International Journal of Information Technology & Decision Making

# Identifying and evaluating factors affecting user privacy in the smart city using the meta-synthesis method and the fuzzy DEMATEL technique

--Manuscript Draft--

| | |
|---|---|
| **Manuscript Number:** | IJITDM-D-22-00174R3 |
| **Full Title:** | Identifying and evaluating factors affecting user privacy in the smart city using the meta-synthesis method and the fuzzy DEMATEL technique |
| **Article Type:** | Research Paper |
| **Keywords:** | user privacy; Smart city; Security; Fuzzy DEMATEL; meta-synthesis method |
| **Corresponding Author:** | Ruhollah Bagheri, Assistant Professor<br>Ferdowsi University of Mashhad Faculty of Economics and Business Administration<br>IRAN (ISLAMIC REPUBLIC OF) |
| **Corresponding Author Secondary Information:** | |
| **Corresponding Author's Institution:** | Ferdowsi University of Mashhad Faculty of Economics and Business Administration |
| **Corresponding Author's Secondary Institution:** | |
| **First Author:** | Rouhollah Bagheri, Assistant Professor |
| **First Author Secondary Information:** | |
| **Order of Authors:** | Rouhollah Bagheri, Assistant Professor |
| | Mahmoud Zahedian Nezhad, Ph.D. student |
| | Mohammad Hosein Panahi Rizi, Ph.D. student |
| | Mosayeb Sadri, Ph.D. student |
| **Order of Authors Secondary Information:** | |
| **Abstract:** | Smart cities are becoming increasingly popular today due to various digital technologies in their infrastructure. One of the most critical challenges in the proper implementation and establishment of these cities is the violation of the security and privacy of users, which leads to citizens' distrust and pessimism about smart city services. Many factors can affect the protection of users' privacy. Identifying these factors helps developers understand what dimensions and aspects are affected users' privacy, through which they can provide appropriate solutions to protect the privacy of the user. Therefore, this study identifies and evaluates these dimensions. The authors proposed a novel methodology for identifying factors influencing user privacy in smart cities using the meta-synthesis method and the fuzzy decision-making trial and evaluation laboratory (DEMATEL). As a result of the meta-synthesis application, the authors identified seven dimensions of interest. Specifically, Awareness and understanding, Trust, Self-control and personalization, Transparency, Reference standards frameworks and rules, Data management, and Security requirements. Moreover, using the DEMATEL technique and expert-based reviews, those seven dimensions were classified as cause and effect. As a result, the authors discovered that security requirements (D7) are the only cause dimension. As effect dimensions, "awareness and understanding (D1)," "data management (D6)," "trust (D2)," "frameworks and standards (D5)," " personalization and self-control (D3)," and "transparency (D4)" have been identified. Furthermore, the authors discovered that transparency is the most effective dimension in terms of affecting user privacy in smart cities. These findings may serve as guidelines for implementing the smart cities initiatives and protecting users' privacy. This study also provides a discussion and insights for smart city developers. |
| **Response to Reviewers:** | First, I would like to express my gratitude to the respected Editor-in-Chief, Dr. Gang Kou, for taking into consideration our efforts in research. We thank the Reviewers for their excellent suggestions and guidance in improving the manuscript's content. We value the time and effort the reviewers spent assessing our manuscript. Thank you for |

| | |
|---|---|
| | the opportunity to submit a revised manuscript and for your constructive comments on our manuscript. We hope, this article can be helpful to both practitioners and academicians in field of smart cities.<br>Reviewers' comments: The references should be updated with the most recent in your paper's research field of relevance.<br>All of the recommended references have been included in the paper. We hope that this addresses the concerns raised by the reviewer.<br>Best regards |

# Identifying and evaluating factors affecting user privacy in the smart city using the meta-synthesis method and the fuzzy DEMATEL technique

**Abstract**. Smart cities are becoming increasingly popular today due to various digital technologies in their infrastructure. One of the most critical challenges in the proper implementation and establishment of these cities is the violation of the security and privacy of users, which leads to citizens' distrust and pessimism about smart city services. Many factors can affect the protection of users' privacy. Identifying these factors helps developers understand what dimensions and aspects are affected users' privacy, through which they can provide appropriate solutions to protect the privacy of the user. Therefore, this study identifies and evaluates these dimensions. The authors proposed a novel methodology for identifying factors influencing user privacy in smart cities using the meta-synthesis method and the fuzzy decision-making trial and evaluation laboratory (DEMATEL). As a result of the meta-synthesis application, the authors identified seven dimensions of interest. Specifically, Awareness and understanding, Trust, Self-control and personalization, Transparency, Reference standards frameworks and rules, Data management, and Security requirements. Moreover, using the DEMATEL technique and expert-based reviews, those seven dimensions were classified as cause and effect. As a result, the authors discovered that security requirements (D7) are the only cause dimension. As effect dimensions, "awareness and understanding (D1)," "data management (D6)," "trust (D2)," "frameworks and standards (D5)," "personalization and self-control (D3)," and "transparency (D4)" have been identified. Furthermore, the authors discovered that transparency is the most effective dimension in terms of affecting user privacy in smart cities. These findings may serve as guidelines for implementing the smart cities initiatives and protecting users' privacy. This study also provides a discussion and insights for smart city developers.

***Keywords***: user privacy, smart city, security, fuzzy DEMATEL, meta-synthesis method

## 1. Introduction

Cities are growing steadily around the world, and urbanization is on the rise. There is a growth in the number of cities, but this does not necessarily mean that they are getting better. As a way to improve the lives of citizens, a new concept of a city has been born: the smart city. A smart city is not clearly defined, but many cities are taking steps to become smarter. The goal of smart cities is to solve many local challenges through information and communication technology, from local economy and transportation to quality of life and e-government. The ability of technology to gather a great deal of information could endanger citizens' privacy, even if it can help solve many of these local problems [1]. To create smart cities, several modern cities integrate information technology into all aspects of city life. An array of applications and technologies are used by smart cities in order to interact with citizens, third parties, and city departments. It is therefore important to better understand the privacy implications of smart cities [2]. A smart city is one that integrates modern technologies to provide efficient and automated services to enhance the quality of life of its citizens [3]. It has become an umbrella term for a wide range of technologies to improve cities' critical infrastructure and quality of life for residents. Using Information and Communication Technology (ICT) infrastructure, smart cities aim to support social and urban interconnection. [1]–[5]. In smart cities, modern technologies are used to enable different components to interact and cooperate, such as mobile cloud computing, electronic objects, networks, sensors, and machine learning. [9]. With the advancement of information technology, it has become possible to collect more data and create services based on that data. City operations were improved by implementing those solutions. In a Smart City, these technologies create an ecosystem of data that can be used to create apps and systems to achieve different goals. As part of the development of smart cities, the Internet of Things (IoT) technology plays an important role. Currently, IoT is a hot topic among researchers and experts. It allows all objects/things in our environment to communicate over the Internet without human intervention [10]. IoT uses the Internet to connect nearly all devices to share data and develop new applications and services that improve our quality of life. Various devices and objects around us can be addressed, recognized, and located using IoT. Wireless or wired connections can be made between various IoT objects. With this addressing scheme, objects can interact and cooperate to create new applications and services, such as smart homes, smart transportation, smart cars, smart grids, smart cities, and smart traffic management. [6] Data about the city are collected, analyzed, and stored by a wide range of municipality departments, private and public stakeholders, and individual citizens and visitors without any coordination or collaboration. Through Wired and Wireless Networks, cities can become smarter in six dimensions: Smart Economy, Smart People, Smart Governance, Smart Mobility, Smart Environment, and Smart Living. It is evident that smart cities are complex and interdependent huge systems that present many political, social, economic, and technical challenges. Security and privacy are two examples of these challenges [3]. These six dimensions are defined as follows [1], [7]–[9]:

1 .Smart economy: The combination of entrepreneurship, innovation, flexibility, labor market productivity, trademarks, and international participation to increase economic competitiveness.

2 .Smart people: This includes citizens' education, social interactions, and perceptions of public life in addition to their education.

3 .Smart governance: Ensures that political engagement, citizen services, and administration are taken into account.

4 .Smart mobility: Utilizing ICT and sustainable and relevant transportation infrastructure to ensure local accessibility and global connectivity.
5 .Smart environment: Preserve green spaces, reduce pollution, conserve resources, and managers for the benefit of the environment.
6. Smart living: Includes many aspects of quality of life, such as health, housing, culture, tourism, and safety.
The numerous vulnerabilities found in each layer of smart applications may pose several security and privacy risks. Furthermore, IoT systems are highly vulnerable to security and privacy risks due to their heterogeneity, scalability, and dynamic nature. As a result of the emergence of new technologies such as machine learning and data mining, attackers have become smarter and can bypass existing attack detection mechanisms [10]. It is important to address cyber-related threats early in the design and development process to prevent undesired outcomes [16]. Despite the IoT's infinite benefits, it also poses several challenges, especially in terms of privacy and security. A fundamental priority must be given to the security and privacy of IoT products and services. Data privacy refers to protecting data from unauthorized access or re-use, as well as protecting the collection process and all operations associated with it. Because of this, smart cities pose a major threat to citizens' privacy: Big data allows the creation of detailed profiles encompassing every aspect of their lives. Interconnectivity further complicates privacy issues. Correlating multiple data sources from different data holders, devices, and applications improves service quality and availability but increases the risk of sensitive data leaks. It is common for smart city applications to collect and transmit data without allowing the user to control it. As a result of this loss of data sovereignty, many people are unable to opt-out of the smart city. Meanwhile, privacy protection does not seem to be a fundamental part of current smart city development [11]. It is the heterogeneity of smart cities that poses the greatest challenge; the protocols and architectures used within smart cities are different and incompatible [17]. Data collection and storage combined with powerful analytics raises the risk of privacy violations. It is imperative that smart city solutions are implemented diligently. Therefore, preserving privacy can be critical to the success of new products or services [18].

### *1.1. Problems, motivation and proposed solution*

The concept of smart cities has been introduced to enhance the quality of life for citizens by incorporating modern technologies into all aspects of city life. As IoT services proliferate, smart city applications are becoming more competitive; It is typically necessary for system developers to meet strict deadlines in order to maintain their competitive advantage. Security and privacy requirements are often considered afterthoughts during this accelerated development process, which can later be incorporated as features. The privacy implications of smart cities need to be better understood to ensure that citizens' data is not misused. Therefore, immature products fail to satisfy the security and privacy requirements of their target applications [17], [19]. As a result of the interconnectedness and independence of objects, as well as their limited computing capabilities, conventional security mechanisms cannot be applied. Since each technology has a different vulnerability, the heterogeneity of the IoT technologies complicates security processes. Moreover, access control systems cannot effectively manage and function due to the volume of data generated by multiple interactions between users and objects. [12].
The dimensions and vital factors affecting the user's privacy are closely related to the privacy of the data. For example, one of them is the General Data Protection Rules (GDPR), which, by specifying rules and standards regarding data privacy, requires

equipment manufacturers and service providers to comply with them to address future privacy issues and prevent data collection from users. The GDPR acts as a regulatory authority to determine how each stakeholder should respond to potential issues. In the smart city, various other factors can affect a user's privacy. For this reason, this article seeks to answer the questions, what are the most important factors affecting user privacy in the smart city? Moreover, which of these factors is more important and effective? To answer the first question and identify these dimensions and factors, this study uses a hybrid approach to extract the effective factors systematically. As to the second question, since these dimensions and important factors in user privacy are closely related, it is impossible to determine which factor is more important than the other. There may be causal relationships between these dimensions. Therefore, these dimensions should be examined using the opinion of experts. On the other hand, experts' opinions are naturally accompanied by a degree of protection and uncertainty, and usually they do not express their answer explicitly, but use qualitative words such as "low", "high" and "average" to express their ideas. Fuzzy set theory is a powerful mathematical tool that can be used in situations of uncertainty. In this research, to solve this problem, the "fuzzy logic" method has been used, so that first the experts' opinion is modeled as a set of fuzzy numbers and then using the Fuzzy DEMATEL method, which shows the causal relationships between dimensions. This method determines and ranks their importance.

