# Identifying Cybersecurity and Information Privacy Challenges During Digital Transformation in Industry (Study: Ministry of Communications and Information Technology)

**K. A. Al-Masouri** [1,*]

Received: 23/05/2025
Revised: 04/08/2025
Accepted: 05/08/2025



[1] Department of Computer Science, College of Computer and Information Sciences, National Institute of Administrative Sciences, Sana'a, Yemen.
*Corresponding Author's Email: Khalidahmed2009@gmail.com

# Identifying Cybersecurity and Information Privacy Challenges During Digital Transformation in Industry (Study: Ministry of Communications and Information Technology)

Khaled Ahmed Al-Masouri
*Department of Computer Science, College of Computer and Information Sciences, National Institute of Administrative Sciences,*
Sana'a, Yemen.
Khalidahmed2009@gmail.com

***Abstract***— The world's increasing focus on new technologies and the emergence of smart cities, despite their potential capabilities and benefits, has raised serious concerns about cybersecurity threats and citizen privacy challenges. Sana'a is no exception to this rule in its smart city transformation process. This research paper, through a descriptive survey, aims to provide a framework for managing cybersecurity and privacy challenges in Sana'a's transition to a smart city. In this research, these challenges were identified through in-depth desk studies and the application of the Fuzzy Delphi method among a sample of experts (including ten senior managers and relevant officials from the Ministry of Communications and Information Technology, the Digital Transformation Department, and the Digital Library in Sana'a). Furthermore, the importance (weight) of each challenge was determined using the Fuzzy Best-Worst Method (FBWM). The results of this study indicated the high ability of the proposed framework to accurately identify and weighthese challenges. The research results indicated the high ability of the proposed framework to accurately identify and assess these challenges, as well as identify the three "challenges—"legislative challenge," "lack of secure communications," and "insecure APIs and protocols"—as "the most significant cybersecurity and privacy challenges in the development of a smart city in the capital, Sana'a. Preventive and corrective measures were presented for each challenge accordingly.

**Keywords—**smart city, cybersecurity, privacy, Fuzzy Delphi method, best approach, worst case.

## I. Introduction

With the global movement toward urbanization and the widespread use of information technology, the concept of smart cities has emerged and has received significant attention from researchers in recent years. The primary goal of smart cities is to improve people's lifestyles, encourage development without compromising the resources of future generations (with a focus on sustainable development), and achieve progress in urban functions. Despite the benefits, smart cities pose hidden risks, including information leaks, cybersecurity threats, privacy challenges, and malicious cyberattacks (Manchanda et al., 2020). Given the uncertainty of the real world and the importance of detecting cyberattacks, the cybersecurity of future smart cities and their smart networks is critical. The current evolution of cybersecurity has not kept pace with the enthusiastic adoption of smart city technologies, so appropriate design based on deep learning methods is essential to protect smart cities from cyber risks (Faotu et al., 2024). In addition to cybersecurity, there are specific privacy issues, particularly those related to direct objectivity, which can be classified into three categories: communication, individual, and business. Phishing, fraud, data breaches, eavesdropping, attacks on networks and websites, and so on, are examples of privacy-related challenges and violations (Aljrad, M.J.H. & Al-Dhlan, 2023).

Sana'a is no exception to these trends in its journey toward becoming a smart city. Providing protection in a smart city involves identifying and assessing threats and challenges and implementing appropriate measures and solutions to address priority challenges. In light of the impact of cybersecurity threats and privacy challenges on reducing the efficiency of smart city development in Sana'a, this study seeks to provide a systematic framework for identifying and analyzing cybersecurity threats and privacy challenges in Sana'a's transition to a smart city. The rest of this article is organized as follows. The next section reviews the research background and defines the initial theoretical framework for the challenges. The research methodology and proposed methodological framework are then presented. The proposed framework for identifying and assessing cybersecurity threats and privacy challenges in the smart city of Sana'a is implemented below. The final section of the article is also dedicated to discussion and conclusions.

## II. Review of Research Background and Theoretical Framework

Given the emerging nature of the current study area, and despite the unique capabilities and functions of smart cities, the number of local and international studies specifically examining the successful implementation of smart cities and the challenges they face is limited. We will present the most important of these studies below.

Alromaihi et al. (2018) analyzed the issue of security and privacy in smart city healthcare applications. In this regard, they reviewed various Internet of Things (IoT) applications and their cyber vulnerabilities and provided a comprehensive assessment of methods for combating cyber attacks. They then presented techniques for countering cyber attacks on smart city healthcare IoT devices and explained the different types of attacks and their associated security needs.

In their research, Berkel et al. (2017) combined threat analysis and enterprise architecture modeling to examine and mitigate these challenges from a holistic perspective. They presented an information security architecture that can help

stakeholders in smart city projects build safer smart cities. Gunduz & Das (2020) analyzed the threats and possible solutions to IoT-based smart grids. They focused on the types of cyberattacks, examined the cybersecurity status of smart grids in depth, and discussed and examined network vulnerabilities, countermeasures, and security requirements. Zhao et al. (2021) presented a systematic review of research published in the field of smart cities between 2011 and 2019. The aim of their study was to create a comprehensive picture of research progress in the field of smart cities, as well as to identify important issues and identify research gaps.

By examining previous domestic research, we note that the limited number of studies conducted in this field have focused more on basic concepts and compiling material in the form of review papers. Among foreign research, some studies focused on introducing new material in this field, as well as examining the shortcomings of smart city implementation in developed countries in the form of case studies and presenting lessons learned, while other studies have only advanced to the stage of identifying smart city security challenges. Without a thorough evaluation and analysis, these studies have simply offered fragmented solutions to address these challenges. To complement previous research and fill research gaps, this study aims to comprehensively examine the research and achievements of researchers in the field of cybersecurity and privacy in smart cities. This is achieved through an analytical study, identifying and converging expert opinions on the cybersecurity threats and privacy challenges facing Sana'a during the transition to a smart city, and determining the degree of importance of these challenges. Through a review of relevant research, a list of cybersecurity threats and privacy challenges in smart cities was compiled. The list, drawn from a set of previous research findings and based on their frequency in articles, is presented in Table 1.

