is challenging.
[31]	Proposed the need for more security awareness among software development teams for developing secure software systems in software development lifecycle.
[32]	Proposed a framework to integrate usability in security controls to improve the user experience as well as resilience against cyber threats.
[33]	Proposed a scheme, "SAMA", which applies homomorphic encryption to ensure privacy during data aggregation.
[34]	Proposed categorization-based solutions to protect users from different security attacks on their mobile phones.
[35]	Emphasized improvements in usability aspects of security controls to transform users from weakest links to active controls against cybersecurity threats.
[36]	Reported users' inability to appropriately control security settings, making them more vulnerable to security threats.
[37]	Proposed a model to improve customer security perception for improving e-commerce security in Saudi Arabia.
[38]	Based on an empirical study in Pakistan, reported how credit card usage concerns, trustworthiness, user feelings, and motivational factors and reputation of an e-commerce application affect customers' perceptions of security and trust.
[39]	Reported email management and infrastructure management as main constructs in security perception of students in Saudi Arabia.
[40]	Highlighted need for enhanced security controls and regular training of employees to better prepare themselves to respond to cybersecurity threats in an agile manner.
[41]	Highlighted how privacy and security concerns as well as trustworthiness levels of end users positively impact a user's perception of usable security and privacy perception of mobile phone applications.
[42]	Discussed establishment of an e-governance system by providing an in-depth case study of Estonia.
[43]	Based on a case study of Estonian Road Information Bureau, highlighted that successful usage of an e-government system requires awareness from the end users.
[44]	Provided detailed insights on adoption of usability in research and development projects across Singapore.
[45]	Based on the analysis of Singapore's Electronic Tax-Filing (E-Filing) system, proposed strategies for building trust of end users in e-government systems.
[46]	Compared data exchange strategies in the health sectors of Norway and Denmark and emphasized the need for collaboration among stakeholders for improvement.
[47]	Explored Danish small- and medium-scale enterprises to evaluate cybersecurity practices and enhance security deficiencies.

3. Materials and Methods

In this paper, we investigate the user perception of the security and privacy of digital services provided to citizens in Saudi Arabia. Saudi Arabia is one of the leading countries in providing digital technologies for its citizens, which makes it an interesting case. In 2024, Saudi Arabia achieved a score of 0.9602 on the United Nations e-government development index and is ranked 6th globally, whereas in the case of the e-participation index, its score is 0.9589, and it is ranked 7th globally. The e-government development index has three sub-indexes, namely online service, telecommunication infrastructure, and human capital, and Saudi Arabia scored 0.9899, 0.9841, and 0.9067 for these categories, respectively [48]. Furthermore, the selection of Saudi Arabia as a case was also influenced by its extensive geopolitical importance in the Middle East, being a key player in the global supply chain of oil and the extensive digital transformation efforts occurring across different domains in Saudi Arabia under the Vision 2030 program [49]. Being the largest economy in the Middle East, in addition to the presence of global companies such as Aramco, makes the security of digital infrastructure more critical. As a result, to attain cybersecurity resilience, the government of Saudi Arabia has established a number of institutions such as the Digital Government Authority [50], the National Cybersecurity Authority [51], and the Saudi Data and Artificial Intelligence Authority [52].

The results of this research will help with understanding the security and privacy challenges faced by citizens while interacting with digital platforms and applications for accessing public services in Saudi Arabia. As a result, this study will help improve the security policies of public services in Saudi Arabia by prioritizing the needs and preferences of citizens while ensuring compliance with legal and regulatory requirements.

In this empirical study, quantitative data were acquired using a questionnaire. The questions in the questionnaire were designed while keeping in mind the end user's security perception and usability implications for secure design. Each question was evaluated on a Likert scale with 5 levels: completely agree, mostly agree, neutral, mostly disagree, and completely disagree. For the content validity of our questionnaire, we had it reviewed by two colleagues, and after the review, the questionnaire was finalized. There was a qualification criterion for filling out the survey—users had to have used an electronic public service—and survey participation was voluntary. The questionnaire was uploaded to Google Forms on 30 April 2025, and the questionnaire remained open for 30 days. We relied on a snowball sampling approach, where we shared the survey link with contacts and obtained their help in collecting survey responses. We collected a total of 960 responses, and out of these, 99 responses were removed due to issues of incompleteness. As a result, 861 valid responses remained, reaching a margin of error of 3.27% with a confidence level of 95%.

Keeping in mind data protection and privacy, only the necessary data were stored using password protection, and they were accessible to the research team only. Participant confidentiality was maintained as the questionnaires did not require any identifiable information. Furthermore, participants were informed about the objective of the study, and informed consent was obtained from the participants before the start of the questionnaire. In order to avoid bias, the questions in the questionnaires were framed to avoid queues or influencing the responses. For the conduct of the study, institutional review board approval was acquired on 23 April 2024, having the number IRB-2024-09-311. Once the data were collected, they were decoded to be processed in SmartPLS 4 [53]. We used the PLS-SEM algorithm, and based on this, we developed a model to review the relationship between different constructs in the questionnaire.

4. Results

In the first section of the questionnaire, there were three generic questions regarding respondents' demographics. The first question was about the geographical locations of the respondents. There were 64 respondents from the northern region, 620 from the eastern region, 74 from the western region, 45 from the southern region, and 58 from the central region of Saudi Arabia. The next question was about the age distribution of the respondents, and there were 668 responses in the age group of 18–30 years, 106 responses in the age group of 31–50 years, 66 responses from 51–60 year-olds, and 21 respondents from respondents older than 60 years. The next question looked at the educational backgrounds of the respondents, where 28 respondents had basic elementary-level education, 50 respondents had intermediate-level education, 97 had secondary-level education, 479 respondents had undergraduate degrees, and 207 respondents had graduate degrees.