Accordingly, the following sections are included in this study: Section 2 reviews the literature and examines the stages of the meta-synthesis approach and the dimensions extracted. Section 3 describes the research methodology as well as the main concepts of fuzzy logic theory and the DEMATEL method. In Section 4, the details of the problem and the method of solving it are examined, and then the findings of prioritizing the dimensions affecting user privacy in the smart city are expressed using the Fuzzy DEMATEL method and the proposed dimensions of the research are validated. Finally, Section 5 summarizes and concludes.

## 2. Literature Review

Various dimensions and factors affect user privacy in the smart city, these dimensions can have both quantitative and qualitative aspects. Since the meta-synthesis method is a qualitative approach that examines and combines both quantitative and qualitative results, it can be a suitable approach to identify these dimensions; therefore, in this study, the meta-synthesis method has been used. This research is applied in terms of purpose and quantitative research in data collection.

In order to identify and extract these dimensions through the meta-synthesis method, the seven-step method of Sandlowski and Barroso (2007) has been adopted. Figure 1 illustrates the steps of this method. The first step in the meta- synthesis approach is to determine the questions that the researcher seeks to answer. The first research question, which was mentioned in the introduction section and this approach has been adopted to answer it, is: What are the most important factors affecting user privacy?

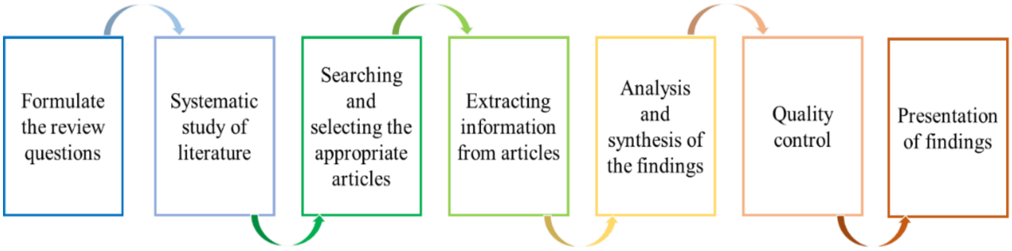
Formulate the review questions
Systematic study of literature
Searching and selecting the appropriate articles
Extracting information from articles
Analysis and synthesis of the findings
Quality control
Presentation of findings

Fig 1. Sandlowski and Barroso 7-step pattern

In the second step, to systematically review the resources, two scientific databases of Web of Science and Scopus were selected and based on three combined keywords, namely "Smart City," "Privacy," and "User," papers were extracted in the period 2010 to 2021. The extraction formula is as follows:

TS= (“Smart city” AND “Privacy” AND “User”)

The third step is to review the articles and select the relevant papers. The selection of these papers is based on the criteria listed in Table 1. The extracted papers were examined in 5 stages, namely in terms of title, abstract, accessibility, content, and finally, the methodological quality of the papers.

Table 1. Criteria for accepting papers

| Criteria | Inclusion criteria | Exclusion criteria |
|---|---|---|
| **Paper’s language** | Studies written in English | Studies not written in English |
| **Time of presenting papers** | Papers published from 2010 to 2021 | Papers published prior to 2010 |
| **Research subject** | Smart city and user’s privacy | Cases different from the mentioned subject |
| **Type of study** | Articles published in Reputable journals and scientific databases | Conference papers, books, websites, and personal comments |

In the screening phase, 134 and 267 articles were extracted from Web of Science and Scopus scientific databases, respectively, of which 55 articles were common between the two databases. At first, each database was reviewed separately based on two steps, i.e., review in terms of title and abstract. Then, before reviewing the third step (review in terms of availability), duplicate and common articles of two databases are identified. Thus, out of 55 common and duplicate papers in both databases, 26 papers were accepted in terms of title and abstract, which Scopus papers were then combined based on Web of Science articles. In other words, 99 papers were reviewed in the fourth stage, i.e., content review from both databases. The screening process of the articles is shown in Figure 2. The last step, the methodological quality review, was omitted due to the excellent quality of the Web of Science and Scopus databases, and 75 papers that were content-acceptable were considered the final number of articles.

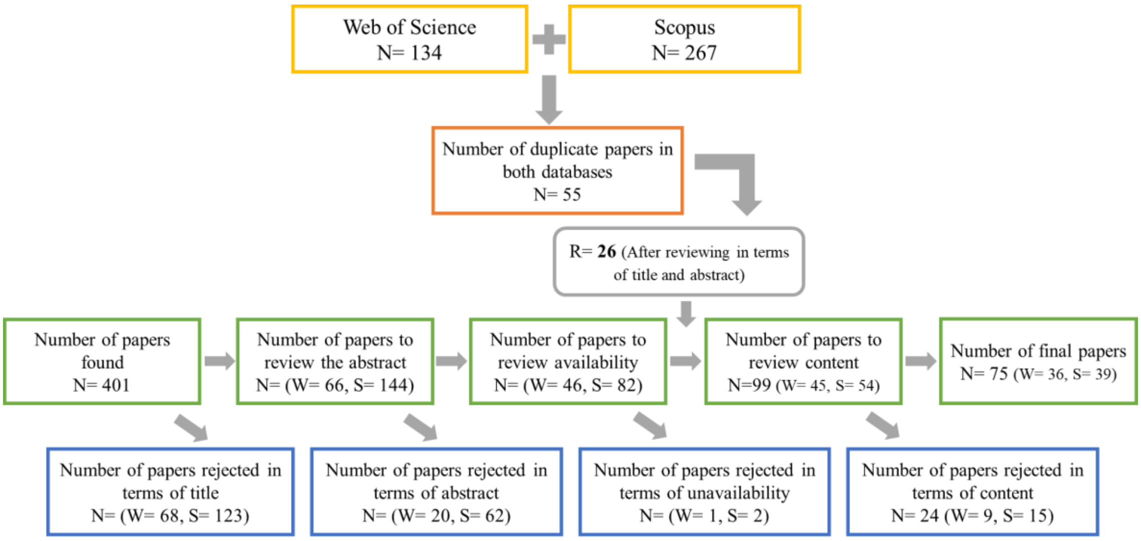
Web of Science
N= 134
Scopus
N= 267
Number of duplicate papers in both databases
N= 55
R= 26 (After reviewing in terms of title and abstract)
Number of papers found
N= 401
Number of papers to review the abstract
N= (W= 66, S= 144)
Number of papers to review availability
N= (W= 46, S= 82)
Number of papers to review content
N=99 (W= 45, S= 54)
Number of final papers
N= 75 (W= 36, S= 39)
Number of papers rejected in terms of title
N= (W= 68, S= 123)
Number of papers rejected in terms of abstract
N= (W= 20, S= 62)
Number of papers rejected in terms of unavailability
N= (W= 1, S= 2)
Number of papers rejected in terms of content
N= 24 (W= 9, S= 15)

Fig 2. The screening process of articles from Web of Science and Scopus

The dimensions affecting users' privacy were extracted and combined in the fourth and fifth steps. The meta-synthesis output showed that seven major dimensions play an important role in protecting users' privacy, in 72 papers addressed the concepts related to these dimensions. The desired dimensions and the articles mentioned are listed in Table 2.

Table 2. Dimensions affecting user privacy in the smart city.

| Dimension | References |
|---|---|
| Awareness and understanding | [13]–[33] |
| Trust | [14], [25], [30], [34]–[41] |
| Self-controlling and personalization | [16], [18], [21], [26], [33], [38], [42]–[51] |
| Transparency | [13]–[19], [25], [29], [32], [33], [40], [49], [50], [52]–[55] |
| Reference standards, frameworks and rules | [16], [17], [19], [21]–[23], [26], [29], [32], [34], [40], [45], [47], [49], [53], [54], [56]–[68] |
| Data management | [17], [35], [39], [50], [56], [61], [63], [69]–[72] |
| Security requirements | [16]–[21], [29], [31], [34], [40], [45], [47], [49], [50], [53]–[55], [62], [63], [65], [71]–[83] |

This study used the agreement kappa coefficient in the fifth step to control and evaluate the extracted dimensions. In this method, extracted dimensions were given to two experts to evaluate the importance of dimensions in terms of their effectiveness. Each expert rated the dimensions separately without knowing the other expert comments. The kappa index value in SPSS software was equal to 0.696. Given an approximate significant number of 0.053, this index is accepted. The results of kappa coefficient calculations are shown in Table 3.

Table 3. Agreement kappa coefficient

| | Value | Asymp.<br>Std. Error | Approximate | Appr. Sig. |
|---|---|---|---|---|
| Measure of Agreement<br>Kappa | 0.0696<br>7 | 0.268 | 1.932 | 0.053 |
| N of Valid Cases | | | | |

Each of the dimensions mentioned in Table 2 is examined in the following subsections.

### *2.1. Understanding and awareness*

Privacy breaches are largely caused by a lack of awareness on the part of users. Smart city users should be fully aware of their protection against all kinds of privacy threats. Users' awareness and knowledge of their rights against privacy risks and vulnerabilities should be enhanced by introducing many smart city programs and technologies [16], [20], [21]. Raising this awareness is a challenging task because it cannot be done directly by researchers and is usually at the disposal of the media and political powers. Awareness includes improving users' knowledge of issues related to collecting private data and how security agencies use this data [39], [62]. Increasing awareness initiatives will be crucial for the safe deployment of smart cities equipped with the Internet of Things. A user's lack of awareness can indicate security and privacy risks that can affect other systems and users in a smart city. In addition to IoT, some new technologies such as artificial intelligence, cloud centers, and Blockchain also offer many initiatives in the smart city. Some of these technologies are not yet fully developed, and there may be concerns about the " Violation " of privacy for users. Therefore, smart city stakeholders and developers need to inform users about the use of these technologies, their data handling, the security they need, and their privacy [32]. Measures may be taken in a particular system to increase public awareness of privacy threats. Privacy awareness systems and services are expected to comply with specific frameworks, laws, regulations, ethical requirements, and operational standards in this area. Using these services will require users to have specialized knowledge and predefined solutions to handle different privacy concerns [35]. Increasing awareness of the privacy threats associated with many smart city applications and technologies is necessary. Users need to understand better that personal data is valuable, leading to their more conscious use of the services within the concept of smart cities. Examining the issue of smart city acceptance by users and stakeholders can also be helpful in realizing this awareness. In this regard, the results of the meta-synthesis approach show that several studies have examined the awareness and perception of smart city users. Those have used theories and models like the unified theory of acceptance and use of technology (UTAUT), UTAUT2, and the technology acceptance model (TAM) to examine this acceptance. For example, Habib. etal. (2020) have proposed a Smart Cities Stakeholder Acceptance Model (SSA), based on the UTAUT2, their results show that the factors of this model significantly affect the desire of citizens to use smart city services. They also see perceived security and privacy as key factors in realizing users' trust in technology [30]. Awareness along with transparency and trust can complement each other in protecting the privacy of users in the smart city. People often associate "smart cities" with privacy concerns, but by providing information about how data is collected and privacy measures, they will feel more comfortable sharing their data [15]. This shows that providing transparency by smart city developers about user data and privacy measures can be effectively related to awareness.

