JDESA
JOURNAL OF DECISION SCIENCE AND APPLICATIONS

Journal of Decision Science and Applications

www.jdesa.org
eISSN: 0000 -000

A Knowledge-Driven Framework for Privacy Personalization in Smart Cities: Integrating Meta-Synthesis, Fermatean Fuzzy SWARA, and Clustering Approach

Mahmoud Zahedian Nezhad[1], Arezu Zamani[2], Tahereh Sepahi[3], Mohammad Mehraeen[4,*], Javad Nazarian-Jashnabadi[5,*]

1 Faculty of Economic and Administrative Sciences, Ferdowsi University of Mashhad, Azadi Square, Mashhad, Iran.
2 Faculty of Economic and Management, Tarbiat Modares University, Jalal-al-Ahmad Street, Tehran, Iran.
3 Department of Management, Faculty of Management and Accounting, Shahid Beheshti University, Tehran, Iran.
4 Faculty of Economic and Administrative Sciences, Ferdowsi University of Mashhad, Azadi Square, Mashhad, Iran.
5 Department of Management, Faculty of Economic, Management and Social Science, Shiraz University, Shiraz, Iran.

ARTICLE INFO

Article history:
Received 29 June 2026
Received in revised form 1 August 2026
Accepted 4 August 2026
Available online 7 August 2026

Keywords:
Smart City; User Privacy and Security; Clustering Techniques; Meta-synthesis Method; Knowledge Management, FF-SWARA

ABSTRACT

In recent years, smart cities have increasingly adopted digital technologies to improve public services, enhance citizens' quality of life, and promote sustainable urban development. However, concerns regarding user privacy and security remain a major barrier to the widespread adoption of smart city services, often reducing users' trust and willingness to engage with these technologies. This study proposes a knowledge management-based framework to support the personalization of user privacy in smart cities by applying the Wiig knowledge management cycle. First, a meta-synthesis approach is employed to identify the key dimensions, factors, and indicators affecting user privacy through a comprehensive review of the existing literature. The extracted knowledge is then refined and validated through semi-structured interviews with two domain experts. Subsequently, the relative importance of the identified dimensions is determined using the Fermatean Fuzzy Step-wise Weight Assessment Ratio Analysis (FF-SWARA) method based on the evaluations of seven experts. The results indicate that Security Requirements (C7) is the most influential dimension, followed by Data Management (C6), Reference Standards, Frameworks, and Rules (C5), Risk and Risk Management (C8), Transparency (C4), Self-Control and Customization (C3), Awareness and Understanding (C1), Trust (C2), and Acceptance of Smart City Applications (C9). The prioritized dimensions are then incorporated into a questionnaire administered to smart city users. Finally, machine learning clustering algorithms are applied to classify users according to their privacy preferences, enabling the development of personalized privacy recommendations tailored to the characteristics and expectations of each user group.

1. Introduction

* Corresponding author.
E-mail address: mehraeen@um.ac.ir
* Corresponding author.
E-mail address: J_Nazarian@shirazu.ac.ir

Smart cities, through the utilization of technologies and digital innovations, bring forth a wide array of services for their citizens, leading to an enhanced quality of life and improved well-being. Smart cities harness advanced technologies and data-driven approaches to elevate urban living standards. These technologies, such as Internet of Things (IoT) devices, sensors, and surveillance systems, generate vast amounts of data [1]–[3]. To effectively provide their services on a broad scale, these cities must continuously generate, store, process, and analyze substantial volumes of data from users, devices, and sensors [4]. The extensive generation, transmission, and processing of this data to offer services to users may result in uncovering behavioral patterns, lifestyle trends, interests, and consumption habits. Additionally, it can provide easier access to citizens' personal and private information, potentially infringing on their privacy [5]. Breaching user privacy stands as one of the most significant challenges threatening the proper implementation of smart cities, leading to citizens' distrust and skepticism towards the services and offerings of the smart city. Knowledge management plays a pivotal role in processing, analyzing, and utilizing this data to enhance urban services, optimize resource allocation, and bolster decision-making. Smart cities must ensure the proper safeguarding of user security and privacy to ensure the acceptance and participation of their citizens, as the benefits of a smart city can be negated if citizens are reluctant to engage [6], [7]. To address these privacy preservation concerns, knowledge management plays a crucial role. By implementing robust data governance frameworks and advanced analytical techniques, smart city managers can effectively anonymize and secure data. Knowledge management approaches can contribute to the development and maintenance of policies ensuring that data is only accessible by authorized personnel, and privacy protections are continuously updated. Furthermore, knowledge management can enhance citizens' awareness of privacy importance within the smart city context. By providing information about data collection methods and the benefits of smart city initiatives, residents can make more informed decisions and actively engage in safeguarding their privacy. Effective knowledge management approaches can contribute to alleviating privacy concerns by ensuring data governance, appropriate security measures, and citizen engagement, ultimately strengthening the smart city ecosystem while respecting privacy and becoming pervasive.