Table 1. A preliminary theoretical framework for cybersecurity threats and privacy challenges in smart cities.

| References | Challenges | Factors |
|---|---|---|
| **Khatoun & Zeadally, 2017; Aldairi, 2017; Alromaihi et al., 2018; Berkel et al., 2018; Braun et al., 2018; Baig et al., 2017; Thing, 2024; Arabo, 2022; Pelton & Singh, 2019;** | 1. Increased volume of digital transactions<br>2. Increase in mobile applications and communications<br>3.Increased use of artificial intelligence in digital networks and machine-to-machine communications<br>4. Vulnerable software and hardware products<br>5. Cyberwarfare and terrorism<br>6. Cyber espionage<br>7. Data manipulation and phishing attacks<br>8. Data loss<br>9. Virus and malware penetration of smart city systems<br>10. Legislative challenges<br>11. Theft of data, information, and physical devices<br>12. Hardware and software inefficiencies<br>13. Challenges in accessing data<br>14. Insecure APIs and protocols<br>15. Denial of service (DoS)<br>16. Sensor failure<br>17. Lack of secure communications<br>18. Challenges in data management and storage<br>19. Disruption of critical infrastructure<br>20. Cloud security<br>21. Threats to artificial intelligence | Cybersecurity Challenges |
| **Aldairi, 2017; Braun et al., 2018; Baig et al., 2017; Thing, 2024;** | 1. Privacy Threats in Data Extraction and Sharing<br>2 .Privacy Threats in Mash-Up Data<br>3 .Eavesdropping<br>4. Data Access Challenge<br>5. Risk to Confidentiality and Integrity<br>6 .Risk of Fraud and Data Leakage<br>7 .Identity Forgery<br>8. Fake Information<br>9. Side Channel Attacks<br>10. Secondary Use of Collected Data<br>11. IP Address Forgery<br>12. Attacks on Data Integrity | Privacy challenges |

## III. Research Methodology and Proposed Methodological Framework

The current study is classified as applied research in terms of its objective. It is descriptive survey research based on a data collection method. The statistical population for this study includes senior managers and relevant officials in the Ministry of Communications and Information Technology, the Digital Transformation Department, and the Digital Library in the Sana'a Municipality. Since decision-making regarding the assessment of the smart city and its security challenges resides at the strategic level of these institutions, and the data required for this research is expected to be available to a small number of organizational managers and experts, ten organizational experts were selected using a purposive sampling method. The demographic information of the expert group in this study is presented in Table .2

Table 2. Demographic Information of the Expert Panel Members

| Date | Work area | Education Level | Experts |
|---|---|---|---|
| **9years** | Ministry of Communications and Information Technology | PhD | 1 |
| **15years** | | Master's Degree | 2 |
| **8years** | | Bachelor's Degree | 3 |
| **10years** | | Master's Degree | 4 |
| **7years** | | PhD | 5 |
| **3years** | Digital Transformation Department | PhD | 6 |
| **6years** | | Master's Degree | 7 |
| **16years** | | Bachelor's Degree | 8 |
| **8years** | Digital Library and Information Exchange | Master's Degree | 9 |
| **5years** | | PhD | 10 |

In this study, a two-part questionnaire was designed by the researcher to collect data. Content validity was used to determine the validity of the questionnaires. The questionnaires were presented to a number of university professors and organizational experts, and the questionnaire components and structure were approved. To measure the reliability of the first questionnaire, the expert opinion convergence threshold (α) was used, which represents the difference in expert consensus over two consecutive iterations of the fuzzy Delphi method. According to the agreement in this study, the minimum expert opinion convergence threshold value is as follows: 0/1= α. The second questionnaire was used to collect the data needed to determine the weights of cybersecurity threats and privacy challenges using the fuzzy best-worst multi-criteria (F-BWM) method. The consistency ratio method was used to measure reliability (Guo & Zhao, 2017). Figure 1 schematically illustrates the structure and steps of the proposed methodological framework.