As shown in Table 2, there were two questions focusing on users' intention to use e-government portals. In the first question, respondents presented their opinions on whether using e-government applications helps them complete their governmental tasks efficiently. A total of 33.68% of the respondents completely agreed, and 23.58% mostly agreed that using e-government applications made their tasks efficient. On the other hand, 21.72% of the respondents remained neutral, 8.48% mostly disagreed, and another 12.54% completely disagreed. In response to the second question, 22.53% of the respondents completely agreed, and 31.82% mostly agreed that the application of security and privacy policies made learning about the usage of e-government applications easy for them, whereas 26.13% of the respondents remained neutral, 11.03% mostly disagreed, and 8.48% completely disagreed.

Table 2. Questions regarding user intention to use e-government portals.

ID	Questions	Completely Agree	Mostly Agree	Neutral	Mostly Disagree	Completely Disagree
I1	It makes it efficient to complete my governmental public service or tasks using e-government applications.	33.68%	23.58%	21.72%	8.48%	12.54%
I2	Application of privacy and security policy makes learning the usage of e-government applications easy for me.	22.53%	31.82%	26.13%	11.03%	8.48%

As shown in Table 3, this subsection of the questionnaire contained six questions focusing on users' concerns in using e-government applications. The first question enquired whether security concerns make e-government portal usage difficult. In response to this question, 8.59% of the respondents completely agreed, 18.58% mostly agreed, 29.73% remained neutral, 28.80% mostly disagreed, and 14.29% completely disagreed that due to security concerns, usage of e-government applications becomes difficult. In response to the statement that even after applying the privacy policy, it is easy to use the technology, 19.40% completely agreed, 36.82% mostly agreed, 29.15% remained neutral, 8.71% mostly disagreed, and 5.92% completely disagreed. In the next question, we enquired whether e-government applications will be more usable after applying security policies. In response to this question, 27.41% of the respondents completely agreed, 31.36% mostly agreed, 26.48% remained neutral, 8.71% mostly disagreed, and 6.04% completely disagreed. In response to the next question, 16.26% of the respondents completely agreed, 32.98% mostly agreed, 31.36% remained neutral, 12.78% mostly disagreed, and 6.62% completely disagreed that end users feel that they have sufficient control over their data while using e-government portals. In response to the next question, 7.67% of the respondents completely agreed, 20.79% mostly agreed, 27.41% remained neutral, 23.81% mostly disagreed, and 20.33%

completely disagreed that they have fears that e-government applications will expose their personal information to others without end users' authorization. For the last question, 19.98% completely agreed, 35.08% mostly agreed, 29.04% remained neutral, 10.92% mostly disagreed, and 4.99% completely disagreed with the fact that they believe e-governmental applications collect only necessary data.

Table 3. Questions regarding citizens' concerns with using e-government portals.

ID	Question	Completely Agree	Mostly Agree	Neutral	Mostly Disagree	Completely Disagree
UC1	It would be difficult for me to use e-government applications to do what I want it to do due to my privacy and security concerns.	8.59%	18.58%	29.73%	28.80%	14.29%
UC2	It would be easy for me to become skillful in the use of the technology, even after applying privacy policy.	19.40%	36.82%	29.15%	8.71%	5.92%
UC3	E-government applications will be more usable after applying privacy and security policies.	27.41%	31.36%	26.48%	8.71%	6.04%
UC4	I feel that I have sufficient control over my own data when interacting with e-government applications.	16.26%	32.98%	31.36%	12.78%	6.62%
UC5	I am concerned that e-government applications will expose my personal information to others without my authorization.	7.67%	20.79%	27.41%	23.81%	20.33%
UC6	I believe that e-government applications collect only the necessary data required for providing the service.	19.98%	35.08%	29.04%	10.92%	4.99%

As shown in Table 4, in this section focusing on trust and behavioral intention to use e-government portals, there were five questions. In the first question of this section, we enquired about the perception of end users and whether e-government applications are more vulnerable to security issues. In response to this question, 9.52% of the respondents completely agreed, 22.53% mostly agreed, 34.96% remained neutral, 18.23% mostly disagreed, and 14.75% completely disagreed. In the next question, we enquired about whether users currently intend to regularly use e-government applications, and 20.09% of the respondents completely agreed, 33.68% mostly agreed, 28.46% remained neutral, 10.34% mostly disagreed, and 7.43% completely disagreed. The third question was whether the user limited the usage of e-governmental portals due to security and privacy concerns. For this question, 7.55% of the respondents completely agreed, 18.12% mostly agreed, 29.73% remained neutral, 28.69% mostly disagreed, and 15.91% completely disagreed. The next question was about whether the end users trusted that e-government managers would think about the end users' interests while using the personal data of end users. For this question, 21.60% of the respondents completely agreed, 35.89% mostly agreed, 28.34% remained neutral, 8.25% mostly disagreed, and 5.92% completely disagreed. The last question in this section was about whether end users perceive that technology providers are honest and transparent with end users regarding user data management. For this question, 9.99% of the respondents completely agreed,23.69% mostly agreed, 36.59% remained neutral, 16.72% mostly disagreed, and 13.01% completely disagreed with it.

Table 4. Questions regarding trust in e-government portals.