Knowledge is a driving force that enables intelligent and informed action. Through improved knowledge, we gain a better understanding of how to perform tasks. Working intelligently entails utilizing the best available knowledge at our disposal. In this study, an attempt has been made to utilize a knowledge management approach and the stages of the Wiig cycle to first gather and encode dimensions (existing knowledge) that impact user privacy preservation in a smart city. Subsequently, employing machine learning techniques, the collected user feedback data is analyzed. By uncovering existing patterns, the study identifies the specific requirements of each user and, through accurate classification, provides suggestions for enhancing their privacy. This process represents the practical application of the acquired knowledge in the realm of privacy improvement. In this study, to acquire both tacit and explicit knowledge, integrate them, and share them with users within the smart city context, the findings of the Wiig knowledge management cycle are employed. Wiig primarily aims to facilitate intelligent performance through the creation, storage, sharing, and utilization of quality knowledge. The Wiig knowledge management cycle pertains to the creation and utilization of knowledge within individuals or organizations. The four main stages of this cycle include creation, storage, integration, and application of knowledge [8]. To this end, aligning with the initial stage of the Wiig knowledge management cycle, in order to generate and obtain knowledge, the dimensions influencing user privacy preservation are initially collected using a meta-synthesis approach as explicit knowledge is necessary. Harnessing explicit knowledge, utilizing a systematic review approach, leads to the collection, organization, and refinement of information, facilitating learning and problem-solving. Subsequently, for a better representation of knowledge and its systematic collection within a coherent model, the relevant knowledge is encoded, yielding an output that plays a pivotal role in user privacy preservation. In the subsequent phase, employing the knowledge acquired in the initial stage, a questionnaire is designed and shared with users to capture their tacit knowledge. Ultimately, following the accumulation of users' tacit knowledge, clustering algorithms are employed to extract their knowledge, categorizing them into different clusters based on their security requirements. To this end, the information garnered from users in the previous stage is subjected to analysis through two distinct approaches.

In the first approach, each dimension is assigned a weight using the average method. Then, for each user, a score is allocated based on the cumulative weights of each dimension (considering users' ratings for each dimension). This score indicates the level of importance of the set of dimensions influencing privacy for each user. Finally, clustering is performed for all individuals using the K-means method, as this method, given its two-dimensional matrix nature, yields the best and most accurate clustering results. The output of this section will be the categorization of users in terms of the significance they attribute to the set of privacy-influencing dimensions. In the second approach, the priority level of each dimension is individually weighted for all users. To achieve this, users are asked to rank dimensions in terms of their prioritization in maintaining their privacy within the smart city. For the analysis of the second approach, clustering is conducted based on the K-modes method, as it proves reliable for multidimensional clustering. Finally, in the concluding phase of the knowledge management cycle, the utilization of knowledge must be executed accurately. Which knowledge is to be employed and for what group of individuals? This involves determining which specific knowledge should be used and for which group of individuals within the context of the smart city. It's essential to consider how this knowledge can be effectively imparted to these individuals to enable them to understand its proper application and believe that implementing this knowledge will enhance their performance [9].