### *2.2. Trust*

Trust is a key factor in the acceptance of new technologies. Numerous definitions of trust have been proposed in the literature. However, trust is usually expressed as one party's willingness to rely on the behavior of another, especially in situations in which the first party is at risk. When dealing with someone you trust, accepting a certain level of risk and vulnerability is always necessary. This risk acceptance is based on the anticipation that the trusted party will take beneficial or essential actions for the vulnerable party [41]. Creating trust among users is essential to expand the operational scope and effectiveness of smart city systems and infrastructure. Users will be reluctant to interact with smart city systems without the trust from all stakeholders. Where users have concerns about security or privacy threats, silence in interaction can indicate low levels of trust [84]. Trust in the smart city, like other areas related to technology, is a fundamental issue. In view of the fact that the smart city environment is surrounded by various sensors and devices that are constantly collecting information that must process and manage data based on user needs. Trust in key actors, governments, private companies, and third parties that collect and process data is crucial. Privacy and trust are interconnected and multidimensional concepts and are determined by various personal and content factors. People are concerned about security vulnerabilities and privacy breaches when using smart city services. Perceived security and privacy are directly related to trust in the use of smart city services. Public trust must be considered in the development of a smart city [85]. Citizens' trust in infrastructure, technology, security services and policies, and privacy in the smart city leads to their satisfaction. By increasing users' satisfaction with the system, it can expect to facilitate and increase their participation and interaction in the development and better implementation of the smart city, which is essential for the successful implementation of the smart city. Acceptance and consent are necessary conditions for the legal collection and processing of data. By creating appropriate trust-based mechanisms, user satisfaction and participation in smart city projects can be guaranteed. However, the consumer cannot adequately express their privacy preferences and trust in the current declaration and consent procedures, which are clearly demonstrated in privacy policies. As smart cities develop, consumers' trust priorities will need to be addressed [39], [86]. To encourage users to use smart city services, smart city civic managers should organize programs and campaigns that increase awareness and trust in users' minds so that they can engage themselves properly and use these services without any fear [38]. Citizen interaction with a smart city can be hindered by the loss of trust and privacy of users. Therefore, in accordance with the law, it is imperative to implement cohesive trust and privacy policies [36].

### *2.3. Transparency*

To maintain users' trust, operations in a smart city must be visible and transparent. Transparency refers to the fact that if users' data is collected and stored by governments and companies, they tell users what data is being stored about them [87]. Data transparency should be considered when designing smart city applications. Users should see the status of their data and know what data is collected, how it is processed, what type of data is stored, with whom it is shared, and how to be protected. For example, cities can send monthly reports to citizens of data stored about them so they can easily correct or delete it. Transparency increases the level of trust of citizens and thus increases the possibility of accepting smart city programs [55]. Transparency helps users understand different levels of privacy by explaining the methods, mechanisms, and operation of systems. Users need to know the answers to the following questions clearly: Who has access to the data? Does the third party have access? What information is inferred from the data? Is their data shared abroad? Is there a known vulnerability in the device? Can they track the user through the data? What can a user do if their personal information is compromised? Is there a copy of the user information? Therefore, developers of initiatives and privacy designers of smart cities must observe the element of transparency, and citizens must be aware of all the information about the fate of their data [35], [39], [62]. As a result, smart city users should be aware of significant doubts about the use of their data [25]. Some smart city stakeholders also believe that data privacy regulations need to be further organized before implementation. Transparency about how and what data is to be used may minimize users' privacy concerns and further their participation in accepting smart city initiatives and disseminating their data. If users know what is going to happen with their data and how it can affect and help their daily activities, in addition to acceptance, they will gain more trust. [32]. Also, the data owner, in addition to observing the full transparency of his/her data, must have full transparency of processes, all security changes, and control of data access, in a word, the whole system must be transparent [17]. Also, if the requirements used to protect the privacy of users are not transparent, this lack of transparency makes it difficult to assess risk and accountability of stakeholders for privacy and security in the smart city. People who design, develop, implement, and deploy smart city initiatives are responsible for ensuring that user privacy and security are not compromised. This transparency in their design, implementation, and operation enables them to be evaluated, validated, and held accountable. Elahi. etal. (2019) show that those responsible for ensuring the privacy and security of citizens and the products of the smart city may violate conditions such as transparency for their own benefit. In order to achieve transparency, they recognize that standards and specifications for smart city products must be developed by independent institutions with participants of all stakeholders [29]. To that end, smart city developers need to reassure users that the security of their personal data is guaranteed. Future measures and precautions may require smart city users to be authenticated, but users may be afraid to share their identity data with regulators. They fear that their data in smart city apps could be linked to their identity data and violate their privacy. Although requiring a user to register before posting content may deter some users from participating, the transparency granted can address these doubts and gain users' trust. Aspects of transparency also encompass algorithmic transparency, i.e., the openness of algorithms for processing, storing, and transferring data. Algorithmic transparency can increase the level of privacy. This is true for almost every technology in the smart city, such as how IoT data is processed or how smart systems make decisions. Transparency of smart systems plays a vital role in protecting the privacy of smart city residents. The lack of transparency of the processing that an application performs poses a significant risk to protecting the privacy of citizens in smart cities [18]. Therefore, implementing new smart city technologies requires new policies for all stakeholders to increase transparency to trade off the benefits of the smart city with its security risks [29], [50].

### *2.4. Personalization and self-controlling*

Designers and planners face significant risks when transitioning from traditional infrastructure to smart city initiatives unless user-related factors are sufficiently considered. Privacy breaches occur when systems collect user information without considering their privacy preferences, so user preferences must be considered when developing a smart city privacy model. Self- controlling means that data owners can manage and control their data and specify details, level of granularity, data protection methods, data collection and data retention intervals. The best smart services should offer a variety of choices based on users' preferences. Options that the user can change according to their preferences, for example: change the device's default permissions and settings, including access to location, image, and videos. This process is time-consuming and requires knowledge and expertise. If the user does not have enough knowledge in this field, the default settings selected by the privacy engineers will be much more important. First, users are asked about general decisions (are they allowed?) And then, more precise controls are given (What type of data are allowed to be collected?) Minor cases are likely to lead to additional information overhead and, it makes the choice for the user more difficult. Using statistical analysis techniques, it is possible to determine which aspects are displayed in the upper layer of the user interface and which elements are displayed in the lower layers. People need different settings, and the default settings cannot be considered for everyone. Users must be clustered based on their behavioral data and analyzed by machine learning to achieve optimal settings in the data set. Clustering methods can improve forecasting accuracy and select the most appropriate settings [18], [46], [67]. Current studies assume the same level of privacy protection for all users, leading to a uniform protection standard. Users' privacy concerns and protection requirements are basically customized in the real world. Especially when it comes to personalization services, it may not be fair to provide the same level of protection for each user [88]. One of the current problems of smart cities is the limitation of users' ability to control their personal information. Suppose smart city services have mechanisms for the level of user control over their data and personalization of services tailored to their activities. The services offer a variety of options for users according to their preferences and interests, and personalize security and privacy concerns in the real world when needed. Because attitudes and requirements may vary from person to person, and each person has their own privacy needs and requirements. Therefore, user-friendly assistants should be developed to facilitate the safe and easy use of various smart city applications. An example of personalizing the privacy of a mobile contact and giving them different access to location information is that some users can access the exact location, some with an error of more than five kilometers, and some have no access at all. It may also be necessary for smart city users to select hardware components and software components in order to build and customize their smart environment. In addition, users must be able to grant and revoke access privileges to other users and service providers. Although service providers need to access, collect, store, and process data in order to provide certain types of services, they must treat consumers fairly and respect their privacy needs [16], [18], [47]–[50]. Unfortunately, many service developers make it impossible for users to manually consider user-centric privacy preferences in their services. It is ideal for users to set their own privacy preferences, and smart city services will automatically conform to these preferences or notify them if they cannot. If possible, the quality of service should not depend on user privacy settings to prevent further punishment of users [42], [51].

### *2.5. Data management*

Data management is one of the most significant issues in the smart city. The output of the meta-synthesis method shows that in most extractive papers, issues related to data and its relationship to user privacy are thoroughly discussed. These issues include data privacy, data confidentiality, collection, storage, access, sharing, merging, and hiding data. In addition, some articles have also examined the role of data governance. All of these issues can be reflected in the importance of data management, which has a lot to do with user privacy. In light of that, this dimension is considered one of the dimensions affecting user privacy. Smart city services and applications generate huge amounts of data that their management is critical. There are various stakeholders in the data management structure, including policymakers, manufacturers, service providers, users, and beneficiaries. The relationship of each of these stakeholders to smart city data may play different roles. These roles include data generators, data collectors, data processors, data providers, and data consumers [56]. Smart city developers and policymakers have proposed various technical and non-technical initiatives for data management. These initiatives can be in the form of standards, frameworks, regulatory rules, or data management reference architectures in the smart city. Major processes in data management include collection and acquisition, storage and processing, dissemination, maintenance, and finally, the use of data, each of which has specific requirements for user's privacy protection [69]. Some actions can affect data richness, quality, and security within these processes and compromise user privacy, such as data fusion, sharing, and access. Data fusion in the data management process is a fundamental step. The reason for the importance of data fusion is that if the number of different platforms and data centers is enormous, user privacy protection will be complex. It should be noted that data fusion also has its own challenges that should be approached appropriately [70]. Technical and socio-legal aspects and challenges must be considered in data management. Technical aspects refer to the role of digital technologies in data management and the use of architectures and systems derived from them [69]. For example, cloud centers and fog and edge computing have made data collection, processing, and storage more manageable and more secure, and blockchain has provided valuable solutions for secure data sharing [53]. For example, Cha. et al. (2021) proposed a blockchain-based cloud architecture based on secret sharing that can solve privacy issues. Data is distributed and stored on multiple blockchain networks in this architecture instead of independent CSPs [79]. However, it should be noted that each of these technologies has its own architecture and even uses different standards, which is another challenge to protecting the security and privacy of users. Data management is also affected by social and legal challenges. The development of different data management frameworks and standards (architectures and technological) and the non-compliance of some of them with the rules and reference standards for data protection, including the GDPR, may create legal challenges. The most important thing, as mentioned in the dimension of transparency, is the accountability and responsibility of each party. This inconsistency and complexity in legal aspects pose many threats to user privacy. Ethical aspects of data management can also be another social and legal challenge. The importance of ethical aspects in data collection and use becomes more apparent. Smart city users must be informed and transparent about managing their data How and what kind of data is to be collected? What are stakeholders supposed to have access to the data? Moreover, other questions arise in the data management process for stakeholders, especially users. Proper data management requires policies and frameworks that facilitate processes and ensure that the security and privacy of data and users are maintained. Governments, regulators, and developers can formulate these policies in collaboration with the expert community.