ID	Questions	Completely Agree	Mostly Agree	Neutral	Mostly Disagree	Completely Disagree
T1	When you use e-government applications, do you think your data are more vulnerable to privacy and security issues?	9.52%	22.53%	34.96%	18.23%	14.75%
T2	I presently intend to use e-government applications regularly for public services.	20.09%	33.68%	28.46%	10.34%	7.43%
T3	I have limited the use the e-government applications because of my privacy and security concerns.	7.55%	18.12%	29.73%	28.69%	15.91%
T4	I trust that e-government application managers would keep my best interests in mind when dealing with my personal data.	21.60%	35.89%	28.34%	8.25%	5.92%
T5	Technological providers (such as software companies and app development companies) are always honest with users when it comes to using private data that they would provide.	9.99%	23.69%	36.59%	16.72%	13.01%

As shown in Table 5, in this subsection of the questionnaire, there were 10 questions focusing on system design and usable security and privacy implications. In the first question, we asked the respondents whether the security policies of e-government applications are visible on the websites. As shown in Table 5, 14.63% of the respondents completely agreed with this, 31.82% mostly agreed, 33.68% remained neutral, 12.20% mostly disagreed, and 7.67% completely disagreed. The next question was targeted at the easy navigation of security policies on e-government portals. For this question, 13.24% of the respondents completely agreed and 36.35% mostly agreed that the security and privacy policies of e-government applications are easily accessible. However, 33.22% remained neutral, 12.54% mostly disagreed, and 4.65% completely disagreed with it. In the next questions, we asked about the data transparency policies of e-government websites, and 15.21% of the respondents completely agreed and 34.38% mostly agreed that the intended usage of data is clearly documented on e-government websites, whereas 34.84% remained neutral, 10.45% mostly disagreed, and 5.11% completely disagreed with this. In the next question, we enquired whether e-government applications have announced a clear policy that users' data will not be accessed without the explicit consent of end users. For this question, 17.54% of the respondents completely agreed, 31.13% mostly agreed, 34.84% remained neutral, 10.69% mostly disagreed, and 5.81% completely disagreed that e-government websites have a public disclosure that end users' data will not be accessed without their consent. Updates in security and privacy policies need to be communicated to end users, and for this statement, 17.42% of the respondents completely agreed, 31.82% mostly agreed, 34.03% remained neutral, 10.80% mostly disagreed, and 5.92% completely disagreed that changes in security policies by e-government portals are communicated to end users. For the question of whether e-government portals implement appropriate alerts to warn users about potential threats, 17.42% of the respondents completely agreed, 33.91% mostly agreed, 32.98% remained neutral, 9.52% mostly disagreed, and 6.16% completely disagreed. In response to the next question, 19.05% of the respondents completely agreed, 34.73% mostly agreed, 31.24% remained neutral, 9.99% mostly disagreed, and 4.99% completely disagreed that error messages on e-government portals are meaningful. In response to the question of whether e-government portals employ multiple user authentication mechanisms, 29.97% of the respondents completely agreed, 29.85% mostly agreed, 26.95% remained neutral,

6.97% mostly disagreed, and 6.27% completely disagreed. Furthermore, in response to the question of whether security and privacy measures adopted by e-government portals create barriers for end users with disabilities, 11.85% completely agreed, 25.20% mostly agreed, 36.00% remained neutral, 19.28% mostly disagreed, and 7.67% completely disagreed. The last question was relevant to universal access to e-government portals, and 35.42% of the respondents completely agreed, 24.27% mostly agreed, 25.87% remained neutral, 8.13% mostly disagreed, and 6.39% completely disagreed that e-government services should be accessible to all end users, especially those with hearing and visual impairments.

Table 5. Questions regarding e-government portal design.

ID	Questions	Completely Agree	Mostly Agree	Neutral	Mostly Disagree	Completely Disagree
US1	Privacy and security policies on the use of e-government applications are visible on the website or app that I use for public services.	14.63%	31.82%	33.68%	12.20%	7.67%
US2	The privacy and security policies of e-government applications are accessible by easy navigation.	13.24%	36.35%	33.22%	12.54%	4.65%
US3	Intended usage of my personal data is clearly mentioned by e-government applications.	15.21%	34.38%	34.84%	10.45%	5.11%
US4	It is clearly mentioned by e-government applications that data will not be accessed without my explicit consent.	17.54%	31.13%	34.84%	10.69%	5.81%
US5	Changes in privacy and security policies are notified to users?	17.42%	31.82%	34.03%	10.80%	5.92%
US6	Security alerts are implemented in e-government applications to alert users about potential threats.	17.42%	33.91%	32.98%	9.52%	6.16%
US7	Privacy- and security-related error messages are meaningful in e-government applications.	19.05%	34.73%	31.24%	9.99%	4.99%
US8	E-government applications employ multiple methods of user authentication (such as two-factor authentication).	29.97%	29.85%	26.95%	6.97%	6.27%
US9	Security and privacy measures implemented by e-government applications create barriers for users with disabilities?	11.85%	25.20%	36.00%	19.28%	7.67%
US10	I believe that e-government services should be accessible to all citizens, including those with visual or hearing impairments	35.42%	24.27%	25.78%	8.13%	6.39%

We further investigated the relationship between user intention to use e-government services, citizens' concerns with using e-government, user trust in e-government portals, and the usability of e-government services. We developed an initial model, which is shown in Figure 1.