In light of the points mentioned above, this research comprises the following sections: The second section delves into the realm of knowledge management and its application within a smart city context. The third section presents the research methodology, which encompasses the meta-synthesis approach for identifying and extracting the influential dimensions of user privacy, the preliminaries of the Fermatean Fuzzy Set (FFS) along with the procedural steps of the FF-SWARA method for determining the relative importance of these dimensions, and the general theory of clustering techniques employed for analyzing user data. The fourth section is dedicated to the findings and results, covering the prioritization of dimensions through the FF-SWARA method based on expert judgments, as well as the implementation and outcomes of the K-means and K-modes clustering algorithms applied to user responses. Finally, the fifth section provides a comprehensive summary, presents the overall conclusions drawn from both the expert-driven multi-criteria decision-making and user-centric clustering analyses, and offers practical recommendations for personalizing privacy preservation in smart cities.

2. Theoretical Foundation & Literature Review

In the midst of rapid urbanization and the intricate challenges faced by cities worldwide, the concept of smart cities has emerged as a promising solution for establishing sustainable, efficient, and livable urban environments. At the heart of this transformation lies the strategic integration of knowledge management methodologies, enabling smart cities to harness their intellectual capital for data-driven decision-making, innovation, and improved service delivery. Knowledge plays a central role, empowering intelligent and informed actions. By enhancing knowledge, we gain a deeper understanding of what needs to be done and how to do it. Smart cities, by leveraging knowledge as a strategic asset, can navigate the complexities of modern urban landscapes and explore new avenues for progress and prosperity. Knowledge management encompasses the systematic collection, organization, analysis, and dissemination of information and expertise within an organization or ecosystem. The Wiig framework emphasizes the primary objective of knowledge management as improving organizational performance by facilitating the creation, storage, sharing, and application of high-quality knowledge. The Wiig model outlines four key stages in the knowledge management cycle: Building knowledge, holding knowledge, pooling knowledge, and applying knowledge. The Wiig knowledge management cycle encompasses a wide range of learning from various sources. Depending on the field and objectives, knowledge can be integrated and applied through diverse methodologies. The knowledge creation phase involves activities sourced from various channels. Knowledge acquisition can take place through research and development projects, innovations, experiments, and more. Knowledge can also be obtained through inculcation, such as extracting expertise from experts and procedural guidelines, engaging in collaborations to acquire technology, or transferring personnel across departments. Additionally, knowledge can be gleaned from real-world observation. The preservation and storage of knowledge entail preserving, accumulating, and embedding knowledge within repositories and knowledge archives. The aggregation and integration of knowledge involve coordinating, collecting, accessing, and retrieving knowledge. Once knowledge sources are identified, they are consolidated into background references within a library or repository to facilitate subsequent access and retrieval. Finally, there are various approaches to applying knowledge, including using general knowledge to analyze exceptional situations, employing knowledge to describe problem domains and situations, analyzing situations with the aid of knowledge, and using knowledge for decision-making. Figure 1 provides a concise overview of the key activities within the Wiig knowledge management cycle [8].

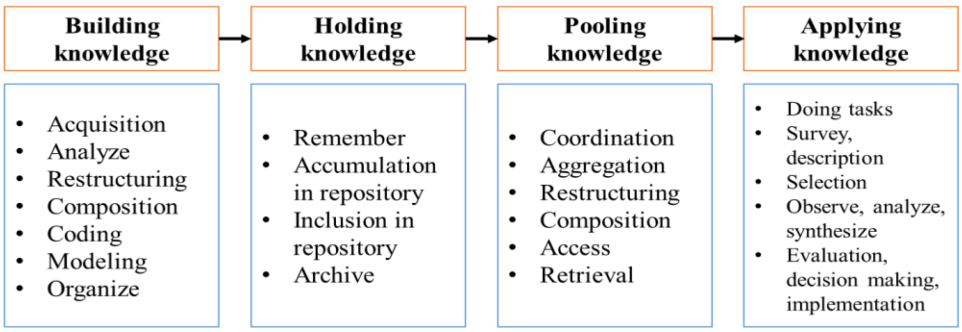


Fig. 1. Activities of the Wiig Knowledge Management Cycle [8].