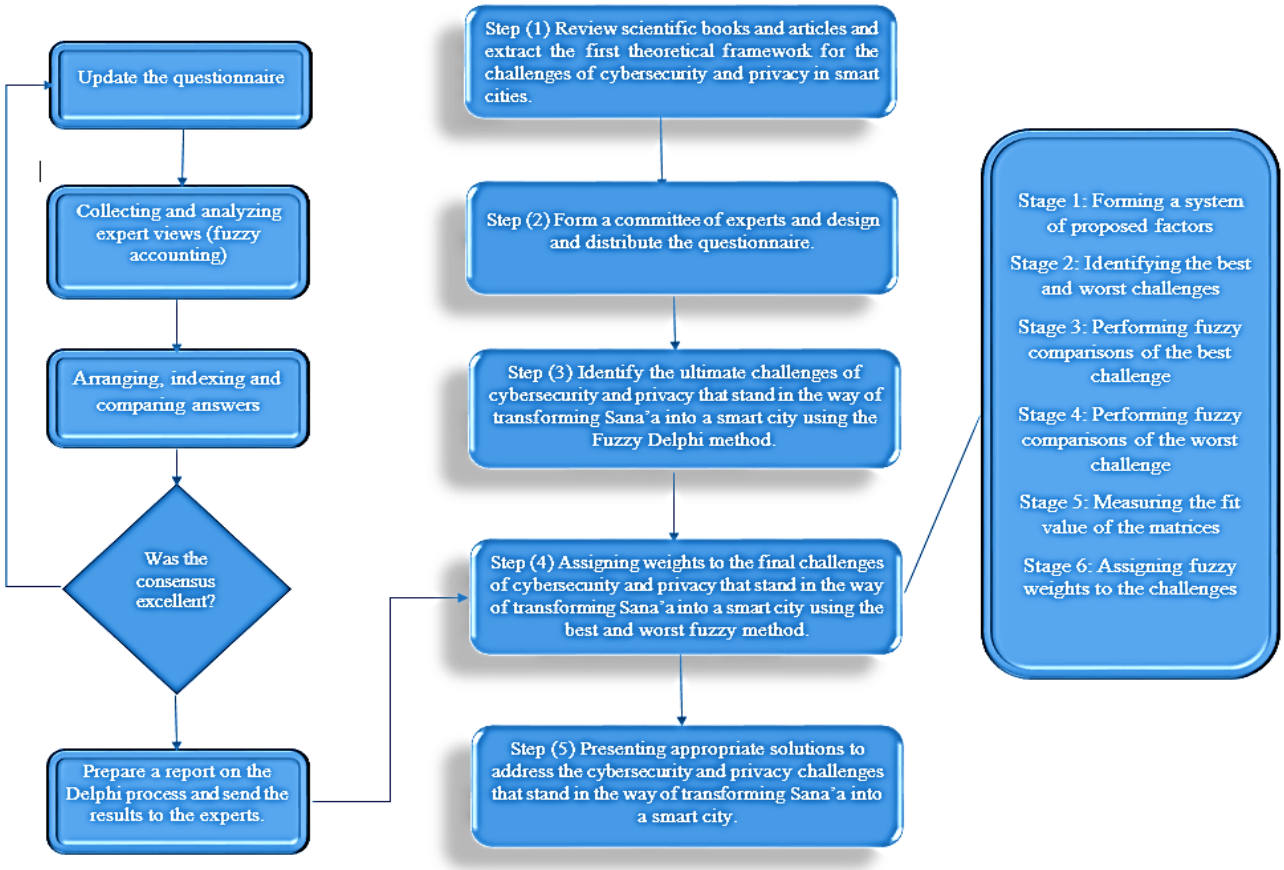


Figure 1. Proposed Methodological Framework

Considering the general research framework, this study utilizes the Fuzzy Delphi method and the Fuzzy Best-Worst method to analyze the data. Excel software was used to define and weigh the cybersecurity and privacy challenges in the Sana'a Smart City, respectively. In the current study, the proposed methods are implemented in an ambiguous environment, using group decision-making. The group decision-making strategy will prevent bias in the results and, by adhering to collective wisdom, will increase decision-making accuracy.

Applying the above methods in an ambiguous environment makes it possible to reduce uncertainty in subjective expert judgments and increase decision-making accuracy by using three-point estimates and considering the likelihood functions of their opinions.

The best-worst method was first introduced by Rezaei (2022). In this method, the best and worst are indexed by the decision maker, and a pair of factors can be compared. Guo & Zhao (2017) presented the fuzzy best-worst method in an article. The fuzzy best-worst method has the salient feature of obtaining weights from indicators with fuzzy numbers rather than specific numbers. Based on the method proposed by the researchers, the algorithm for solving the indicator weighting problem includes five main steps: 1) Forming a system of decision-making indicators, 2) Identifying the best (most important) and worst (least important) indicators, 3) Performing fuzzy preferential comparisons for the best indicator, 4) Performing fuzzy preferential comparisons for the worst indicator, 5) Measuring the fit rate of the matrices, and Determining the optimal fuzzy weights for the indicators (Guo & Zhao, 2017).

## IV. Data Analysis

By conducting desk studies and surveying the cybersecurity and privacy challenges in Table1, the Fuzzy Delphi method was adopted to adapt and localize the initial theoretical framework to the prevailing social, economic, cultural, political, legal, and technological infrastructure environment in Sana'a. The Fuzzy Delphi method, a combination of the Delphi method and fuzzy logic, was first introduced by Kaufman and Gupta in the 1980s. Experts used fuzzy numbers to make three-point estimates of phenomena (Chen, 2022). In this method, membership functions are used to represent expert opinions. This avoids the need for experts to constantly revise their opinions. Furthermore, since all opinions are described in terms of membership degrees, no useful information is lost.

With the distribution of the first questionnaire, the opinions of experts during the various rounds of this method regarding cybersecurity threats and privacy challenges were presented and analyzed. It should be noted that, based on the organizational experts' perspective, the level of acceptance of each challenge after consensus was considered to be 5. The threshold level of disagreement between the two survey phases, which represents the stopping state of the Fuzzy Delphi algorithm, was considered to be 0.1. After the Fuzzy Delphi questionnaire was sent to the experts and completed using Table 3, the results of their opinion statistics were compiled. Based on the opinions of 10 experts, their combined opinions were calculated using the arithmetic mean, and then the fuzz was removed.

Table 4presents the results of the experts' opinions on cybersecurity threats and privacy challenges in Sana'a's transition to a smart city in the first phase of the survey.

Table 3. Verbal expressions of the level of agreement on the presence of cybersecurity threats and privacy challenges, particularly in the Sana'a Smart City, and corresponding triangular fuzzy numbers.

| The corresponding triangular fuzzy number | Verbal phrase |
|---|---|
| **(1 ،1 ،3)** | Very little |
| **(1 ،3 ،5)** | A little |
| **(3 ،5 ،7)** | Average |
| **(5 ،7 ،9)** | much |
| **(7 ،9 ،10)** | Too much |

Table 4. Average expert opinions in the first phase of the survey

| Fuzzy Average Comments | Average Comments | Cybersecurity Threats and Privacy Challenges | Dimension |
|---|---|---|---|
| **6.33** | (2.5 ,2.7 ,7.8) | Increasing volume of digital transactions | Cybersecurity Challenges |
| **6.73** | (6.5 ,6.7 ,1.9) | Increasing applications and mobile communications | |
| **5.88** | (8.3 ,8.6 ,5.8) | Increasing use of artificial intelligence in digital networks and machine-to-machine communications | |
| **6.93** | (8.5 ,8.7 ,3.9) | Vulnerable software and hardware products | |
| **3.75** | (3 ,6.5 ,3.7) | Cyberwar and terrorism | |
| **5.93** | (5 ,8.6 ,5.8) | Cyber espionage | |
| **3.68** | (8.3 ,6.5 ,5.7) | Data tampering and phishing attacks | |
| **5.38** | (3.3 ,3.6 ,1.8) | Data loss | |
| **6.5** | (3.5 ,3.7 ,9) | Virus and malware penetration of smart city systems | |
| **6.75** | (6.5 ,6.7 ,9) | Legislative challenges | |
| **3.6** | (6.3 ,6.5 ,6.7) | Data, information, and physical device theft | |
| **3.33** | (3.4 ,3.5 ,3.7) | Hardware and software inefficiencies | |
| **5.48** | (3.4 ,3.6 ,1.8) | Challenges in accessing data | |
| **6.08** | (5 ,7 ,7.8) | Insecure APIs and protocols | |
| **5.1** | (2.3 ,6 ,8.7) | Denial of service (DoS) | |