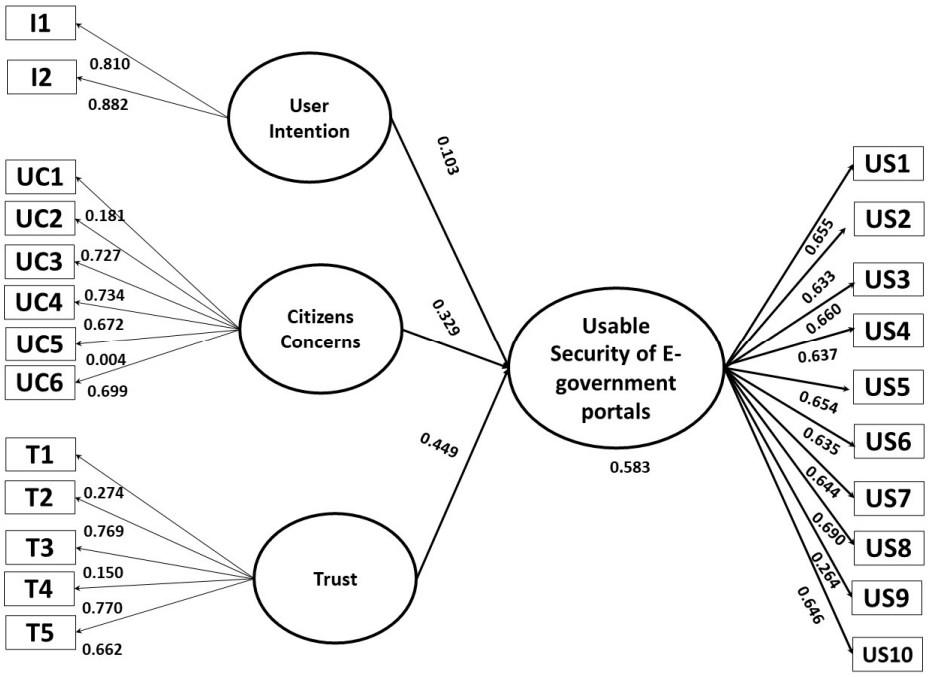


Figure 1. Initial PLS model.

As the model highlights, UC 1, UC 5, T3, y8, and US9 had less than the acceptable value of 0.6, which means that they were insignificant in the model outcome. Therefore, we reconstructed the model by removing the insignificant factors, as shown in Figure 2.

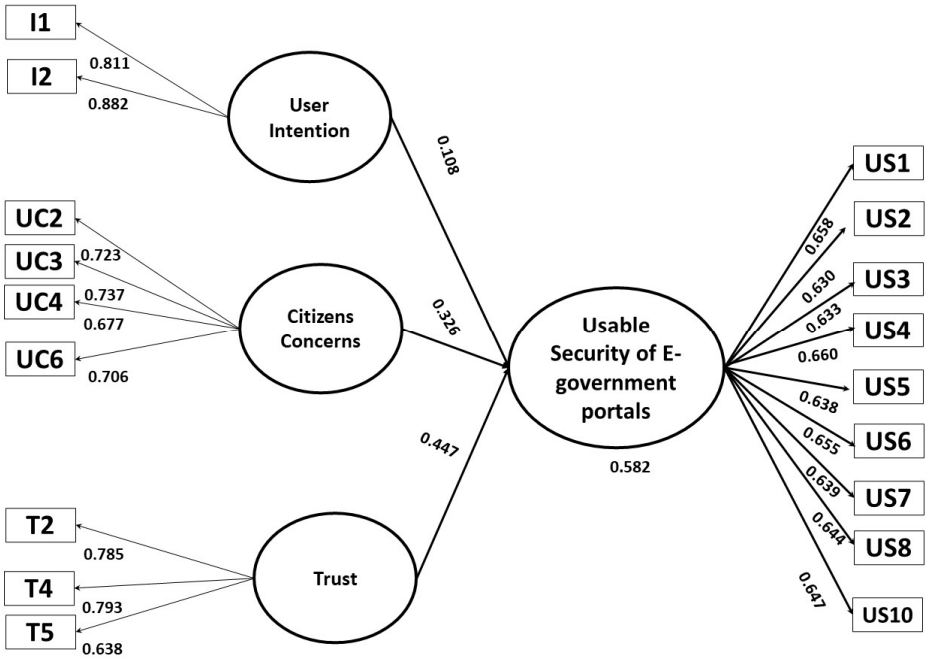


Figure 2. Modified PLS model.

As shown in Table 6, the R-squared value was more than 0.5, which highlights that the model is acceptable [54]. Furthermore, the average variance extracted for all constructs was more than 0.5, which highlights an acceptable level of convergent validity. Composite reliability (rho_a) values between 0.6 and 0.7 are considered acceptable [55]. As shown in Table 6, our values fell in that range, highlighting the reliability of the data. Similarly, the composite reliability (rho_c) values for all constructs were greater than 0.7, which indicates good reliability [56].

Table 6. Reliability values of the model.

Construct	R-Squared	Composite Reliability (rho_a)	Average Variance Extracted	Composite Reliability (rho_c)
User intention to use e-government services	-	0.628	0.717	0.835
Citizens' concerns with using e-government	-	0.674	0.506	0.803
Trust in e-government portals	-	0.612	0.551	0.785
Usable design of e-government services	0.582	0.832	0.426	0.869

5. Discussion

Upon closely analyzing the results, it can be seen that user intention, citizens' concerns, and trust are key factors in citizens' perceptions of the usable security of e-government portals. Therefore, it is critical to improve users' intentions and trust and minimize citizens' concerns to improve user perceptions. Therefore, it is recommended that e-government applications in Saudi Arabia need to make more efforts to make security and privacy policies more visible and accessible. Based on this, we present a model which can help in improving the usable security of e-government applications. As shown in Figure 3, our model has three main stakeholders, which are citizens, government service provider organizations, and government cybersecurity regulators. The model advocates for strong collaborative efforts among citizens, governmental service provision organizations, and governmental cybersecurity regulators to foster usable digital transformation in governmental public service provision. Citizens need to take care of cyber hygiene; governmental service providers need to adopt a security-by-design approach and ensure a usable platform; and a government's cybersecurity department needs to ensure appropriate laws are implemented.