In the field of knowledge management, once the decision is made that newly discovered or identified content holds sufficient value, the next step is to contextualize the content. This involves establishing a connection between the knowledge and individuals who are well-informed about the content. These well-informed individuals are those who have gained significant experience in using this content. Contextualizing knowledge also involves identifying key attributes of the content to better align it with a diverse user base. For example, personalizing content to match the preferences of end-users [8]. In the final stage of the Wiig Knowledge Management Cycle, the effective application of knowledge must be carried out. This stage includes internalizing knowledge, which involves understanding the content and recognizing that the presented knowledge offers a better way to accomplish tasks, thereby facilitating its use in personalization and user profiling. Utilizing classification techniques, learning methodologies, and personalization or profiling techniques can help ensure the best possible alignment between users and content [10]. The easier it is for a user to find, understand, and internalize knowledge, the more successful they will be in its practical application. Furthermore, in user profile personalization, identifying a user's interests based on their preferences or behavior can present knowledge content in an integrated and coherent manner, enhancing its accessibility and relevance to the user [9].

Knowledge management is a multidisciplinary field with its unique characteristics, and it has been the subject of extensive research concerning its role in smart cities and its various influential aspects. Notable studies have shed light on the multifaceted dimensions of knowledge management in the context of smart cities. Israilidis et al. (2021) conducted a systematic review and identified five distinct topics of knowledge management in smart cities. These topics include strategy and vision, frameworks, enablers and barriers, citizen engagement, and benefits. Furthermore, they emphasize the significance of knowledge-sharing and learning in the context of smart cities, outlining three future perspectives: socio-technical approaches to smart cities, integration of knowledge-sharing perspectives, and the development of organizational learning capabilities [11]. Borba et al. (2020) found that the knowledge-sharing process in a smart city serves as a crucial intersection between various domains. They argue that smart city initiatives encompass more than just the utilization of information and communication technology in urban environments. Human knowledge and the different stages of its consolidation and sharing play a vital role in the process of "smartification." The authors stress the importance of considering recommendations and insights from service providers who contribute significantly to smart city development. They also highlight the essential role of the culture of knowledge sharing and identify four main stakeholders impacting knowledge management in smart cities: companies, governments, communities, and universities. Within the community segment, they emphasize citizen awareness, culture, knowledge sharing, and issues related to open data accessibility [12]. Roblek and Meško (2020) take a holistic approach to understanding the governance process of smart cities and delve into the phenomenon of knowledge management within this context. They explore knowledge-based activities in smart cities, urban data platforms, cyber-physical environments, smart (urban) technologies, and the key stakeholders involved. According to their perspective, knowledge management mechanisms in smart cities are rooted in socio-technical approaches, integrating knowledge management methods, and fostering the development of learning skills. The key stakeholders identified in smart city systems include users (such as citizens), enablers (such as information technology and communication companies), providers of resources (such as universities and research institutions), and framework enablers (such as government and policymakers). They emphasize the importance of leveraging implicit knowledge to generate new knowledge within a smart city, which involves advanced urban technologies collecting knowledge from citizens and transferring raw data to data processing and storage centers [13], [14].

Laurinia (2021) investigates the relationship between smart cities and the knowledge society, underscoring the importance of knowledge as a shared asset for experts and citizens in achieving sustainable development. The study focuses on the integration of human knowledge and artificial intelligence within geographical knowledge systems, utilizing processed machine-readable knowledge and rules. It elaborates on geographical rules to address spatial issues and proposes a comprehensive structure for geographical knowledge base systems, highlighting the role of collective human intelligence. The paper suggests that artificial intelligence and knowledge management can enhance urban governance, emphasizing the necessity of practical experiments and essential elements such as data transformation into knowledge, encoding rules in a machine-process able language, and designing a dedicated inference engine for successful implementation [15]. Abdalla et al. (2023) address the crucial importance of effective knowledge management in handling the COVID-19 pandemic, particularly within the context of smart cities. The study underscores the urgent need for immediate solutions and rapid responses in epidemic prevention and management. Smart city technologies offer various tools for capturing, acquiring, sharing, and transferring knowledge, which can aid decision-making and managerial efforts in combating the pandemic [16]. The paper employs a systematic literature review to explore the role of smart cities in managing COVID-19-related knowledge. Findings reveal that advanced information and communication technology (ICT) applications in smart cities play a pivotal role in knowledge capture and sharing. These strategies enable the extraction of knowledge through data collection and analysis from various databases, allowing for efficient handling and analysis of vast and unpredictable amounts of data. Implementing knowledge management initiatives related to COVID-19 has the potential to improve pandemic planning, treatment, and control, enhance decision-making, and enable effective disaster management. Nevertheless, managing the substantial volume of complex and unstructured data remains a significant challenge for these initiatives. To address this, the paper proposes a conceptual model illustrating the relationship between smart city strategies, knowledge management, and COVID-19, providing insights to facilitate decision-making for the recovery process [17]. Chang et al. (2018), have explored the challenges of assessing smart and sustainable cities in the context of global climate change and urbanization. Their study advocates merging KBUD, smart city, and sustainable development concepts, presenting a conceptual framework proposal for knowledge-based, smart, and sustainable cities. KBUD considers knowledge as a central element in the development strategy, aiming to transition cities and regions into sustainable and prosperous localities. Their conclusion emphasizes the importance of an integrated approach to smart and sustainable city assessment, facilitating evidence-based policymaking and fostering KBUD within cities. The transition from industrial to knowledge-based cities reflects the shift from tangible to intangible assets, with knowledge being considered valuable capital. KBUD proves to be compatible with promoting smart and sustainable cities by articulating development domains comprehensively [18].