| | | | |
|---|---|---|---|
| **3.05** | (2.3 ,5 ,7) | Sensor failure | |
| **5.53** | (6.3 ,3.6 ,1.8) | Lack of secure communications | |
| **3.88** | (8.3 ,8.5 ,5.7) | Challenges in data management and storage | |
| **5.68** | (6.3 ,6.6 ,3.8) | Disruption of critical infrastructure | |
| **5.88** | (8.3 ,8.6 ,5.8) | Cloud security | |
| **3.7** | (8.3 ,6.5 ,3.7) | AI threats | |
| **6.5** | (3.5 ,3.7 ,9) | Privacy Threats in Data Extraction and Sharing | Privacy challenges |
| **5.88** | (8.3 ,8.6 ,5.8) | Privacy Threats in Data | |
| **6.13** | (5 ,7 ,8.5) | Eavesdropping | |
| **3.65** | (6.3 ,6.5 ,3.7) | Data Access Challenge | |
| **6.08** | (5 ,7 ,7.8) | Confidentiality and Integrity Risk | |
| **6.18** | (2.5 ,7 ,5.8) | Fraud and Data Leakage Risk | |
| **3.9** | (3 ,8.5 ,6.7) | Identity Forgery | |
| **5.9** | (8.3 ,8.6 ,3.8) | Fake Information | |
| **5.3** | (3.3 ,2.6 ,8) | Side Channel Attacks | |
| **5.68** | (6.3 ,6.6 ,3.8) | Secondary Use of Collected Data | |
| **5.55** | (6.3 ,3.6 ,8) | IP Address Forgery | |
| **5.15** | (2.4 ,6 ,6.7) | Attack on data integrity | |

In the second phase of the survey, after updating the first questionnaire and applying each expert's opinion to the average of the opinions, experts were given the opportunity to revise their previous opinions if they wished. In accordance with the first phase, after the results of the new expert opinions were tallied, the average opinions were calculated and simplified. Finally, the difference between the average opinions in these two phases was calculated according to Table 5. Indicators for which the difference between the averages of these two phases was less than the minimum (0.1) were excluded from the survey process or included in the third phase of the survey.

Table 5. Differences in Expert Opinions in the First and Second Phases of the Survey

| **Differences in Steps 1 & 2** | **Average Comments in Step 2** | **Average Comments in Step 1** | **Cybersecurity Threats and Privacy Challenges** | **Dimension** |
|---|---|---|---|---|
| **0.17** | 6.5 | 6.44 | Increasing volume of digital transactions | Cybersecurity Challenges |
| **0.20** | 6.94 | 6.74 | Increasing applications and mobile communications | |
| **0.15** | 5.74 | 5.88 | Increasing use of artificial intelligence in digital networks and machine-to-machine communications | |
| **0.02** | 6.95 | 6.94 | Vulnerable software and hardware products | |
| **0.08** | 4.84 | 4.75 | Cyberwar and terrorism | |
| **0.12** | 6.05 | 5.94 | Cyber espionage | |
| **0.24** | 4.45 | 4.68 | Data tampering and phishing attacks | |
| **0.64** | 4.85 | 5.48 | Data loss | |
| **0.77** | 5.74 | 6.5 | Virus and malware penetration of smart city systems | |
| **0.20** | 6.95 | 6.75 | Legislative challenges | |
| **0.28** | 4.88 | 4.6 | Data, information, and physical device theft | |
| **0.45** | 4.88 | 4.44 | Hardware and software inefficiencies | |
| **1.04** | 4.45 | 5.48 | Challenges in accessing data | |
| **0.02** | 6.1 | 6.08 | Insecure APIs and protocols | |
| **0.45** | 5.45 | 5.1 | Denial of service (DoS) | |
| **0.20** | 4.25 | 4.05 | Sensor failure | |
| **0.50** | 5.04 | 5.54 | Lack of secure communications | |
| **0.04** | 4.85 | 4.88 | Challenges in data management and storage | |
| **0.17** | 5.85 | 5.68 | Disruption of critical infrastructure | |
| **0.04** | 5.85 | 5.88 | Cloud security | |
| **0.45** | 4.25 | 4.7 | AI threats | |
| **0.02** | 6.48 | 6.5 | Privacy Threats in Data Extraction and Sharing | Privacy challenges |
| **0.05** | 5.84 | 5.88 | Privacy Threats in Data | |
| **0.42** | 6.45 | 6.14 | Eavesdropping | |

| | | | |
|---|---|---|---|
| **0.05** | 4.6 | 4.65 | Data Access Challenge |
| **0.00** | 6.08 | 6.08 | Confidentiality and Integrity Risk |
| **0.14** | 6.05 | 6.18 | Fraud and Data Leakage Risk |
| **0.40** | 5.2 | 4.9 | Identity Forgery |
| **0.05** | 5.84 | 5.9 | Fake Information |
| **0.50** | 4.8 | 5.4 | Side Channel Attacks |
| **0.05** | 5.64 | 5.68 | Secondary Use of Collected Data |
| **0.08** | 5.64 | 5.55 | IP Address Forgery |
| **0.08** | 5.24 | 5.15 | Attack on data integrity |

According to the results, it can be noted that the expert panel reached consensus on 79challenges whose level of disagreement in the first and second rounds of the survey was below the minimum (1.7) (the challenges are highlighted in bold in the table above). Therefore, the survey process for these challenges was discontinued. Of these challenges, three—"Cyberwar and Terrorism," "Data Management and Storage Challenge," and "Data Access Challenge"—had an acceptance level below 5. Therefore, they were removed from the final theoretical framework for cybersecurity threats and privacy challenges in Sana'a Smart City. A further 71 challenges were included in the final theoretical framework. By repeating the survey process for four stages, consensus was reached on all challenges, and the final theoretical framework for cybersecurity threats and privacy challenges in Sana'a's transition to a smart city was obtained, as shown in Table .6