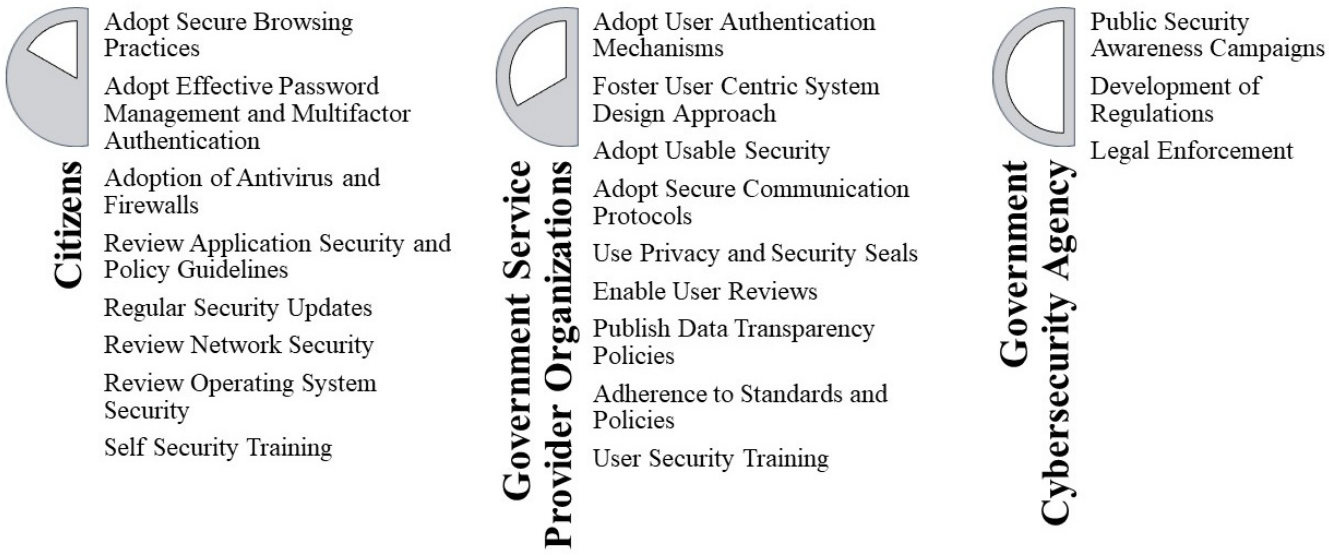


Figure 3. Usable cybersecurity enhancement model.

From the citizens' point of view, they must adopt secure browsing practices while using the internet. This includes using secure websites with secure hypertext transfer protocol (https) instead of conventional hypertext transfer protocol, as the encryption used in https ensures that data transfer is secure. It is also important that operating systems and internet browsers are regularly updated and that built-in security features of browsers

such as popup blockers and tracking protections are used. Caution should be used when opening suspicious links, downloading files from untrusted sources, and disabling scripts. Public Wi-Fi connections should be avoided, and browser cookies should be deleted. Third-party cookies should be blocked in internet settings. Internet extensions should be reviewed regularly, and unwanted extensions may be uninstalled. The autofill features of the browser may not be used. To protect personal data, passwords must be effectively managed by users. Users need to keep strong passwords, which should be a combination of letters, numbers, and special characters so that they cannot be used by anyone else. Passwords need to be unique across platforms, and they should not be reused or contain personal information. Rather than saving passwords with computer files, paper notes, or auto-fill in browsers, a well-known password manager application may be used. The passwords should be regularly changed, and password hint options may not be exercised. Additionally, multi-factor authentication mechanisms should be used. Account activity needs to be periodically monitored, and in case of any suspicious activity, passwords should be changed immediately.

Furthermore, the adoption of firewalls on the network and antivirus software on personal devices can reduce the risk of cyber-attacks. Firewalls can detect incoming data to filter unauthorized access based on deployed policies and detect unusual traffic patterns to protect against phishing and distributed denial of service attacks. On the other hand, the use of antivirus software on personal devices helps detect and remove malware from the internet and other external devices. Security policies and guidelines of applications should be regularly reviewed to protect personal devices and information from misuse. In this way, users can see the data management practices of applications and customize permission settings based on their preferences, which will help with protecting personal information. Furthermore, based on these regular reviews, users remain aware of new threats and recommendations to improve personal security. As bugs and vulnerabilities are continuously updated, it is critical that operating systems and other applications be continuously updated to enhance cybersecurity resilience. Such a proactive approach not only protects a personal device but also a network, as threats are identified at the first instance rather than proliferating to the entire network. Another important activity end users need to carry out is to conduct periodic security reviews of the network. Users need to update the default name and user of the network to a secure account which does not reveal any personal information. The Wi-Fi password should be strong. All devices, including smart TVs and cameras on the network, should have updated operating systems. The network should be scanned, and logs should be reviewed to identify any unauthorized device on the network. A guest account may be enabled rather than sharing the main account credentials with any visitors. Firewalls and antivirus applications are recommended to secure the network. Operating system security must also be periodically reviewed by end users. The operating system should be set to automatic update mode to avoid missing any critical updates. In case the devices are shared among different users, the account type should be reviewed to verify the permissions. The backup and recovery settings need to be reviewed, and services which are not required may be disabled from operating system settings. To improve cybersecurity resilience, users need to educate themselves. Users may access free documentation and videos about cybersecurity basics to enhance their awareness of cybersecurity threats and self-protection. Users may access online tools to practice simulated cybersecurity scenarios and participate in online forums to be aware of recent news.