3. Research Methodology

This section describes the research methodology adopted in this study which consists of three main stages. First, a meta-synthesis approach is employed to identify the dimensions, factors, and indicators related to user privacy in smart cities. Second, the FF-SWARA method is applied to determine the relative importance of the identified criteria based on expert judgments. Finally, clustering methods are utilized to categorize users according to their privacy-related characteristics, facilitating the development of personalized knowledge management strategies. The details of each stage are presented in the following subsections.

3.1 Meta-synthesis approach

In a smart city, user privacy is impacted by a range of dimensions and factors, encompassing both quantitative and qualitative aspects. To thoroughly comprehend these dimensions, the study employs the meta-synthesis approach, which is a qualitative method capable of analyzing and combining both quantitative and qualitative findings. This research is applied in its objectives and employs mixed method for data collection. To identify and extract these dimensions, the seven-step method by Sandelowski and Barroso (2007) has been implemented [19], [20]. Figure 2 provides an overview of the stages involved in this method.

The first step in the meta-synthesis approach involves identifying the questions that the researcher intends to explore. The central questions of this research, as introduced in the introductory section and approached through the adoption of this method, are:

1. What are the most influential dimensions affecting the preservation of user privacy?
2. Which dimensions are evident in existing documents and previous research as explicit knowledge?
3. What are the opinions of users regarding the dimensions extracted as tacit knowledge?
4. How is the acquired knowledge from the extracted dimensions utilized for the preservation of user privacy?

These questions form the basis of the study's inquiry and guide the research in identifying and understanding the dimensions that impact user privacy in a smart city.

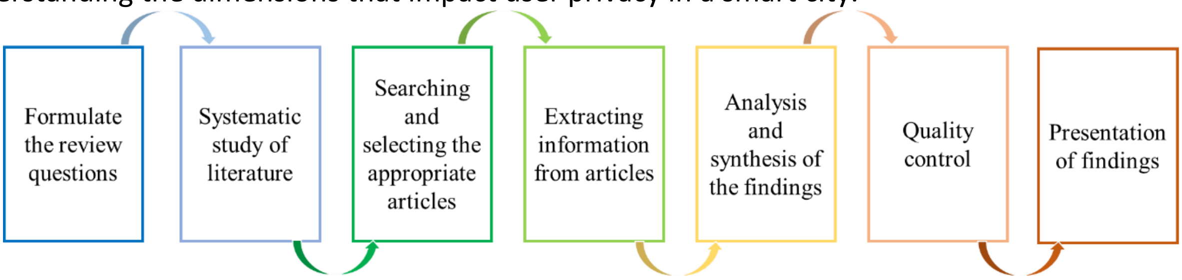


Fig. 2. The 7-Step Pattern of Sandelowski and Barroso [19]

In the second step of the meta-synthesis, a systematic examination of sources was conducted using two scholarly databases, namely Web of Science and Scopus. Articles were selected based on the combination of three key terms: "Smart City," "Privacy," and "User," within the time frame spanning from 2010 to the end of 2021. The extraction formula used is presented below:

TS= ("Smart city" AND "Privacy" AND "User")

The third step of the meta-synthesis process entails the review and selection of relevant articles. The selection of these articles was guided by the criteria detailed in Table 1. Following this, the extracted articles underwent a comprehensive 5-stage evaluation process, which involved the scrutiny of titles, abstracts, accessibility, content relevance, and, lastly, the assessment of methodological quality.