Table 6. Final Theoretical Framework for Cybersecurity Threats and Privacy Challenges in Sana'a's Transition to a Smart City

| **Cybersecurity Challenges and Privacy Challenges** | **Dimensions** |
|---|---|
| Increasing volume of digital transactions (C1) | Cybersecurity |
| Increasing mobile applications and communications (C2) | Challenges |
| Existence of vulnerable software and hardware products (C3) | |
| Cyber espionage (C4) | |
| Virus and malware penetration of smart city systems (C5) | |
| Legislative law (C6) | |
| Insecure APIs and protocols (C7) | |
| Denial of service attacks (C8) | |
| Lack of secure connectivity (C9) | |
| Disruption of critical infrastructure (C10) | |
| Cloud security (C11) | |
| Privacy threats in data extraction and sharing (P1) | Privacy Challenges |
| Privacy threats in data (P2) | |
| Mixed eavesdropping (P3) | |
| Confidentiality and integrity risks (P4) | |
| Fraud and data leakage risks (P5) | |
| Identity theft (P6) | |
| Fake information (P7) | |
| Secondary use of collected data (P8) | |
| IP address spoofing (P9) | |
| Attacks on data integrity (P10) | |

Next, to determine the weights of these threats and challenges using the fuzzy best-worst multi-criteria decision-making method, a questionnaire was first designed and distributed among the members of the regulatory expert panel. In this questionnaire, to determine the best and worst indicators, the average acceptance value of these indicators using the fuzzy Delphi method, in addition to the direct views of the expert panel members, was used as criteria. The challenges "Legislative Challenge (C6)" and "Identity Theft (P9)" were identified as the best and worst indicators, respectively. The results are shown in Table 7.

Table 7. Average Expert Opinions on the Priority of the Best (Most Important) Challenge in "Legislative Challenge" (C6) "relative to Other Challenges and Other Challenges relative to the Worst (Least Important) Challenge, "Identity Theft (P9)"

| **Worst Indicator** | **Best Indicator** | **Indicators** | **Dimensions** |
|---|---|---|---|
| (5.3, 6.2, 17.2) | (7.2, 2.2, 72.1) | C1 | Cybersecurity Challenges |
| (2.2, 7.2, 25.2) | (8.2, 2.2, 82.1) | C2 | |
| (1.2, 7.2, 2.2) | (1.2, 6.2, 12.2) | C3 | |
| (9.2, 4.2, 9.2) | (4, 5.2, 2) | C4 | |
| (9.2, 4.2, 92.2) | (6.2, 1.2, 62.2) | C5 | |
| (95.2, 5.2, 5.2) | (1, 1, 1) | C6 | |
| (25.2, 9.2, 45.2) | (2, 5.2, 2.2) | C7 | |
| (5.2, 2, 52.2) | (8.2, 2.2,82.1) | C8 | |
| (55.2, 1.2, 65.2) | (9.2, 5.2, 12.2) | C9 | |

| | | | |
|---|---|---|---|
| (55.2, 1.2, 67.2) | (7.2, 2.2, 7.2) | C10 | |
| (8.2, 2.2, 8.2) | (25.2, 9.2, 47.2) | C11 | |
| (2.2, 7.2, 22.2) | (2.2, 7.2, 22.2) | P1 | Privacy Challenges |
| (7.2, 2.2, 72.2) | (6.2, 1.2, 65.1) | P2 | |
| (25.2, 8.2, 25.2) | (2.2, 7.2, 22.2) | P3 | |
| (45.2, 2, 55.2) | (7.2, 2.2, 7.2) | P4 | |
| (1.2, 6.2, 12.2) | (1.2, 6.2, 12.2) | P5 | |
| (95.2, 5.2, 7.2) | (4.2, 9.2, 42.2) | P6 | |
| (21.2, 8.2, 2.7) | (2, 5.2, 2) | P7 | |
| (2.2, 7.2, 22.1) | (85.2, 4.2, 97.1) | P8 | |
| (1, 1, 1) | (95.2, 5.2, 5.2) | P9 | |
| (22, 7.2, 22.2) | (2, 5.2, 2.2) | P10 | |

By entering the resulting values into a linear programming model, an expanded model consisting of 63 variables and 184 constraints was introduced into the GAMS program. By solving the model, the optimal value for the challenge weight vector and function was determined, and the goal was as shown in Table 1. Given that, according to the standard, the concordance index (CI) for is 6.69, and for the value is 8.04. Since this study obtained then, by making this number certain, the resulting value is 3.5. By calculating the arithmetic means of 6.69and $\tilde{a}_{BW} =$ 8.04, the concordance factor becomes .7.36

$$\tilde{a}_{BW} = (3/05,3/5,3/95)$$

Table 8. Final weights for cybersecurity threats and privacy challenges in Sana'a during the transition to a smart city.

| $w_j^*$ | $\widetilde{w}_j^*$ | **Challenges** |
|---|---|---|
| 0.0435 | (0.033 ,0.033 ,0.062) | C1 |
| 0.0355 | (0.034 ,0.034 ,0.063) | C2 |
| 0.0380 | (0.036 ,0.037 ,0.063) | C3 |
| 0.0323 | (0.035 ,0.032 ,0.051) | C4 |
| 0.0370 | (0.038 ,0.036 ,0.06) | C5 |
| 0.0930 | (0.09 ,0.093 ,0.098) | C6 |
| 0.0515 | (0.036 ,0.051 ,0.069) | C7 |
| 0.0390 | (0.038 ,0.037 ,0.068) | C8 |
| 0.0537 | (0.039 ,0.053 ,0.071) | C9 |
| 0.0328 | (0.033 ,0.032 ,0.056) | C10 |
| 0.0393 | (0.038 ,0.038 ,0.066) | C11 |
| 0.0352 | (0.034 ,0.034 ,0.061) | P1 |
| 0.0347 | (0.035 ,0.034 ,0.057) | P2 |
| 0.0362 | (0.035 ,0.035 ,0.062) | P3 |
| 0.0338 | (0.033 ,0.033 ,0.058) | P4 |
| 0.0378 | (0.033 .0.037 .0.066) | P5 |
| 0.0348 | (0.033 ,0.034 ,0.059) | P6 |
| 0.0370 | (0.031 ,0.037 ,0.063) | P7 |
| 0.0362 | (0.038 ,0.035 ,0.059) | P8 |
| 0.0200 | (0.019 ,0.002 ,0.021) | P9 |
| 0.0388 | (0.037 ,0.038 ,0.063) | P10 |
| | 1.286 | $\bar{\xi}^*$ Quantity |
| | 7.36 | Compatibility Index |
| | 0.175 | Compatibility Rate |