Government service provider organizations have the responsibility to enhance end users' cybersecurity resilience. Organizations need to ensure that their online platforms possess user authentication mechanisms to increase user trust. Designing technological

systems which foster a user-centric approach will help with understanding end user needs and aligning system features with them. Such an approach will ensure that user needs are appropriately integrated into a system's design, thus enhancing the user's trust and involvement in such a system. Furthermore, fostering usable security and privacy in technological systems will ensure that cybersecurity controls are usable and guide users in secure usage. It is also the responsibility of organizations to adopt secure communication in their IT artifacts by adopting secure technologies, policies, and a robust monitoring framework. The adoption of secure communication channels will ensure that data exchange within the company's technological network is secure. This includes secure communication protocols such as https, adopting encryption algorithms, key management, and security certificates. The presence of security and privacy seals on organizational web pages increases trust in users, and users feel secure while browsing these organizational websites. Such certification seals provide confidence to end users that these websites meet security criteria. Additionally, the provision of user reviews on organizational websites also builds trust for the end user that organizations are transparent and users can publish their positive or negative experiences openly to guide other prospective users. Concerns about data usage policies are a major factor in building the trust of end users. Organizations should ensure that their user data management policies are transparent, and these should be publicly available on their websites to make users aware. The adoption of well-known cybersecurity standards and policies ensures that organizations not only aim to protect their IT infrastructure but also educate stakeholders about potential security threats and adopt best practices. Standards and policies like ISO 27001 [57], ISO/IEC 27005 [58], NIST cybersecurity framework [59], HIPAA [60], and GDPR [25] provide clear security expectations adopted by organizational IT infrastructure, resulting in a secure organizational culture. Compliance and audit mechanisms ensure that organizations are adopting appropriate security controls. Organizations should also use gamification and quizzes to train end users about cybersecurity awareness to promote a secure culture.

Government cybersecurity agencies are the third major actor in our model; they should raise the cybersecurity awareness of the masses. This includes large-scale awareness campaigns using traditional advertising media and online channels and providing educational content. Such campaigns can promote secure behavior among the public. The government may partner with the private sector to run such campaigns. Additionally, any new cyber threat information may be shared with the public for their awareness. Schools and universities may be engaged, and specialized events may be organized to improve community cybersecurity readiness. Government campaigns can benefit from gamification to enhance user participation in cybersecurity training. Another important task of the government is to develop laws to protect user security and privacy. Having a robust legal environment increases users' trust in digital channels. Governments also need to implement these laws as well to ensure that online crimes can be reduced.

6. Conclusions

Digital transformation in the governmental sector has enabled service excellence for citizens around the world. However, security and privacy concerns hurt the acceptability of e-government services for end users. The usable security and privacy paradigm advocates for adopting a user-centric design in designing security controls to minimize their complexity without compromising security. To improve security, end users need to be aware of the sensitivity of information shared with technological systems and the associated threats. In this paper, we explored the usable security and privacy perception of end users in Saudi Arabia and described a model which can help in improving cybersecurity and thus contribute to fostering a cybersecurity-resilient digital transformation initiative. The

findings are relevant to system designers and policymakers for facilitating end users and fostering enhanced adoption.

This study has certain limitations which need to be taken into account while generalizing the results. Firstly, the adopted sampling approach of random sampling did not result in equal participation of the entire population. Furthermore, in our study, respondents were not balanced based on demographic characteristics such as geographical region, age group, and educational level. Secondly, the sample size was small compared with the actual population of government service users in the country. Therefore, in the future, we would like to follow up with detailed quantitative and qualitative studies to understand the insights of respondents. Quantitative studies with large sample sizes selected using stratified sampling, based on attributers such as gender, educational background, and geographical region to have a representative sample, will help in evaluating the validity of the findings. On the other hand, qualitative studies will help understand the deep insights and reasons of users. Furthermore, our proposed model needs to be evaluated in longitudinal empirical studies to measure its effectiveness in shaping end users' cybersecurity behavior. Once sufficient case studies are documented, the model may be refined based on the results of the case studies in diverse geographical, cultural, and user communities.

Funding: This research received no external funding.

Institutional Review Board Statement: An institutional review was conducted and approved by the Ethics Committee of Imam Abdulrahman Bin Faisal University on 23 April 2024 (IRB-2024-09-311).

Informed Consent Statement: Informed consent for participation in the questionnaire was obtained from all subjects.