### *2.6. Security and privacy reference rules, frameworks and standards*

Implementing smart city initiatives requires policies, standards, regulations, and reference frameworks. One of the smart city issues that depend on these policies is data privacy protection and consequently user. This subsection discusses the concepts of privacy protection in the form of protection standards, certificates, general data protection laws and regulations, legal and regulatory aspects. These non-technical mechanisms act as a complement to the technical mechanisms. They must be carefully designed in a comprehensive privacy protection mechanism and fully considered in developing a smart city. Data can play a considerable role in protecting users' privacy. As mentioned in the Data Management subsection, several processes are involved in data management, each of which affects user privacy. A well-defined and enforceable law must govern the data lifecycle to ensure stakeholders follow accepted ethical standards during production, use, dissemination, classification, and storage. On the other hand, in addition to data security, breaches of the safety of infrastructures such as devices, services, and platforms may also pose a potential threat to user privacy. Smart city developers and privacy frameworks designers cannot set different standards, regulations, and policies to protect data privacy and user privacy (apart from protecting the security of infrastructure and systems). The wide range of these policies and standards creates a great deal of complexity and exposes smart city stakeholders to various rules and solutions. There are still no universally agreed protocols, standards, and reference rules for user privacy in the smart city. If there are laws, they are formulated and implemented locally [89]. Following standardized methods and techniques is very important for implementing a smart city. For example, to ensure that the devices and technologies used in the smart city are safely and efficiently produced and utilized, standards have been developed that equipment manufacturers and developers are required to comply with. International Electrotechnical Commission (IEC) and International Telecommunications Union (ITU) have also developed standards in this area. The most prominent standards in this field have been provided by ISO, IEC, ITU, IEEE [1]. Therefore, according to various contexts and initiatives in smart cities, developers have developed and implemented these laws and policies by their region. For example, the European Union and various countries such as the United States, China, Mexico, India, and Brazil have adopted their protection laws. In this regard, the Organization for Economic Co-operation and Development (OECD) has established a framework for protection by limiting data collection and the need for user satisfaction, if possible, and individuals' awareness of any data collection. In addition, Asia-Pacific APEC provides a framework for defining concepts such as injury prevention, warning, data collection restrictions, the use of personal information, security protections, access, correction, and accountability. With the GDPR, The European Union has created a new framework for data protection with new obligations for organizations and the wider domain. As part of this law, the consumer also has rights, including access to their data, the right to be forgotten, the right to modify, and the right to restrict the processing of their data. There are clear rules regarding collecting data from individuals, access to personal data, modification and deletion, not automatically creating user profiles, and granting the right to protest. Substantial consequences will follow if these laws are not followed (fines up to 20 million euros or 4% of global revenues, whichever is higher) [36], [90], [91]. These frameworks and rules also provide requirements and guidelines to protect data and user privacy. The role of the GDPR can be considered a regulatory body for smart city stakeholders (such as equipment manufacturers, service providers, application developers, and users), and even governments, which monitor their activities and behaviors concerning users' data and privacy. In addition to developers, research in designing smart city frameworks and architectures has presented its initiatives in line with reference frameworks such as the GDPR. For example, Badii. et al. (2020) have proposed an architecture called Snap4City for Smart City, whose security solutions are based on GDPR guidelines. This architecture is designed based on many security requirements related to the protection of data and user privacy in smart cities [58]. Makhdoom. et al. (2020) have also developed a blockchain-based framework (called PrivySharing) for privacy preservation and secure data sharing in the smart city, the proposed solution of which meets some of the important requirements of the GDPR. Their proposed strategy in this framework ensures that the user's data is kept confidential and processed securely and that this data is provided to stakeholders on a context basis [53]. The meta-synthesis output indicates that further research has referred to the GDPR as a reference standard and framework for data protection and user privacy. Policy-makers and stakeholders must develop reference frameworks for implementing smart city initiatives in conjunction with reference policies and regulations like GDPR to avoid future risks. The importance of these policies is increased due to the intelligent behavior of services, the use of emerging technologies such as IoT, and, most importantly, the produced open data. Lupi (2019) has proposed a scheme called (CDP) for city data that serves as a tool for data governance and their use for development purposes. This plan focuses on privacy and data manipulation in the smart city. The critical point of this plan is that it is a framework that can connect different stakeholders in terms of regulatory, legal, and incentive aspects of city data, which are based on a set of CDP implementation mechanisms [56]. As mentioned in the previous subsections, transparency in the design and implementation of smart city initiatives, especially data management and how to protect users' privacy, is essential. Defining this transparency requires setting standards that independent institutions should develop with the participation of all stakeholders. On the other hand, reference standards can publicly announce and formulate the requirements of this transparency [29]. To clarify this transparency and ensure users' private data confidentiality, the government and the corporate sectors can work together against possible misuse. Meanwhile, governments must enforce strict regulations to punish privacy violators, regardless of who they are [57].

### *2.7. Security requirements*

Smart city services, systems, plans, and architectures are required to comply with security features and requirements so that the security of infrastructure and privacy of data and users are not exposed to potential threats. The most basic security requirements to be included in smart city plans and initiatives are the requirements of confidentiality, integrity, and availability (CIA). The output of the meta-synthesis approach shows that authentication, access control, data confidentiality, user privacy, and resistance to attacks have received the most research attention. In addition, there are other requirements such as anonymity, public and private keys, auditing, accountability, and non-traceability. Security requirements must be considered by equipment manufacturers, service providers, and application developers and incorporated into their services and applications. Some of these requirements, such as authentication, access control, and public and private keys, have a technical aspect, and others, such as auditing, accountability, responsibility, and liability, have a non-technical aspect. A clear example of the security requirements that smart city stakeholders must adhere to is the requirements listed in the Information Security Management System (ISMS) standard and ISO version 27001. In addition to maintaining the security of services, security requirements play an essential role in protecting users' privacy. When designing applications and services, it is necessary to understand what security requirements are required according to the specific context and needs of the system. For example, consider secure data sharing, where requirements such as authentication, authorization, access control, data confidentiality, integrity, non-repudiation, and anonymity may be required to share data or even affect user privacy in data sharing [53], [79]. Violation of any of these requirements or disregarding them can harm user privacy. Studies also that have presented various initiatives for the smart city have proposed specific requirements to review and evaluate the security of these initiatives. Developers need to comply with the essential and general requirements for maintaining the safety and privacy of their users to achieve the optimal level of safety. Identifying and examining smart city security requirements requires research that does not fit into the scope of this study. For example, in a study, Kalloniatis. et al. (2019) have listed the significant features that affect the privacy of data and the user, which includes 17 concepts [31]. Besides identifying these requirements, evaluating them can positively affect smart city initiatives and their stakeholders.

## 3. Research Methodology

This article examines the dimensions of privacy affecting smart city users, as mentioned in Section 2. In the initial phase of the research, these dimensions were extracted through a meta-synthesis approach. Table 2 of the second section lists these dimensions. For the second phase, which aimed to determine the cause-and-effect relationships between dimensions and prioritization the importance of each of them, the fuzzy DEMATEL approach has been used. For this purpose, this section examines the steps of the fuzzy DEMATEL method.

### *3.1. Fuzzy sets*

In the real world, the goals and limitations of decision-making are not precisely known [92]; Sometimes, human judgments in decision-making are not entirely accurate and are faced with ambiguity [93]. These judgments are expressed in linguistic terms "low," "medium," "high," etc., and this unreliability and uncertainty in decision-making are related to the environment [94]. The theory of fuzzy number sets, introduced by L. A. Zadeh in 1965, can effectively counter ambiguities about linguistic thoughts and terms (human judgments) expressed as linguistic variables when making decisions. When information is incomplete or ambiguous, it determines its effectiveness in decision-making [95]. Fuzzy numbers can be used to transform these linguistic terms into decision-making, meaning that these numbers represent the linguistic variables of experts in decision-making. Unlike definite sets, fuzzy sets use the rate or "degree of membership" for the membership of an element to the set [96], [97]. For any element such as X in the crisp set of A, it can be represented by the following membership function (1):

$$\mu_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases} \qquad (1)$$

Whereas in a fuzzy set, the membership of each element in the set can be expressed as follows:

$\mu_A(x) \in [0\ \text{و}\ 1]$ , In other words, the membership of any element, such as $x$ in the set of $A$ , can have some value between zero and one, Where $\mu_A(x)=1$ indicates $x$ belongs to $A$ , and while $\mu_A(x)=1$ indicates that $x$ does not belong to the fuzzy set of $A$ , and this is the main step in modeling uncertainty. On the other hand, fuzzy numbers are generalizations of crisp numbers. Triangular and trapezoidal fuzzy numbers are the most common ones [96], [97]. $F=(l,m,u)$ represents the triangular fuzzy number, as shown in Figure 3 [93], Where $l$ is the number or lower bound, $m$ is the number mode and, $u$ is the number or upper bound. The membership function of a triangular fuzzy number can be defined as follows (2) [93], [96], [98].

$$\tilde{M}(x) = \begin{cases} 0, & x < l, \\ (x-l)/(m-l), & l \le x \le m, \\ (u-x)/(u-m), & m \le x \le u, \\ 0, & x > u, \end{cases} \qquad (2)$$

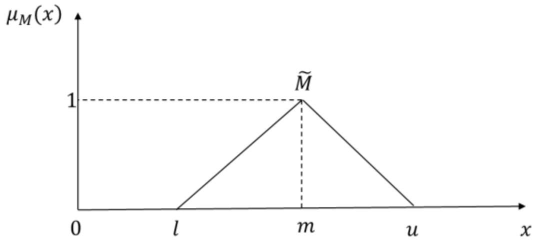

Fig 3. Show triangular fuzzy number [93]

For two triangular fuzzy numbers $\tilde{A}_1=(l_1,m_1,u_1)$ and $\tilde{A}_2=(l_2,m_2,u_2)$, the arithmetic operators can be defined as follows [93], [96], [99]:

1- Sum of triangular fuzzy numbers: $\tilde{A}_1+\tilde{A}_2=(l_1+l_2,m_1+m_2,u_1+u_2)$

2- Subtraction of triangular fuzzy numbers: $\tilde{A}_1-\tilde{A}_2=(l_1-u_2,m_1-m_2,u_1-l_2)$

3- Multiply of triangular fuzzy numbers: $\tilde{A}_1\times\tilde{A}_2=(l_1\times l_2,m_1\times m_2,u_1\times u_2)$

4- Division of triangular fuzzy numbers: $A_1 / \tilde{A}_2 = \left(l_1 / l_2, m_1 / m_2, u_1 / u_2\right)$

### *3.2. DEMATEL Technique*

DEMATEL's method (Decision Making Trial and Evaluation Laboratory) was introduced at the Geneva Research Center between 1972 to 1976 to discuss complex and comprehensive decision-making issues by Gabus and Fontella [93], [97]. The DEMATEL method is formed based on matrix theory and graph theory (Digraph) [100], Which can evaluate cause-and-effect relationships between variables or criteria [94]. This method is a practical and effective tool for visualizing complex causal relationships. By establishing an understandable structural model of the system, the method identifies the relationships between the criteria and expresses the influence and severity of each variable [96], [100].

The Fuzzy DEMATEL method uses fuzzy linguistic variables and analyzes the cause-and-effect relationships between variables facilitating decision-making under environmental uncertainty [94], [99]. Namely, the experts determine the severity of the impact and importance of each of the variables with verbal expressions. To avoid ambiguity, these expressions are converted to fuzzy numbers such as, fuzzy triangular numbers [96], [97], [100]. The Fuzzy DEMATEL method has been used in management and collaboration in the supply chain, tracking, energy supply, supplier selection, operation, learning management system, and other research areas [93], [94], [96]–[100]. This research uses triangular (or triple) fuzzy numbers to determine the distance based on the given values (converting qualitative expressions to fuzzy numbers) by experts' opinions.

The steps of the fuzzy DEMATEL method are as follows [93]–[105]:

The first stage, **group formation:** At this stage, consult with experts with sufficient knowledge and experience about the issue.

The second stage is determining the criteria to be evaluated and the design of linguistic scales: The research or problem's dimensions and indicators are defined in this stage. The experts are asked to compare pairs of criteria based on their impact on each other, using a square matrix to measure the relationships between the criteria. Experts every home of this matrix fill using qualitative terms (linguistic) and based on pairwise comparisons. This matrix is called the "Initial Direct-Relation Matrix." After completing the matrices, verbal expressions must be converted to fuzzy numbers. The following Table 4 lists the fuzzy equivalent of the variables used in the experts' language:

Table 4. The Linguistic Terms and their fuzzy equivalents in the research [96], [100]

| Linguistic Terms | Crisp equivalent/ Influence score | Triangular Fuzzy Numbers |
|---|---|---|
| No Influence (NO) | 0 | (0.0, 0.1, 0.3) |
| Very Low Influence (VL) | 1 | (0.1, 0.3, 0.5) |
| Low Influence (L) | 2 | (0.3, 0.5, 0.7) |
| High Influence (H) | 3 | (0.5, 0.7, 0.9) |
| Very High Influence (VH) | 4 | (0.7, 0.9, 1.0) |

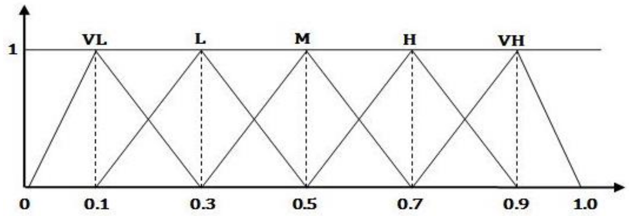

Fig 4. Triangular fuzzy number diagram for the selected verbal expressions in Table 4

The second step in this stage is to calculate the average matrix of experts' opinions in accordance with the following relation (3):

$$\tilde{z} = \frac{\tilde{x}^1 + \tilde{x}^2 + \tilde{x}^3 + \ldots + \tilde{x}^p}{p} \qquad (3)$$

In this regard, $p$ is the number of experts, and $\tilde{x}^1$, $\tilde{x}^2$, and $\tilde{x}^p$ are the paired scale 1 to $p$, respectively, and $\tilde{z}$ is the triangular fuzzy number in the form of $\tilde{z}_{ij} = (l_{ij}, m_{ij}, u_{ij})$.