It was noted that five challenge indicators—legislative law (C6), lack of secure communications (C9), insecure protocols (C7), cloud security (C11), and denial-of-service (DoS) attacks (C8)—were identified as the most significant challenges in improving Sana'a's smart city. These five indicators belong to the "cybersecurity threats" dimension, demonstrating the importance of this dimension, from the experts' perspective, to the successful implementation of Sana'a's smart city infrastructure and system. Among the privacy challenges, "attack on data integrity (P10)" was also identified as a significant challenge in improving Sana'a's smart city. The identification of the proposed indicators does not indicate the unimportance of the other indicators; rather, each indicator has a different degree of importance in the emergence of challenges in the Sana'a improvement process, according to the resulting weights. Furthermore, the results obtained for the consistency rate indicate a high degree of consistency in the results and reliability of the questionnaire for this step of the methodology. Since determining the importance of cybersecurity threats and privacy challenges depends on the subjective judgments and expressed preferences of the members of the expert panel in an environment of uncertainty, predicting the behavior of experts' risk tolerance levels using the alpha cut approach based on the weights obtained for these threats and challenges can provide the basis for a sensitivity analysis of this issue.

In other words, this approach will determine the extent to which increasing or decreasing the risk tolerance of experts when presenting their judgments on the relative priority of indicators over each other changes the resulting weights of these indicators. Each complete fuzzy set is uniquely defined by its alpha cutoffs. The alpha cutoffs for any fuzzy number, for any alpha value in the interval [0, 1], are a closed interval of real numbers. The closer the alpha cutoffs in the proposed range are to zero, the lower the risk level of experts in presenting their judgments on the indicators. The results of the sensitivity analysis of experts' opinions regarding the relative priority of indicators at different alpha cutoff levels are presented in Table .9

Table 9. Prediction, sensitivity analysis, expert opinions, and final weights of cybersecurity threats and privacy challenges in smart city development in Sana'a

| Alpha Surface | | | | | | | | | | Factor |
|---|---|---|---|---|---|---|---|---|---|---|
| **α=0/1** | **α=0/2** | **α=0/3** | **α=0/4** | **α=0/5** | **α=0/6** | **α=0/7** | **α=0/8** | **α=0/9** | **α=1** | |
| 1 / 1418 | / 1463 1 | 1 / 466 | / 1469 1 | / 1463 1 | 1 / 1431 | / 1434 1 | 1 / 1457 | 1 / 1441 | 1 / 1445 | C1 |
| 1 / 1417 | / 1413 1 | / 1416 1 | / 1439 1 | / 1411 1 | 1 / 1431 | / 1434 1 | 1 / 1467 | 1 / 1451 | 1 / 1455 | C2 |
| 1 / 1431 | / 1436 1 | / 1434 1 | / 1437 1 | / 1431 1 | 1 / 1411 | / 1436 1 | 1 / 1414 | 11417 | 1 / 1411 | C3 |
| 1 / 1433 | / 1433 1 | / 1431 1 | / 1471 1 | / 1431 1 | 1 / 1436 | / 1475 1 | 1 / 1475 | 1 / 1474 | 1 / 1479 | C4 |
| 1 / 1411 | / 1416 1 | / 1414 1 | / 1417 1 | / 1411 1 | 1 / 1431 | / 1416 1 | 1 / 1414 | 1 / 1417 | 1 / 1411 | C5 |
| 1 / 1341 | / 1341 1 | / 1341 1 | / 1341 1 | / 1341 1 | 1 / 1331 | / 1341 1 | 1 / 1341 | 1 / 1331 | 1 / 1341 | C6 |
| 1 / 1574 | / 1579 1 | / 1537 1 | / 1537 1 | / 1571 1 | 1 / 1573 | / 1571 1 | 1 / 1571 | 1 / 1536 | 1 / 1575 | C7 |
| 1 / 1576 | / 1577 1 | / 1531 1 | / 1574 1 | / 1571 1 | 1 / 1516 | / 1517 1 | 1 / 1431 | 1 / 1444 | 1 / 1431 | C8 |
| 1 / 1543 | / 1541 1 | / 1536 1 | / 1545 1 | / 1549 1 | 1 / 1547 | / 1547 1 | 1 / 1593 | 1 / 1571 | 1 / 1571 | C9 |
| 1 / 1447 | / 1447 1 | / 1441 1 | / 1471 1 | / 1471 1 | 1 / 1475 | / 1477 1 | 1 / 1477 | 1 / 1471 | 1 / 1471 | C10 |
| 1 / 1571 | / 1575 1 | / 1577 1 | / 1513 1 | / 1511 1 | 1 / 1514 | / 1517 1 | 1 / 1433 | 1 / 1436 | 1 / 1437 | C11 |
| 1 / 1417 | / 1411 1 | / 1461 1 | / 1466 1 | / 1467 1 | 1 / 1467 | / 1453 1 | 1 / 1456 | 1 / 1454 | 1 / 1457 | P1 |
| 1 / 1453 | / 1451 1 | / 1456 1 | / 1455 1 | / 1457 1 | 1 / 1457 | / 1457 1 | 1 / 1443 | 1 / 1441 | 1 / 1441 | P2 |
| / 21417 1 | / 1411 1 | / 1411 1 | / 1416 1 | / 1417 1 | 1 / 1417 | / 1463 1 | 1 / 1466 | 1 / 1464 | 1 / 1467 | P3 |
| 1 / 1457 | / 1457 1 | / 1451 1 | / 1441 1 | / 1441 1 | 1 / 1445 | / 1447 1 | 1 / 1447 | 1 / 1441 | 1 / 1471 | P4 |
| 1 / 1437 | / 1437 1 | / 1431 1 | / 1411 1 | / 1411 1 | 1 / 1415 | / 1417 1 | 1 / 1417 | 1 / 1411 | 1 / 1411 | P5 |
| 1 / 1467 | / 1467 1 | / 1461 1 | / 1451 1 | / 1451 1 | 1 / 1455 | / 1457 1 | 1 / 1457 | 1 / 1451 | 1 / 1441 | P6 |
| 1 / 1411 | / 1411 1 | / 1411 1 | / 1411 1 | / 1411 1 | 1 / 1411 | / 1411 1 | 1 / 1411 | 1 / 1411 | 1 / 1411 | P7 |
| 1 / 1417 | / 1411 1 | / 1411 1 | / 1416 1 | / 1417 1 | 1 / 1417 | / 1463 1 | 1 / 1466 | 1 / 1464 | 1 / 1467 | P8 |
| 1 / 1711 | / 1711 1 | / 1711 1 | / 1711 1 | / 1711 1 | 1 / 1711 | / 1711 1 | 1 / 1711 | 1 / 1711 | 1 / 1711 | P9 |
| 1 / 1517 | / 1517 1 | / 1511 1 | / 1431 1 | / 1431 1 | 1 / 1435 | / 1437 1 | 1 / 1437 | 1 / 1431 | 1 / 1411 | P10 |