Data Availability Statement: The data of this study were not made public due to privacy issues. However, they can be acquired on request from the corresponding author.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Alshammari, W.S.; Ajoud, M.E.K.; Ibrahim, A.I.H.; Al Shamlan, A.E.; Alsalman, A.I. Impact of E-government on Institutional Performance: Fostering Sustainable Higher Educational Practices. *Eur. J. Sustain. Dev.* **2025**, *14*, 169. [CrossRef]
2. Ghobakhloo, M.; Iranmanesh, M.; Foroughi, B.; Tseng, M.L.; Nikbin, D.; Khanfar, A.A. Industry 4.0 digital transformation and opportunities for supply chain resilience: A comprehensive review and a strategic roadmap. *Prod. Plan. Control.* **2025**, *36*, 61–91. [CrossRef]
3. Vrana, J.; Singh, R.R. Digitization, digitalization, digital transformation, and beyond. In *Handbook of Nondestructive Evaluation 4.0*; Springer Nature: Cham, Switzerland, 2025; pp. 1–26.
4. Onesi-Ozigagun, O.; Ololade, Y.J.; Eyo-Udo, N.L.; Ogundipe, D.O. Leading digital transformation in non-digital sectors: A strategic review. *Int. J. Manag. Entrep. Res.* **2024**, *6*, 1157–1175. [CrossRef]
5. Malik, M.; Andargoli, A.; Clavijo, R.C.; Mikalef, P. A relational view of how social capital contributes to effective digital transformation outcomes. *J. Strateg. Inf. Syst.* **2024**, *33*, 101837. [CrossRef]
6. Iuliano, G.; Cuadrado-Ballesteros, B.; Bisogno, M. Citizens'e-participation in the digital world: Empirical insights from Europe. *Public Money Manag.* **2025**, *45*, 12–21. [CrossRef]
7. Hossen, M.D.; Abedin, M.Z.; Chowdhury, T.M.; Islam, Z.; Kabir, M.R. Unveiling the Impact of E-Governance on the Transformation from Digital to Smart Bangladesh. *Pak. J. Life Soc. Sci.* **2025**, *23*, 85–108. [CrossRef]
8. Chan, F.K.; Thong, J.Y.; Brown, S.A.; Venkatesh, V. Design characteristics and service experience with e-government services: A public value perspective. *Int. J. Inf. Manag.* **2025**, *80*, 102834. [CrossRef]
9. Jejeniwa, T.O.; Mhlongo, N.Z.; Jejeniwa, T.O. Conceptualizing e-government initiatives: Lessons learned from Africa-US collaborations in digital governance. *Int. J. Appl. Res. Soc. Sci.* **2024**, *6*, 759–769. [CrossRef]
10. Saeed, S.; Gull, H.; Aldossary, M.M.; Altamimi, A.F.; Alshahrani, M.S.; Saqib, M.; Zafar Iqbal, S.; Almuhaideb, A.M. Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications. *Information* **2024**, *15*, 764. [CrossRef]
11. Damaraju, A. Cloud Security Challenges and Solutions in the Era of Digital Transformation. *Int. J. Adv. Eng. Technol. Innov.* **2024**, *1*, 387–413.

12. Azizi, M.; Hakimi, M.; Amiri, F.; Shahidzay, A.K. The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges. *Open Access Indones. J. Soc. Sci.* **2024**, *7*, 1473–1482.
13. van der Kleij, R.; Van Hemert, D.; Te Paske, B.J.; Rooijakkers, T. Human-Centric Security Engineering: Towards a Research Agenda. *Hum. Factors Des. Eng. Comput.* **2024**, *159*, 8–10.
14. de Nobrega, K.M.; Rutkowski, A.F.; Saunders, C. The whole of cyber defense: Syncing practice and theory. *J. Strateg. Inf. Syst.* **2024**, *33*, 101861. [CrossRef]
15. Ghahramani, F.; Yazdanmehr, A.; Chen, D.; Wang, J. Continuous improvement of information security management: An organisational learning perspective. *Eur. J. Inf. Syst.* **2023**, *32*, 1011–1032. [CrossRef]
16. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors* **2023**, *23*, 6666. [CrossRef]
17. Shoemaker, D.; Kohnke, A.; Sigler, K. *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity*; CRC Press: Boca Raton, FL, USA, 2020.
18. Kling, R. The organizational context of user-centered software designs. *MIS Q.* **1977**, *1*, 41–52. [CrossRef]
19. Norman, D. Cognitive engineering. In *User Centered System Design*; Lawrence Erlbaum Associates, Inc.: Mahwah, NJ, USA, 1986.
20. Wulf, V.; Müller, C.; Pipek, V.; Randall, D.; Rohde, M.; Stevens, G. Practice-based computing: Empirically grounded conceptualizations derived from design case studies. In *Designing Socially Embedded Technologies in the Real-World*; Springer: London, UK, 2015; pp. 111–150.
21. Acar, Y.; Fahl, S.; Mazurek, M.L. You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In Proceedings of the 2016 IEEE Cybersecurity Development (SecDev), Boston, MA, USA, 3–4 November 2016; pp. 3–8.
22. Fischer-Hübner, S.; Karegar, F. Overview of Usable Privacy Research: Major Themes and Research Directions. In *The Curious Case of Usable Privacy: Challenges, Solutions, and Prospects*; Springer: Cham, Switzerland, 2024; pp. 43–102.
23. IBM Cost of a Data Breach Report. 2020. Available online: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf (accessed on 6 February 2025).
24. Forbes. Available online: https://www.forbes.com/sites/joemckendrick/2013/11/20/cloud-computing-may-save-u-s-federal-government-20-billion-a-year-but-theres-more-to-it-than-just-cost-savings/ (accessed on 6 February 2025).
25. Goldberg, S.G.; Johnson, G.A.; Shriver, S.K. Regulating privacy online: An economic evaluation of the GDPR. *Am. Econ. J. Econ. Policy* **2024**, *16*, 325–358. [CrossRef]
26. Estonia. Available online: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf (accessed on 6 February 2025).
27. Cybersecurity in Estonia. 2024. Available online: https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf (accessed on 6 February 2025).
28. Dixon, P. A Failure to "Do No Harm"—India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US. *Health Technol.* **2017**, *7*, 539–567. [CrossRef]
29. National Fraud Initiative. Available online: https://www.audit.wales/sites/default/files/2022-07/nfi_work_programme_final_eng.pdf (accessed on 6 February 2025).
30. Haney, J.; Cunningham, C.; Furman, S.M. Towards Integrating Human-Centered Cybersecurity Research into Practice: A Practitioner Survey. In Proceedings of the Symposium on Usable Security and Privacy (USEC), San Diego, CA, USA, 26 February 2024.
31. Kurdi, M.H.; Denden, M.; Paul, D. A Study on the Challenges of Human-Centric Cyber-Security and the Guarantee of Information Quality. *J. Inf. Secur.* **2024**, *15*, 218–231. [CrossRef]
32. Albarrak, A.M. Integration of Cybersecurity, Usability, and Human-Computer Interaction for Securing Energy Management Systems. *Sustainability* **2024**, *16*, 8144. [CrossRef]
33. Jastaniah, K.; Zhang, N.; Mustafa, M.A. Efficient user-centric privacy-friendly and flexible wearable data aggregation and sharing. *IEEE Trans. Cloud Comput.* **2024**, *12*, 967–982. [CrossRef]
34. Farzand, H.; Abraham, M.; Brewster, S.; Khamis, M.; Marky, K. A Systematic Deconstruction of Human-Centric Privacy & Security Threats on Mobile Phones. *Int. J. Hum. Comput. Interact.* **2024**, *41*, 1628–1651.
35. Zimmermann, V.; Schöni, L.; Schaltegger, T.; Ambuehl, B.; Knieps, M.; Ebert, N. Human-Centered Cybersecurity Revisited: From Enemies to Partners. *Commun. ACM* **2024**, *67*, 72–81. [CrossRef]
36. Frik, A.; Kim, J.; Sanchez, J.R.; Ma, J. Users' expectations about and use of smartphone privacy and security settings. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, New Orleans, LA, USA, 29 April–5 May 2022; pp. 1–24.
37. Gull, H.; Saeed, S.; Iqbal, S.Z.; Bamarouf, Y.A.; Alqahtani, M.A.; Alabbad, D.A.; Saqib, M.; Al Qahtani, S.H.; Alamer, A. An empirical study of mobile commerce and customers security perception in Saudi Arabia. *Electronics* **2022**, *11*, 293. [CrossRef]
38. Saeed, S. A customer-centric view of E-commerce security and privacy. *Appl. Sci.* **2023**, *13*, 1020. [CrossRef]