The third stage, **normalization of the Direct-Relations Matrix**: With possession "Initial Direct-Relation Matrix," the matrix of " normalized direct-relation fuzzy" is made. At this stage, the table of averages of the resulting opinions is normalized to make its scale comparable and standard. The following relations (4,5) are used to normalize:

$$\tilde{a}_{ij} = \sum_{j=1}^{n} \tilde{z}_{ij} = \left( \sum_{j=1}^{n} l_{ij}, \sum_{j=1}^{n} m_{ij}, \sum_{j=1}^{n} u_{ij} \right), \quad u = \max_{1 \le i \le n} \left( \sum_{j=1}^{n} u_{ij} \right) \qquad (4)$$

$$\tilde{x} = \begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \cdots & \tilde{x}_{1j} \\ \tilde{x}_{21} & \tilde{x}_{22} & \cdots & \tilde{x}_{2j} \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ \tilde{x}_{i1} & \tilde{x}_{i2} & \cdots & \tilde{x}_{ij} \end{bmatrix}, \quad \tilde{x}_{ij} = \frac{\tilde{Z}_{ij}}{u} = \left( \frac{l_{ij}}{u}, \frac{m_{ij}}{u}, \frac{u_{ij}}{u} \right) \qquad (5)$$

Here $i$ is the row number, and $j$, the column number, for example, $\tilde{x}_{12}$ represents the degree of impact that the dimension of 1 has on the dimension of 2. And the relation $\tilde{x}_{ij}$ is used to calculate the matrix of average $\tilde{x}$.

The fourth stage is **calculating the total-relation fuzzy matrix**: In this stage, by first calculating the inverse of the normalized matrix, then subtracting it from the identity matrix (unit), and finally multiplying the norm matrix in the resulting matrix. To do this, it first needs to compute the fuzzy matrix of total relations through relation

$\tilde{\mathrm{T}} = \lim_{n\to\infty}(x + x^2 + ... + x^n)$ and then obtain each fuzzy number element that is $\tilde{t}_{ij} = (l_{ij}^{''}, m_{ij}^{''}, u_{ij}^{''})$ from the relations (6) and (7):

$$\tilde{\mathrm{T}} = \begin{bmatrix} \tilde{t}_{11} & \dots & \tilde{t}_{1n} \\ . & . & . \\ . & . & . \\ . & . & . \\ \tilde{t}_{n1} & \dots & \tilde{t}_{nn} \end{bmatrix} \qquad (6)$$

$$\left[l_{ij}''\right] = x_l \times \left(I - x_l\right)^{-1} \quad , \quad \left[m_{ij}''\right] = x_m \times \left(I - x_m\right)^{-1} \quad \text{and}$$
$$\left[u_{ij}''\right] = x_r \times \left(I - x_u\right)^{-1} \qquad (7)$$

I is the unit matrix in these relationships, and $x_l$, $x_m$, and $x_u$ are each matrix $n \times n$ ; Its elements form the lower, middle, and upper numbers of the fuzzy numbers of the triangular matrix $x$ , respectively.

The fifth stage is **creating and analyzing a causal diagram**: The first step is to calculate the sum of elements of each row $(D_i)$ and each column $(R_i)$ matrix of $\mathrm{T}$. In order to draw a causal diagram, these two values must be stated in the form of a crisp. For this reason, the "Mean value" method is used to "defuzzification" these two values. Use the following relation (8) to defuzzification the values to get a crisp value:

$$B = \frac{l + u + 2m}{4} \qquad (8)$$

The next step is to use the following relations (9) for the sum row and column:

$$\tilde{D} = \left(\tilde{D}_i\right)_{n\times 1} = \left[\sum_{j=1}^{n} \tilde{\mathrm{T}}_{ij}\right]_{n\times 1} \quad \text{and} \quad \tilde{R} = \left(\tilde{R}_i\right)_{1\times n} = \left[\sum_{j=1}^{n} \tilde{\mathrm{T}}_{ij}\right]_{1\times n} \qquad (9)$$

Where $\tilde{D}$ and $\tilde{R}$ are matrices $n \times 1$ and $1 \times n$, respectively. The Importance of the criteria (dimensions) $(\tilde{D}_i + \tilde{R}_i)$ and the relationship between the criteria $(\tilde{D}_i - \tilde{R}_i)$ are determined in the next step. If $\tilde{D}_i - \tilde{R}_i > 0$ is, the relevant criterion is "effective," and if $\tilde{D}_i - \tilde{R}_i < 0$ is, the relevant criterion is " Impressive." The next step $\tilde{D}_i + \tilde{R}_i$ and $\tilde{D}_i - \tilde{R}_i$ from the previous step, should show the relationships between the criteria. After the defuzzification of the numbers, a Cartesian coordinate system is plotted. In this system, the longitudinal axis represents the values of $\tilde{D}_i + \tilde{R}_i$ and the transverse axis of the values of $\tilde{D}_i - \tilde{R}_i$ . Therefore, the horizontal vector in the coordinate system is the amount of impact of the factor or dimension desired in the system; in other words, whatever this amount is greater for one factor, it interacts more with other system factors. The vertical vector of the coordinate system shows the power of influence of each factor. If this value is positive for a factor, the variable is causal; if negative, the variable is considered an effect.

## 4. Validation and implication

This section evaluates the validation of the presented method and finally expresses the results of this evaluation. The evaluation of the relationships between the dimensions based on the order of the steps of the fuzzy DEMATEL method is expressed in output tables, which are given in sub-section (4.1). Then sub-section (4.2) analyzes and examines the findings of this evaluation.

### *4.1. Validation*

According to the first and second stages of the Fuzzy DEMATEL method, seven university experts in the field of IoT and security were given a questionnaire. They were asked to identify the relations and importance between the dimensions in Table 2. After collecting the questionnaires, the linguistic terms were modeled in the form of fuzzy numbers using the relations mentioned in Table 2; thus, the initial direct-relation matrix was obtained. Table 5 shows the average matrix for experts' opinions.

Table 5. average matrix for experts' opinions

| | **D1** | **D2** | **D3** | **D4** | **D5** | **D6** | **D7** |
|---|---|---|---|---|---|---|---|
| **D1** | (0, 0, 0) | (0/61, 0/81, 0/94) | (0/33, 0/53, 0/70) | (0/47, 0/67, 0/84) | (0/44, 0/64, 0/81) | (0/39, 0/59, 0/76) | (0/39, 0/59, 0/76) |
| **D2** | (0/44, 0/64, 0/81) | (0, 0, 0) | (0/41, 0/61, 0/81) | (0/53, 0/73, 0/89) | (0/39, 0/59, 0/79) | (0/33, 0/53, 0/73) | (0/36, 0/56, 0/76) |
| **D3** | (0/26, 0/44, 0/63) | (0/33, 0/53, 0/71) | (0, 0, 0) | (0/44, 0/64, 0/81) | (0/33, 0/53, 0/73) | (0/27, 0/47, 0/67) | (0/33, 0/53, 0/73) |
| **D4** | 0/31, 0/50, 0/70) | (0/36, 0/56, 0/74) | (0/30, 0/50, 0/7) | (0, 0, 0) | (0/21, 0/41, 0/61) | (0/33, 0/53, 0/71) | (0/36, 0/56, 0/76) |
| **D5** | (0/37, 0/56, 0/73) | (0/39, 0/59, 0/79) | (0/33, 0/53, 0/73) | (0/39, 0/59, 0/79) | (0, 0, 0) | (0/34, 0/53, 0/71) | (0/36, 0/56, 0/74) |
| **D6** | (0/41, 0/61, 0/79) | (0/36, 0/56, 0/74) | (0/39, 0/59, 0/79) | (0/44, 0/64, 0/84) | (0/50, 0/70, 0/87) | (0, 0, 0) | (0/39, 0/59, 0/79) |
| **D7** | (0/41, 0/61, 0/79) | (0/47 0/67, 0/84) | (0/41, 0/61, 0/79) | (0/53, 0/73, 0/9) | (0/47, 0/67, 0/84) | (0/41, 0/61, 0/79) | (0, 0, 0) |

After calculating the above matrix, according to relations (4) and (5), the initial direct-relations matrix can be normalized, which is shown in Table 6.

Table 6. Normalized direct-relation matrix for Experts' opinions

| | **D1** | **D2** | **D3** | **D4** | **D5** | **D6** | **D7** |
|---|---|---|---|---|---|---|---|
| **D1** | (0, 0, 0) | (0/12, 0/16, 0/19) | (0/07, 0/11, 0/14) | (0/1, 0/14, 0/17) | (0/09, 0/13, 0/16) | (0/08, 0/12, 0/15) | (0/08, 0/12, 0/15) |
| **D2** | (0/09, 0/13, 0/16) | (0, 0, 0) | (0/08, 0/12, 0/16) | (0/11, 0/15, 0/18) | (0/08, 0/12, 0/16) | (0/07, 0/11, 0/15) | (0/07, 0/11, 0/15) |
| **D3** | (0/05, 0/09, 0/13) | (0/07, 0/11, 0/14) | (0, 0, 0) | (0/09, 0/13, 0/16) | (0/07, 0/11, 0/15) | (0/05, 0/1, 0/14) | (0/07, 0/11, 0/15) |
| **D4** | (0/06, 0/10, 0/14) | (0/07, 0/11, 0/15) | (0/06, 0/1, 0/14) | (0, 0, 0) | (0/04, 0/08, 0/12) | (0/07, 0/11, 0/14) | (0/07, 0/11, 0/15) |
| **D5** | (0/08, 0/11, 0/15) | (0/08, 0/12, 0/16) | (0/07, 0/11, 0/15) | (0/08, 0/12, 0/16) | (0, 0, 0) | (0/07, 0/11, 0/14) | (0/07, 0/11, 0/15) |
| **D6** | (0/08, 0/12, 0/16) | (0/07, 0/11, 0/15) | (0/08, 0/12, 0/16) | (0/09, 0/13, 0/17) | (0/1, 0/14, 0/18) | (0, 0, 0) | (0/08, 0/12, 0/16) |
| **D7** | (0/08, 0/12, 0/16) | (0/1, 0/14, 0/17) | (0/08, 0/12, 0/16) | (0/11, 0/15, 0/18) | (0/1, 0/14, 0/17) | (0/08, 0/12, 0/16) | (0, 0, 0) |

According to relations (6) and (7), the Fuzzy total-relation matrix $(\mathrm{T})$ is calculated, which its results are shown in Table 7.