Figure 2. Predicting changes in the weights of cybersecurity threats and privacy challenges in smart city development in Sana'a, based on experts' risk tolerance levels and their subjective judgments regarding the relative priority of indicators.

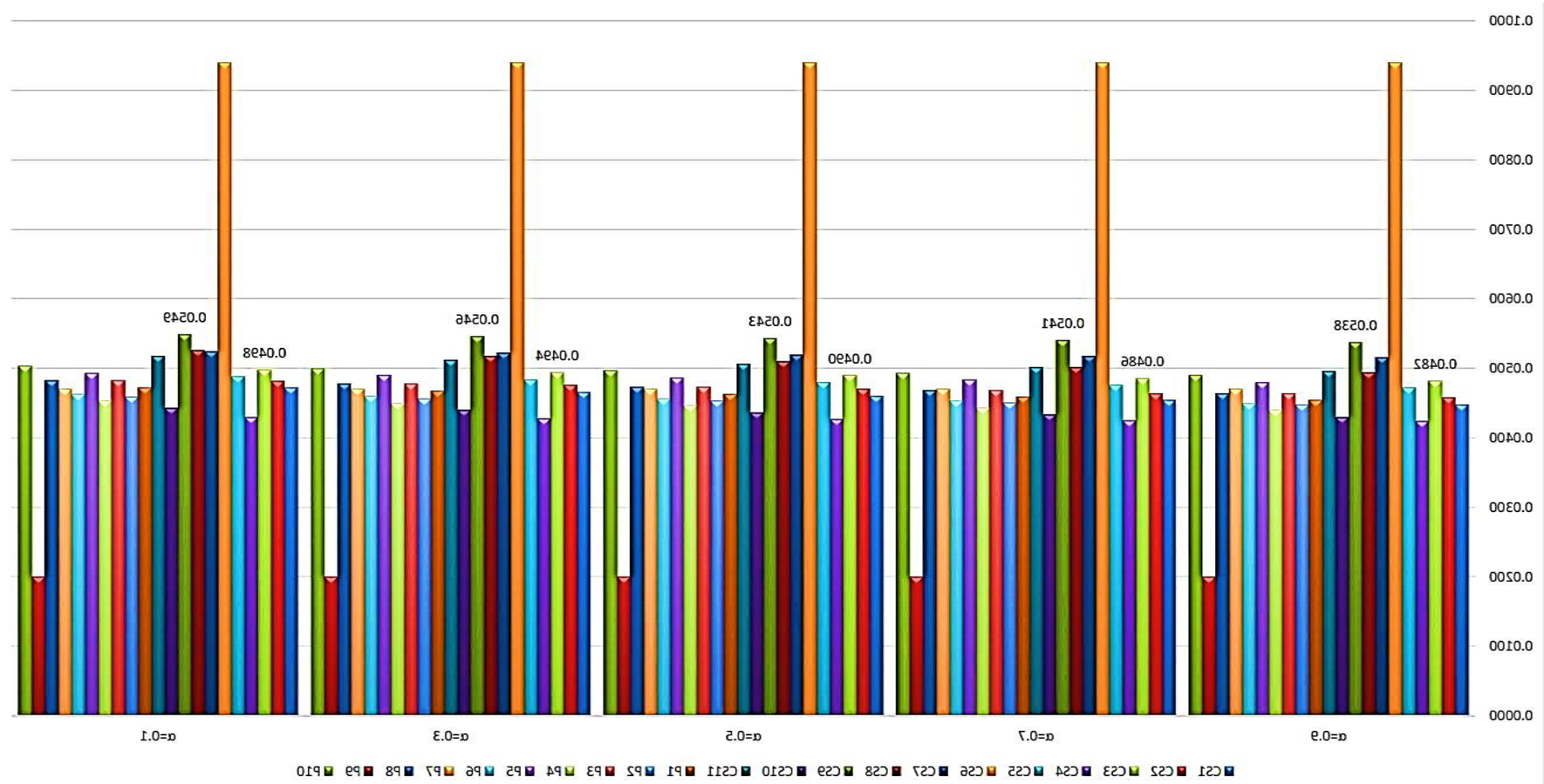


Figure 2. Predicting the weights of cybersecurity threats and privacy challenges in smart city development in Sana'a, based on experts' risk awareness levels

https://doi.org/10.20428/jst.v30i9.3037

As it turns out, as the experts' risk level increased in their judgments regarding the relative importance of cybersecurity threats and privacy challenges (by decreasing the alpha threshold), the weight assigned to that threat and challenge increased. Given that the fuzzy probability functions for all challenges are equal (i.e., the triangular functions are considered linear), the increasing weight of threats and challenges was achieved by decreasing the alpha threshold, according to the slope of the triangular boundary line of that indicator, by a certain factor.