39. Saeed, S. Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. *Sustainability* **2023**, *15*, 9426. [CrossRef]
40. Saeed, S. Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. *Sustainability* **2023**, *15*, 6019. [CrossRef]
41. Saeed, S. Usable Privacy and Security in Mobile Applications: Perception of Mobile End Users in Saudi Arabia. *Big Data Cogn. Comput.* **2024**, *8*, 162. [CrossRef]
42. Metcalf, K.N. How to build e-governance in a digital society: The case of Estonia. *Rev. Catalana Dret Pub.* **2019**, *58*, 1.
43. Roots, L. E-governance in providing public services in Estonia: A case study. *Zesz. Nauk. Politech. Poznańskiej. Organ. i Zarządzanie* **2017**, *74*, 77–93. [CrossRef]
44. Lim, K.Y. Usability in Singapore. In *Global Usability*; Springer: London, UK, 2011; pp. 285–307.
45. Lim, E.T.; Tan, C.W.; Cyr, D.; Pan, S.L.; Xiao, B. Advancing public trust relationships in electronic government: The Singapore e-filing journey. *Inf. Syst. Res.* **2012**, *23*, 1110–1130. [CrossRef]
46. Larsen, H.C. Secure Data Exchange in Healthcare Infrastructure-A Case Study of Norway and Denmark. Master's Thesis, University of Agder, Kristiansand, Norway, 2024.
47. Kankam-Boateng, J.; Peressotti, M.; Mayer, P. Mapping Cybersecurity Practices and Mental Models in Danish Small and Medium Enterprises (SMEs): A Comprehensive Study using Focus Groups. In Proceedings of the 20th Symposium on Usable Privacy and Security, SOUPS 2024, Philadelphia, PA, USA, 11–13 August 2024.
48. e-gov Index. Available online: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/149-Saudi-Arabia (accessed on 6 February 2025).
49. Vision 2030. Available online: https://www.vision2030.gov.sa/en (accessed on 6 February 2025).
50. Digital Government Authority. Available online: https://dga.gov.sa/en (accessed on 6 February 2025).
51. National Cybersecurity Authority. Available online: https://nca.gov.sa/en/ (accessed on 6 February 2025).
52. SDAIA. Available online: https://sdaia.gov.sa/en/default.aspx (accessed on 6 February 2025).
53. Smart PLS 4. Available online: https://www.smartpls.com/ (accessed on 6 February 2025).
54. Ozili, P.K. The acceptable R-square in empirical modelling for social science research. In *Social Research Methodology and Publishing Results: A Guide to Non-Native English Speakers*; IGI Global: Hershey, PA, USA, 2023; pp. 134–143.
55. Cheung, G.W.; Cooper-Thomas, H.D.; Lau, R.S.; Wang, L.C. Reporting reliability, convergent and discriminant validity with structural equation modeling: A review and best-practice recommendations. *Asia Pac. J. Manag.* **2024**, *41*, 745–783. [CrossRef]
56. Hair, J.F., Jr.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M.; Danks, N.P.; Ray, S. *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*; Springer Nature: Cham, Switzerland, 2021; p. 197.
57. Calder, A.; Watkins, S. *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002*; Kogan Page Ltd.: New York, NY, USA, 2008.
58. Agrawal, V. Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard. In Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance, Frankfurt, Germany, 19–21 July 2016; pp. 101–111.
59. Shen, L. The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer* **2014**, *10*, 16.
60. Sadri, M. HIPAA: A Demand to Modernize Health Legislation. *Undergrad. Law Rev. UC San Diego* **2024**, *2*, 24–48. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.