Table 7. Fuzzy total-relations matrix

| | D1 | D2 | D3 | D4 | D5 | D6 | D7 |
|---|---|---|---|---|---|---|---|
| **D1** | (0/07, 0/27, -0/59) | (0/19, 0/44, -0/47) | (0/13, 0/37, -0/48) | (0/17, 0/44, -0/52) | (0/15, 0/4, -0/48) | (0/14, 0/37, -0/46) | (0/14, 0/38, -1/5) |
| **D2** | (0/15, 0/37, -0/45) | (0/07, 0/28, -0/63) | (0/14, 0/37, -0/46) | (0/18, 0/43, -0/51) | (0/14, 0/37, -0/48) | (0/12, 0/35, -0/46) | (0/13, 0/36, -1/49) |
| **D3** | (0/1, 0/31, -0/43) | (0/12, 0/34, -0/45) | (0/05, 0/23, -0/55) | (0/15, 0/38, -0/47) | (0/12, 0/33, -0/44) | (0/1, 0/31, -0/42) | (0/11, 0/32, -1/36) |
| **D4** | (0/11, 0/31, -0/42) | (0/12, 0/34, -0/45) | (0/11, 0/31, -0/43) | (0/06, 0/26, -0/61) | (0/1, 0/31, -0/46) | (0/11, 0/31, -0/42) | (0/12, 0/32, -1/35) |
| **D5** | (0/13, 0/34, -0/44) | (0/14, 0/37, -0/46) | (0/12, 0/34, -0/44) | (0/14, 0/38, -0/5) | (0/06, 0/25, -0/59) | (0/12, 0/33, -0/43) | (0/12, 0/34, -1/42) |
| **D6** | (0/14, 0/37, -0/46) | (0/14, 0/39, -0/51) | (0/14, 0/37, -0/47) | (0/16, 0/42, -0/53) | (0/16, 0/4, -0/48) | (0/06, 0/25, -0/59) | (0/14, 0/37, -1/5) |
| **D7** | (0/15, 0/39, -0/31) | (0/17, 0/42, -0/33) | (0/15, 0/39, -0/31) | (0/18, 0/45, -0/34) | (0/16, 0/41, -0/32) | (0/14, 0/38, -0/3) | (0/07, 0/28, -1/44) |

According to the fifth step and the relation (8), the above matrix is defuzzification. Then the sum of elements of each row $(D_i)$ and each column $(R_i)$ are calculated according to the relation (9). Table 6 indicates these results.

Table 6. Defuzzification Matrix and sum of its rows and columns

| DF | D1 | D2 | D3 | D4 | D5 | D6 | D7 | D |
|---|---|---|---|---|---|---|---|---|
| **D1** | 0/00 | 0/15 | 0/10 | 0/13 | 0/12 | 0/10 | -0/15 | 0/45 |
| **D2** | 0/11 | 0/00 | 0/11 | 0/13 | 0/10 | 0/09 | -0/16 | 0/38 |
| **D3** | 0/07 | 0/09 | -0/01 | 0/11 | 0/08 | 0/07 | -0/15 | 0/26 |
| **D4** | 0/08 | 0/09 | 0/08 | -0/01 | 0/06 | 0/08 | -0/15 | 0/23 |
| **D5** | 0/09 | 0/10 | 0/09 | 0/10 | -0/01 | 0/09 | -0/15 | 0/31 |
| **D6** | 0/11 | 0/10 | 0/10 | 0/12 | 0/12 | -0/01 | -0/16 | 0/38 |
| **D7** | 0/15 | 0/17 | 0/15 | 0/19 | 0/16 | 0/15 | -0/20 | 0/77 |
| **R** | 0/62 | 0/70 | 0/61 | 0/77 | 0/64 | 0/57 | -1/13 | |

Finally, according to Table 5, the importance of dimensions $(\tilde{D}_i + \tilde{R}_i)$ and the relation between dimensions $(\tilde{D}_i - \tilde{R}_i)$ are specified. Now, the degree of the cause and effect of the dimensions should be determined. As stated, if $(\tilde{D}_i - \tilde{R}_i)$ is positive, that dimension will be the cause, and if is negative, it will be the effect. Table 9 demonstrates these results.

Table 9. The amount of importance and relation between dimensions (cause and effect)

| Dimension | D+R | D-R | Cause/Effect |
|---|---|---|---|
| **D1** | 1/07 | -0.17 | Cause |
| **D2** | 1.08 | -0.32 | Cause |
| **D3** | 0.86 | -0.35 | Cause |
| **D4** | 1.00 | -0.54 | Cause |
| **D5** | 0.95 | -0.33 | Cause |

| | | | |
|---|---|---|---|
| **D6** | 0.96 | -0.19 | Cause |
| **D7** | -0.36 | 1.90 | Effect |

Figure 5 shows the level of importance and cause-effect between dimensions. The horizontal axis indicates the importance of dimensions, and the vertical axis shows their cause and effect.

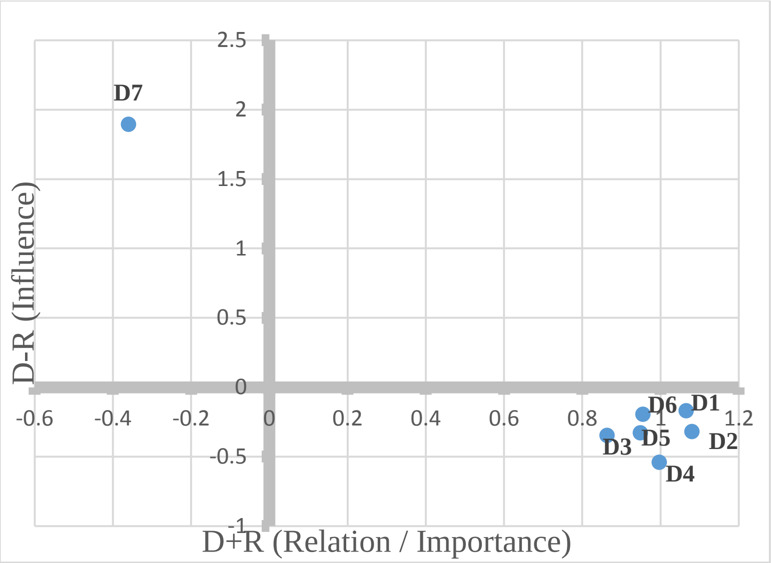

Fig 5. The diagram of importance (D + R) and amount of cause and effect (D-R) of the dimensions affecting the protection of user privacy in the smart city

### *4.2. Implication of findings*

According to the above points in Figure (5), the dimensions above and below the horizontal axis constitute the cause and effect dimensions, respectively. The higher dimension indicates a greater degree of cause, and the lower dimension suggests a greater degree of effect. Among the cause and effect dimensions, the value of $(\tilde{D}_i + \tilde{R}_i)$ indicates the intensity of interaction of each dimension with other dimensions. In this way, in the group of the cause dimensions, the higher the value of $(\tilde{D}_i + \tilde{R}_i)$, that dimension is more important and is placed as a higher priority. Also, among the effect dimensions, the lower the value of $(\tilde{D}_i + \tilde{R}_i)$, the dimension is more important and is placed as a higher priority. As can be seen, "security requirements (D7)" is the only cause dimension, and "awareness and understand (D1)," " data management (D6)," "trust (D2)," "frameworks and standards (D5)," "personalization and self-controlling (D3)," and "transparency (D4)" are identified as effect dimensions. In Figure 1, among the effect dimensions, as it appears, all these dimensions are close to each other. It is impossible to distinguish between these dimensions when it comes to the most effective. However, according to the results, it can be said that "transparency" is the most effective among the dimensions. Finally, the degree of influence of the dimension affecting the user's privacy in the smart city can be ranked in order, which are "security requirements," "awareness and understanding," "data management," "trust," "reference standards, frameworks and rules," "self-controlling and personality," and "transparency." On the one hand, "security requirements," which is the only dimension in the cause category, is also known as the most important dimension of this category. On the other hand, among the effect dimensions, as can be seen, they are all close to each other in terms of importance, but "personalization and self-controlling" is the most important dimension. Table 10 outlines the importance and priority of the cause-and-effect dimensions.

Table 10. Ordering the importance and priority of dimensions affecting user privacy in the smart city in two categories of cause and effect

| Cause / Effect | Dimensions |
|---|---|
| **Cause** | Security Requirements |
| **Effect** | 1. Self-Controlling and Personalization, 2. Reference Standards, Frameworks and Rules, 3. Data Management, 4. Transparency, 5. Awareness and Understanding, 6. Trust |

## 5. Conclusions and Suggestions

Smart cities have provided various initiatives and benefits for users in an age of digital technologies and can be considered one of the innovative concepts in this evolution. Users must become practically involved to take advantage of these initiatives and benefits. A vast amount of data and information about them is continually collected, processed, stored, and used here. One issue affecting the acceptance and use of smart city initiatives is protecting the security and privacy of users and their data. In this regard, to address these concerns, steps should be taken to implement smart city initiatives. One of these measures is to identify and evaluate the factors and criteria that affect the protection of user privacy in the smart city. This study has taken two steps to identify and evaluate these factors. In the first step, a meta-synthesis method was used to identify factors affecting privacy, leading to the extraction of seven dimensions, including “awareness and understanding,” “trust,” “self-controlling and personalization,” “transparency, reference standards, frameworks, and rules,” and “security requirements.” In the second step, the fuzzy DEMATEL model is used to evaluate the importance and effectiveness of these dimensions and examine the seventh step of the meta-synthesis approach (i.e., the control and presentation step). The DEMATEL 's approach is chosen to examine the cause-and-effect relations between dimensions from the experts' point of view since their opinions are always uncertain, and they express them more in terms of verbal expressions such as "high" and "average." Therefore, the DEMATEL method is evaluated with the help of a fuzzy set known as the fuzzy DEMATEL approach. In this step, smart city experts were provided with the extraction dimensions and asked to determine their importance and relationships. Fuzzy DEMATEL was used to analyze the results of questionnaires by converting verbal expressions into fuzzy numbers using fuzzy sets. The results of the analysis show that there is a causal relationship between the dimensions. It means that the factors affecting users' privacy in a smart city fall into two categories: cause and effect.  As well the importance of each dimension was outlined in each category. By considering users' privacy, it would be possible to improve user privacy by determining what dimensions are the cause, what dimensions are the effect, and what the relationships among them are. According to the results, it was observed that "security requirements" is the most cause, and "transparency" is the most effective dimension among the factors affecting the users' privacy in the smart city. In addition, the "security requirements" was recognized as the only cause dimension that affects all other dimensions. In terms of importance, this is the most important dimension in the cause dimensions' category. All effect dimensions are closely related, but from the perspective of importance, "personalization and self-controlling" gained the most, and "trust" gained the least importance.

As a result, this research highlights what smart city developers and stakeholders will need to consider and what steps they will need to take to protect privacy. By doing so, stakeholders and developers of the smart city should pay more attention to which factors may affect users' privacy in the smart city. The "security requirements" play an important role in protecting users' privacy. This factor shows its effects in both technical and non-technical aspects. The technical aspects of communicating securely between entities, data transfer, and data management require security requirements such as authentication, access control, confidentiality, anonymity, non-repudiation, integrity, and other requirements that revolve around the CIA's three core security requirements. Nontechnical requirements like auditing, accountability, and responsibility can also be highly effective in maintaining security and privacy. As confirmed by the analysis of this study, establishing these requirements and adhering to the programs and initiatives, developers make available to them can play a significant role in maintaining user privacy in other respects. The identification and evaluation of these requirements will assist in developing laws, standards, and reference frameworks for security and privacy, which will guide policy-makers and stakeholders of the smart city in establishing these requirements in services and initiatives. Reference standards such as ISMS and ISO versions can be used to identify and evaluate security requirements. Research outputs can also be a promising method for identifying and evaluating these requirements. Even a security requirements reference framework can determine which requirements need to be more focused on by stakeholders to manage data in any process, such as acquisition, transfer, storage, sharing, and use. In order to identify these requirements for data management, reference frameworks and standards such as the GDPR (for data confidentiality and privacy) is also an important factor for proper data control and management. The standards explain and clarify the responsibility and accountability of smart city stakeholders regarding users' privacy.

Various initiatives and services are created in the smart city, each with its own requirements. Before these initiatives are implemented, security requirements and standards, and user privacy frameworks must be identified and informed to citizens and users. As Habib. et al. (2020) showed in their research, that the security and privacy perceived by the user can gain their trust and make their acceptance understandable to the user [30]. Besides this awareness, assurance by the developers of smart city initiatives to protect users' privacy and provide full transparency will be essential. Among the dimensions affecting user privacy in terms of importance, as the results of the analysis show, it is suggested that the establishment and evaluation of security requirements be considered by developers first. Among the effective dimensions, as it turned out, it is better to embed personalization and self-controlling mechanisms in smart city initiatives and services to strengthen users' privacy so that users can decide on their sensitive data. These mechanisms can include delegating authority to share specific data, third-party access to the data, the option to "opt-out" of sending data, revoking the authorization of untrusted users, the amount and timing of data storage, and other mechanisms. However, it is essential to note that achieving this self-controlling mechanism requires developers to provide transparency and codify appropriate policies and standards. After granting this personalization to users, their awareness of properly managing their data and providing transparency throughout the system will gain users' trust. Finally, paying attention to these dimensions can be reflected in improving and enhancing user privacy.