## V. Discussion and Conclusion

Since the successful implementation of the Sana'a Smart City project depends on identifying and assessing cybersecurity threats and privacy challenges and providing a documented plan to address the prioritized threats and challenges, the current study was written with the aim of presenting a model for analyzing cybersecurity threats and privacy challenges in Sana'a's transition to a smart city. This research, both objectively and in terms of communication with the academic community, is expected to address the priorities in the source documentation system, as well as in terms of research methodology and data analysis tools. In this research, a unique model for assessing cybersecurity threats and privacy challenges was implemented using a mixed-method approach, using a fuzzy decision-making approach. Having a plan for addressing cybersecurity and privacy threats, obstacles, and challenges is an important step toward the successful implementation of the Sana'a Smart City project. Based on the research findings, the following strategies and operational plans were proposed to address the threats and challenges identified in the development of the Sana'a Smart City project. These strategies include creating a culture of respect for the legal aspects of security, implementing safety standards, following the recommendations of national cybersecurity agencies and IT security actors, promoting appropriate practices for the use of ICT, developing performance standards, and educating specialists, technicians, programmers, and experts with experience in the fields of networking, ICT, and computer science to include technical measures in their agendas to address cybersecurity threats and privacy challenges. These measures include closing intrusion routes by establishing secure protocols, providing physical security for equipment, network cables, and servers, encrypting network traffic using stable symmetric algorithms, enhancing cloud security, using secure connections such as VPNs for remote access, securing wireless networks with WPA 2protocols, deploying firewalls at every transmission point, etc.

## References

[1] A. AlDairi, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies," *Procedia Computer Science*, vol. 109, pp. 1086–1091, 2022, doi: 10.1016/j.procs.2017.05.391.

[2] S. Alromaihi, W. Elmedany, and C. Balakrishna, "Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications," in *Proc. 6th Int. Conf. Future Internet of Things and Cloud Workshops (FiCloudW)*, 2018, pp. 140–145, IEEE, doi: 10.1109/WFiCloud.2018.00028.

[3] M. J. H. Aljrad and K. Al-Dhlan, "The Effect of Using Social Engineering for Cybersecurity on the Internet of Things Environment," *مجلة العلوم والتكنولوجيا*, vol. 27, no. 2, pp. 43–47, 2023, doi: 10.20428/jst.v27i2.2055.

[4] A. Arabo, "Cyber security challenges within the connected home ecosystem futures," *Procedia Computer Science*, vol. 61, pp. 227–232, 2022, doi: 10.1016/j.procs.2015.09.201.

[5] Z. A. Baig et al., "Future challenges for smart cities: Cyber-security and digital forensics," *Digital Investigation*, vol. 22, pp. 3–13, 2020, doi: 10.1016/j.diin.2017.06.015.

[6] A. R. Berkel, P. M. Singh, and M. J. van Sinderen, "An Information Security Architecture for Smart Cities," in *Int. Symp. Business Modeling and Software Design*, Cham: Springer, 2018, pp. 167–184.

[7] T. Braun, B. C. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustainable Cities and Society*, vol. 39, pp. 499–507, 2018, doi: 10.1016/j.scs.2018.02.039.

[8] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustainable Cities and Society*, art. no. 102655, 2020, doi: 10.1016/j.scs.2020.102655.

[9] C. H. Cheng and Y. Lin, "Evaluating the best main battle tank using fuzzy decision theory with linguistic criteria evaluation," *European Journal of Operational Research*, vol. 142, no. 1, pp. 174–186, 2022, doi: 10.1016/S0377-2217(01)00280-6.

[10] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, art. no. 107094, 2020, doi: 10.1016/j.comnet.2019.107094.

[11] S. Guo and H. Zhao, "Fuzzy best-worst multi-criteria decision-making method and its applications," *Knowledge-Based Systems*, vol. 121, pp. 23–31, 2017, doi: 10.1016/j.knosys.2017.01.010.

[12] C. Manchanda, N. Sharma, R. Rathi, B. Bhushan, and M. Grover, "Neoteric security and privacy sanctuary technologies in smart cities," in *Proc. IEEE 9th Int. Conf. Communication Systems and Network Technologies (CSNT)*, 2020, pp. 236–241, doi: 10.1109/CSNT48778.2020.9115780.

[13] M. Mohammadpourfard, A. Khalili, I. Genc, and C. Konstantinou, "Cyber-Resilient Smart Cities: Detection of Malicious Attacks in Smart Grids," *Sustainable Cities and Society*, art. no. 103116, 2021, doi: 10.1016/j.scs.2021.103116.

[14] J. N. Pelton and I. B. Singh, "Cyber Defense in the Age of the Smart City," in *Smart Cities of Today and Tomorrow*, Cham: Copernicus, 2019, pp. 67–83, doi: 10.1007/978-3-319-95822-4_4.

[15] J. Rezaei, "Best-worst multi-criteria decision-making method: Some properties and a linear model," *Omega*, vol. 64, pp. 126–130, 2022, doi: 10.1016/j.omega.2015.12.001.

[16] V. L. Thing, "Cyber security for a smart nation," in *Proc. IEEE Int. Conf. Computational Intelligence and Computing Research (ICCIC)*, 2014, pp. 1–3, doi: 10.1109/ICCIC.2014.7238277.

[17] F. Zhao, O. I. Fashola, T. I. Olarewaju, and I. Onwumere, "Smart city research: A holistic and state-of-the-art literature review," *Cities*, vol. 119, art. no. 103406, 2021, doi: 10.1016/j.cities.2021.103406.

[18] A. Taklo Beighsh and M. Shayan Fard, "Challenges and Strategies for Security and Privacy in Smart City Applications," in *Proc. 4th Nat. Conf. New Ideas in Engineering*, Rasht, 2019.