This study examined only two scientific databases, Web of Science and Scopus, based on three main keywords to identify and extract the dimensions affecting the user's privacy. To extract more dimensions, researchers can search other scientific databases. Suggestions for future research are also provided, which include the following:

1 Using other MCDM approaches to evaluate these dimensions and their relationships.

2 Evaluate these dimensions from the perspective of users and citizens of the smart city and identify other dimensions that affect their privacy.

3 Design a recommendation system based on effective dimensions from the perspective of smart city users that can offer other users personalized suggestions on improving their privacy.

In the continuation of future research programs, the research team of this study is also investigating the second and third suggestions.

## References

[1] C. S. Lai *et al.*, “A Review of Technical Standards for Smart Cities,” *Clean Technol.*, vol. 2, no. 3, pp. 290–310, 2020.

[2] A. Kar, V. Ilavarasan, M. P. Gupta, M. Janssen, and R. Kothari, “Moving beyond Smart Cities: Digital Nations for Social Innovation & Sustainability,” *Inf. Syst. Front.*, vol. 21, 2019.

[3] L. Anthopoulos, M. Janssen, and V. Weerakkody, “A Unified Smart City Model (USCM) for Smart City Conceptualization and Benchmarking,” in *E-Planning and Collaboration: Concepts, Methodologies, Tools, and Applications*, 2018, pp. 523–540.

[4] M. Lom and O. Pribyl, “Smart city model based on systems theory,” *Int. J. Inf. Manage.*, vol. 56, p. 102092, 2021.

[5] S. Mamonov, M. Koufaris, and R. Benbunan-Fich, “The Role of the Sense of Community in the Sustainability of Social Network Sites,” *Int. J. Electron. Commer.*, vol. 20, pp. 470–498, 2016.

[6] H. F. Atlam and G. B. Wills, “IoT Security, Privacy, Safety and Ethics,” in *Digital Twin Technologies and Smart Cities*, M. Farsi, A. Daneshkhah, A. Hosseinian-Far, and H. Jahankhani, Eds. Cham: Springer International Publishing, 2020, pp. 123–149.

[7] H.-D. Evers, T. Menkhoff, K. Ning, and Y. W. Chay, *Living in Smart Cities. Innovation and Sustainability*. 2018.

[8] C. Nikoloudis *et al.*, “An Evaluation Model for Smart City Performance with Less Than 50,000 Inhabitants: A Greek Case Study,” 2020, pp. 15–21.

[9] G. Kou, S. Yüksel, and H. Dinçer, “Inventive problem-solving map of innovative carbon emission strategies for solar energy-based transportation investment projects,” *Appl. Energy*, vol. 311, p. 118680, 2022.

[10] T. Mecheva and N. Kakanakov, “Cybersecurity in Intelligent Transportation Systems,” *Computers*, vol. 9, no. 4, 2020.

[11] D. Eckhoff and I. Wagner, “Privacy in the Smart City – Applications, Technologies, Challenges and Solutions,” *IEEE Commun. Surv. Tutorials*, vol. PP, p. 1, 2017.

[12] P. Radoglou Grammatikis, P. Sarigiannidis, and I. Moscholios, “Securing the Internet of Things: Challenges, Threats and Solutions,” 2018.

[13] F. Ullah, S. Qayyum, M. J. Thaheem, F. Al-Turjman, and S. M. E. Sepasgozar, “Risk management in sustainable smart cities governance: A TOE framework,” *Technol. Forecast. Soc. Change*, vol. 167, 2021.

[14] C. Wiencierz and M. Luenich, “Trust in open data applications through transparency,” *NEW MEDIA Soc.*

[15] R. Vasileva, L. Rodrigues, N. Hughes, C. Greenhalgh, M. Goulden, and J. Tennison, “What Smart Campuses Can Teach Us about Smart Cities: User Experiences and Open Data,” *INFORMATION*, vol. 9, no. 10, 2018.

[16] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, “Privacy-Preserving Solutions for Blockchain: Review and Challenges,” *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[17] M. Anisetti, C. Ardagna, V. Bellandi, M. Cremonini, F. Frati, and E. Damiani, “Privacy-aware Big Data Analytics as a service for public health policies in smart cities,” *Sustain. Cities Soc.*, vol. 39, pp. 68–77, 2018.

[18] D. Eckhoff and I. Wagner, “Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 489–516, 2018.

[19] J. L. Hernandez-Ramos *et al.*, “Security and privacy in internet of things-enabled smart cities: Challenges and future directions,” *IEEE Secur. Priv.*, vol. 19, no. 1, pp. 12–23, 2021.

[20] M. D. Lytras and A. Visvizi, “Who Uses Smart City Services and What to Make of It: Toward Interdisciplinary Smart Cities Research,” *SUSTAINABILITY*, vol. 10, no. 6, 2018.

[21] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, “Preserving privacy in internet of things: a survey,” *Int. J. Inf. Technol.*, vol. 10, no. 2, pp. 189–200, 2018.

[22] R. Khatoun and S. Zeadally, “Cybersecurity and privacy solutions in smart cities,” *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 51–59, 2017.

[23] M. A. Javed, E. B. Hamida, and W. Znaidi, “Security in intelligent transport systems for smart cities: From theory to practice,” *Sensors (Switzerland)*, vol. 16, no. 6, 2016.

[24] Y. Li, W. Dai, Z. Ming, and M. Qiu, “Privacy Protection for Preventing Data Over-Collection in Smart City,” *IEEE Trans. Comput.*, vol. 65, no. 5, pp. 1339–1350, 2016.

[25] T. E. Julsrud and J. R. Krogstad, “Is there enough trust for the smart city? exploring acceptance for use of mobile phone data in oslo and tallinn,” *Technol. Forecast. Soc. Change*, vol. 161, 2020.

[26] A. M. Hassan and A. I. Awad, “Urban Transition in the Era of the Internet of Things: Social Implications and Privacy Challenges,” *IEEE Access*, vol. 6, pp. 36428–36440, 2018.

[27] V. Butot, P. S. Bayerl, G. Jacobs, and F. de Haan, “Citizen repertoires of smart urban safety: Perspectives from Rotterdam, the Netherlands,” *Technol. Forecast. Soc. Change*, vol. 158, 2020.

[28] J. (Jove) Hou, L. Arpan, Y. Wu, R. Feiock, E. Ozguven, and R. Arghandeh, “The Road toward Smart Cities: A Study of Citizens’ Acceptance of Mobile Applications for City Services,” *ENERGIES*, vol. 13, no. 10, 2020.

[29] H. Elahi, G. Wang, T. Peng, and J. Chen, “On Transparency and Accountability of Smart Assistants in Smart Cities,” *Appl. Sci.*, vol. 9, no. 24, 2019.

[30] A. Habib, D. Alsmadi, and V. R. Prybutok, “Factors that determine residents’ acceptance of smart city technologies,” *Behav. Inf. Technol.*, vol. 39, no. 6, SI, pp. 610–623, 2020.

[31] C. Kalloniatis, D. Kavroudakis, A. Polidoropoulou, and S. Gritzalis, “Designing Privacy-Aware Intelligent Transport Systems: A Roadmap for Identifying the Major Privacy Concepts,” *Int. J. Appl. GEOSPATIAL Res.*, vol. 10, no. 1, pp. 73–91, 2019.

[32] L. de Wijs, P. Witte, and S. Geertman, “How smart is smart? Theoretical and empirical considerations on implementing smart city objectives - a case study of Dutch railway station

areas," *Innov. Eur. J. Soc. Sci. Res.*, vol. 29, no. 4, pp. 424–441, 2016.

[33] D. Belanche, L. V Casalo-Arino, and A. Perez-Rueda, "Determinants of multi-service smartcard success for smart cities. development: A study based on citizens' privacy and security perceptions," *Gov. Inf. Q.*, vol. 32, no. 2, pp. 154–163, 2015.

[34] J. A. Sánchez Alcón, L. López, J.-F. Martínez, and G. R. Cifuentes, "Trust and privacy solutions based on holistic service requirements," *Sensors (Switzerland)*, vol. 16, no. 1, 2015.

[35] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning," *J. Syst. Archit.*, vol. 115, 2021.

[36] C. D. Cottrill, N. Jacobs, M. Markovic, and P. Edwards, "Sensing the City: Designing for Privacy and Trust in the Internet of Things," *Sustain. Cities Soc.*, vol. 63, 2020.

[37] S. Chatterjee, "The safety of IoT-enabled system in smart cities of India: do ethics matter?," *Int. J. Ethics Syst.*, vol. 36, no. 4, pp. 601–618, 2020.

[38] S. Chatterjee and A. K. Kar, "Effects of successful adoption of information technology enabled services in proposed smart cities of India: From user experience perspective," *J. Sci. Technol. POLICY Manag.*, vol. 9, no. 2, SI, pp. 189–209, 2018.

[39] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustain. Cities Soc.*, vol. 39, pp. 499–507, 2018.

[40] G. Alandjani, "Features and potential security challenges for IoT enabled devices in smart city environment," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 8, pp. 231–238, 2018.

[41] H. Yeh, "The effects of successful ICT-based smart city services: From citizens' perspectives," *Gov. Inf. Q.*, vol. 34, no. 3, pp. 556–565, 2017.

[42] V. Beltran, A. F. Skarmeta, and P. M. Ruiz, "An ARM-compliant architecture for user privacy in smart cities: SMARTIE-quality by design in the IoT," *Wirel. Commun. Mob. Comput.*, vol. 2017, 2017.

[43] Z. Khan, Z. Pervez, and A. G. Abbasi, "Towards a secure service provisioning framework in a Smart city environment," *Futur. Gener. Comput. Syst.*, vol. 77, pp. 112–135, 2017.

[44] A. Avgerou, P. E. Nastou, D. Nastouli, P. M. Pardalos, and Y. C. Stamatiou, "On the Deployment of Citizens' Privacy Preserving Collective Intelligent eBusiness Models in Smart Cities," *Int. J. Secur. ITS Appl.*, vol. 10, no. 2, pp. 171–184, 2016.

[45] S. Ahmed, "Security and privacy in smart cities: Challenges and opportunities," *Int. J. Eng. Trends Technol.*, vol. 68, no. 2, pp. 1–8, 2020.

[46] V. Moustaka, Z. Theodosiou, A. Vakali, A. Kounoudes, and L. G. Anthopoulos, "Enhancing social networking in smart cities: Privacy and security borderlines," *Technol. Forecast. Soc. Change*, vol. 142, pp. 285–300, 2019.

[47] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018.

[48] H. Elahi, A. Castiglione, G. Wang, and O. Geman, "A human-centered artificial intelligence approach for privacy protection of elderly App users in smart cities," *Neurocomputing*, vol. 444, pp. 189–202, 2021.

[49] A. A. Omar *et al.*, "A Transparent and Privacy-Preserving Healthcare Platform with Novel Smart Contract for Smart Cities," *IEEE Access*, vol. 9, pp. 90738–90749, 2021.

[50] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2019.

[51] J. A. Martinez, J. L. Hernandez-Ramos, V. Beltran, A. Skarmeta, and P. M. Ruiz, "A user-centric Internet of Things platform to empower users for managing security and privacy concerns in the Internet of Energy," *Int. J. Distrib. Sens. NETWORKS*, vol. 13, no. 8, 2017.

[52] J. D. Fernandez *et al.*, "User consent modeling for ensuring transparency and compliance in smart cities," *Pers. UBIQUITOUS Comput.*, vol. 24, no. 4, SI, pp. 465–486, 2020.

[53] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Comput. Secur.*, vol. 88, 2020.

[54] S. Daoudagh *et al.*, "Data protection by design in the context of smart cities: A consent and

access control proposal," *Sensors*, vol. 21, no. 21, 2021.

[55] S. K. Singh, Y.-S. Jeong, and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart City," *Sustain. Cities Soc.*, vol. 60, 2020.

[56] L. Lupi, "City Data Plan: The Conceptualisation of a Policy Instrument for Data Governance in Smart Cities," *URBAN Sci.*, vol. 3, no. 3, 2019.

[57] N. H. Abosaq, "Impact of Privacy Issues on Smart City Services in a Model Smart City," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 2, pp. 177–185, 2019.

[58] C. Badii, P. Bellini, A. Difino, and P. Nesi, "Smart City IoT Platform Respecting GDPR Privacy and Security Aspects," *IEEE ACCESS*, vol. 8, pp. 23601–23623, 2020.

[59] S. Bennati, I. Dusparic, R. Shinde, and C. M. Jonker, "Volunteers in the Smart City: Comparison of Contribution Strategies on Human-Centered Measures," *SENSORS*, vol. 18, no. 11, 2018.

[60] G. Shaffer, "applying a contextual integrity framework to privacy policies for smart technologies," *J. Inf. Policy*, vol. 11, pp. 222–265, 2021.

[61] S. Bannerman and A. Orasch, "Privacy and smart cities: A Canadian survey," *Can. J. Urban Res.*, vol. 29, no. 1, pp. 17–38, 2020.

[62] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, 2019.

[63] J. Curzon, A. Almehmadi, and K. El-Khatib, "A survey of privacy enhancing technologies for smart cities," *Pervasive Mob. Comput.*, vol. 55, pp. 76–95, 2019.

[64] F. Yang and J. Xu, "Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law," *Asia Pacific Policy Stud.*, vol. 5, no. 3, pp. 533–543, 2018.

[65] S. Chatterjee, A. K. Kar, and M. P. Gupta, "Alignment of IT Authority and Citizens of Proposed Smart Cities in India: System Security and Privacy Perspective," *Glob. J. Flex. Syst. Manag.*, vol. 19, no. 1, pp. 95–107, 2018.

[66] H. S. M. Lim and A. Taeihagh, "Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications," *Energies*, vol. 11, no. 5, 2018.

[67] L. van Zoonen, "Privacy concerns in smart cities," *Gov. Inf. Q.*, vol. 33, no. 3, pp. 472–480, 2016.

[68] Y. Seto, "Application of privacy impact assessment in the smart city," *Electron. Commun. Japan*, vol. 98, no. 2, pp. 1427–1435, 2015.

[69] A. Gharaibeh *et al.*, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2456–2501, 2017.

[70] L. Qi *et al.*, "Privacy-Aware Data Fusion and Prediction With Spatial-Temporal Context for Smart City Industrial Environment," *IEEE Trans. Ind. INFORMATICS*, vol. 17, no. 6, pp. 4159–4167, 2021.

[71] J. Chen, L. Ramanathan, and M. Alazab, "Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities," *Microprocess. Microsyst.*, vol. 81, 2021.

[72] Z. Guan *et al.*, "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, 2018.

[73] L. Fang, H. Zhang, M. Li, C. Ge, L. Liu, and Z. Liu, "A Secure and Fine-Grained Scheme for Data Security in Industrial IoT Platforms for Smart City," *IEEE INTERNET THINGS J.*, vol. 7, no. 9, pp. 7982–7990, 2020.

[74] F. Wu, X. Li, L. Xu, S. Kumari, D. Lin, and J. J. P. C. Rodrigues, "An anonymous and identity-trackable data transmission scheme for smart grid under smart city notion," *Ann. Telecommun.*, vol. 75, no. 7–8, SI, pp. 307–317, 2020.

[75] K. Chaturvedi, A. Matheus, S. H. Nguyen, and T. H. Kolbe, "Securing Spatial Data Infrastructures for Distributed Smart City applications and services," *Futur. Gener. Comput. Syst. Int. J. ESCIENCE*, vol. 101, pp. 723–736, 2019.

[76] C. Huang, R. Lu, X. Lin, and X. Shen, "Secure Automated Valet Parking: A Privacy-Preserving Reservation Scheme for Autonomous Vehicles," *IEEE Trans. Veh. Technol.*,

vol. 67, no. 11, pp. 11169–11180, 2018.

[77] M. Nikooghadam, H. Amintoosi, S. K. H. Islam, and M. F. Moghadam, “A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance,” *J. Syst. Archit.*, vol. 115, 2021.

[78] R. Zhou, X. Zhang, X. Wang, G. Yang, N. Guizani, and X. Du, “Efficient and Traceable Patient Health Data Search System for Hospital Management in Smart Cities,” *IEEE INTERNET THINGS J.*, vol. 8, no. 8, pp. 6425–6436, 2021.

[79] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, “Blockchain-empowered cloud architecture based on secret sharing for smart city,” *J. Inf. Secur. Appl.*, vol. 57, 2021.

[80] N. W. Hundera, C. Jin, M. U. Aftab, D. Mesfin, and S. Kumar, “Secure outsourced attribute-based signcryption for cloud-based Internet of Vehicles in a smart city,” *Ann. Telecommun.*, vol. 76, no. 9–10, SI, pp. 605–616, 2021.

[81] S. S. Alotaibi, “Registration Center Based User Authentication Scheme for Smart E-Governance Applications in Smart Cities,” *IEEE ACCESS*, vol. 7, pp. 5819–5833, 2019.

[82] A. Kumar, K. Abhishek, X. Liu, and A. Haldorai, “An Efficient Privacy-Preserving ID Centric Authentication in IoT Based Cloud Servers for Sustainable Smart Cities,” *Wirel. Pers. Commun.*, vol. 117, no. 4, pp. 3229–3253, 2021.

[83] A. S. Elmaghraby and M. M. Losavio, “Cyber security challenges in smart cities: Safety, security and privacy,” *J. Adv. Res.*, vol. 5, no. 4, pp. 491–497, 2014.

[84] N. B. Truong, T.-W. Um, and G. M. Lee, “A reputation and knowledge based trust service platform for trustworthy social internet of things,” *Innov. clouds, internet networks (ICIN), Paris, Fr.*, pp. 104–111, 2016.

[85] H. Zhang, M. Babar, M. U. Tariq, M. A. Jan, V. G. Menon, and X. Li, “SafeCity: Toward safe and secured data management design for IoT-enabled smart city planning,” *IEEE Access*, vol. 8, pp. 145256–145267, 2020.

[86] S. Chatterjee, A. K. Kar, and M. P. Gupta, “Success of IoT in smart cities of India: An empirical analysis,” *Gov. Inf. Q.*, vol. 35, no. 3, pp. 349–361, 2018.

[87] V. Albino, U. Berardi, and R. M. Dangelico, “Smart cities: Definitions, dimensions, performance, and initiatives,” *J. urban Technol.*, vol. 22, no. 1, pp. 3–21, 2015.

[88] E. Ismagilova, L. Hughes, N. Rana, and Y. Dwivedi, “Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework,” *Inf. Syst. Front.*, 2020.

[89] C. Perera, M. Barhamgi, A. K. Bandara, M. Ajmal, B. Price, and B. Nuseibeh, “Designing privacy-aware internet of things applications,” *Inf. Sci. (Ny).*, vol. 512, pp. 238–257, 2020.

[90] T. van den Broek and A. F. van Veenstra, “Governance of big data collaborations: How to balance regulatory compliance and disruptive innovation,” *Technol. Forecast. Soc. Change*, vol. 129, 2017.

[91] Z. Allam and D. Jones, “On the Coronavirus (COVID-19) Outbreak and the Smart City Network: Universal Data Sharing Standards Coupled with Artificial Intelligence (AI) to Benefit Urban Health Monitoring and Management,” *Healthcare*, vol. 8, p. 46, 2020.

[92] L. A. Zadeh, “Fuzzy Sets,” *Inf. Control*, vol. 8, pp. 338–353, 1965.

[93] E. Akyuz and E. Celik, “Journal of Loss Prevention in the Process Industries A fuzzy DEMATEL method to evaluate critical operational hazards during gas freeing process in crude oil tankers,” *J. Loss Prev. Process Ind.*, vol. 38, pp. 243–253, 2015.

[94] I. Vardopoulos, “Critical sustainable development factors in the adaptive reuse of urban industrial buildings . A fuzzy DEMATEL approach,” *Sustain. Cities Soc.*, vol. 50, no. May, p. 101684, 2019.

[95] H. Xiao, Y. Zhang, G. Kou, S. Zhang, and J. Branke, “Ranking and selection for pairwise comparison,” *Nav. Res. Logist.*, 2023.

[96] D. J. Jeng, “Computers & Industrial Engineering Generating a causal model of supply chain collaboration using the fuzzy DEMATEL technique q,” *Comput. Ind. Eng.*, vol. 87, pp. 283–295, 2015.

[97] S. Luthra, K. Govindan, R. K. Kharb, and S. Kumar, “Evaluating the enablers in solar power developments in the current scenario using fuzzy DEMATEL : An Indian perspective,” *Renew. Sustain. Energy Rev.*, vol. 63, pp. 379–397, 2016.

[98] M. Nazir and N. Cavus, “Fuzzy DEMATEL method for identifying LMS evaluation criteria,” *Procedia Comput. Sci.*, vol. 120, pp. 742–749, 2018.

[99] K. Lin, M. Tseng, and P. Pai, “Resources , Conservation and Recycling Sustainable supply chain management using approximate fuzzy DEMATEL method,” *"Resources, Conserv. Recycl.*, vol. 128, pp. 134–142, 2018.

[100] X. Fu, N. Wang, S. Jiang, F. Yang, J. Li, and C. Wang, “A research on influencing factors on the international cooperative exploitation for deep-sea bioresources based on the ternary fuzzy DEMATEL method,” *Ocean Coast. Manag.*, vol. 172, no. February, pp. 55–63, 2019.

[101] C. Lin, G. Kou, Y. Peng, and F. E. Alsaadi, “Aggregation of the nearest consistency matrices with the acceptable consensus in AHP-GDM,” *Ann. Oper. Res.*, pp. 1–17, 2020.

[102] J. Zhang, G. Kou, Y. Peng, and Y. Zhang, “Estimating priorities from relative deviations in pairwise comparison matrices,” *Inf. Sci. (Ny).*, vol. 552, pp. 310–327, 2021.

[103] D. Yu, G. Kou, Z. Xu, and S. Shi, “Analysis of collaboration evolution in AHP research: 1982--2018,” *Int. J. Inf. Technol. Decis. Mak.*, vol. 20, no. 01, pp. 7–36, 2021.

[104] F. Acuña-carvajal, L. Pinto-tarazona, H. López-ospina, R. Barros-castro, L. Quezada, and K. Palacio, “An integrated method to plan , structure and validate a business strategy using fuzzy DEMATEL and the balanced scorecard,” *Expert Syst. Appl.*, vol. 122, pp. 351–368, 2019.

[105] Y. Li, G. Kou, G. Li, and Y. Peng, “Consensus reaching process in large-scale group decision making based on bounded confidence and social network,” *Eur. J. Oper. Res.*, vol. 303, no. 2, pp. 790–802, 2022.

## Identifying and evaluating factors affecting user privacy in the smart city using the meta-synthesis method and the fuzzy DEMATEL technique

First, I would like to express my gratitude to the respected Editor-in-Chief, Dr. Gang Kou, for taking into consideration our efforts in research. We thank the Reviewers for their excellent suggestions and guidance in improving the manuscript's content. We value the time and effort the reviewers spent assessing our manuscript. Thank you for the opportunity to submit a revised manuscript and for your constructive comments on our manuscript. We hope, this article can be helpful to both practitioners and academicians in field of smart cities.

### Reviewers' comments: The references should be updated with the most recent in your paper's research field of relevance.

All of the recommended references have been included in the paper. We hope that this addresses the concerns raised by the reviewer.

Best regards