Table 1
Acceptance criteria for articles

Criteria	Inclusion Criteria	Exclusion Criteria
Language of Articles	Articles Written in English	Non-English Articles
Submission Time of Articles	Published Articles from 2010 to 2021	Articles Published Before 2010

Research Topic	User Privacy in Smart Cities	Cases Differing from the Mentioned Topic
Research Scope	Identification of Dimensions, Factors, and Indicators Affecting User Privacy in Smart Cities	Cases Differing from the Mentioned Scope

During the screening phase, a preliminary total of 134 articles were retrieved from the Web of Science academic database, and 267 articles were obtained from the Scopus academic database. Out of these, 55 articles were identified as common to both databases. The identification of these shared articles was carried out through a sequential process. Initially, both databases were separately assessed based on titles and abstracts, following a two-step procedure. Subsequently, before proceeding to the third step (accessibility review), duplicate and shared articles from both databases were identified. This resulted in 26 articles, out of the 55 common and duplicate ones, being accepted based on the first two steps. Further integration was conducted between the shared Scopus articles and the ones extracted from Web of Science. In other words, 99 articles underwent content assessment in the fourth step, involving the examination of both databases. The screening process, consisting of five steps, is depicted in Figure 3. The last step, which involves evaluating the methodological quality of articles, was omitted because both the Web of Science and Scopus databases were deemed to have satisfactory quality. As a result, a total of 75 articles that met the acceptable content criteria were chosen as the final set of articles for analysis.

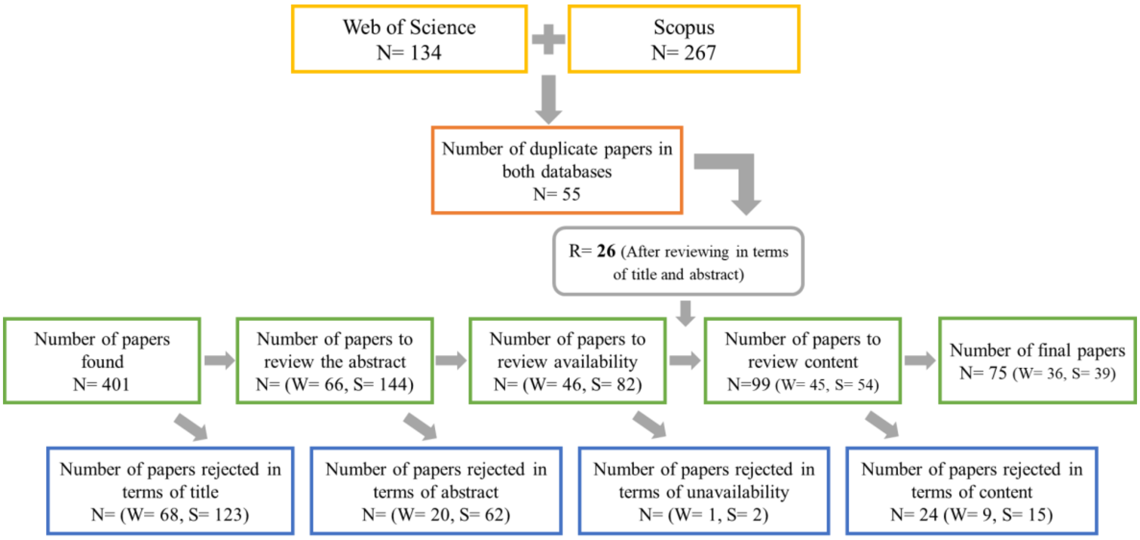


Fig. 3. The process of article screening based on the meta-synthesis approach.

In the fourth and fifth steps of the meta-synthesis process, the influential dimensions of user privacy were extracted and integrated. The result of the meta-synthesis approach identified nine major dimensions that have a substantial impact on safeguarding user privacy, as described in 72 articles discussing concepts related to these dimensions. The relevant dimensions and the articles that cover them are provided in detail in Table 2.

Table 2
Influential dimensions on user privacy in smart cities

Dimensions	References
Awareness and understanding	[21]–[41]
Trust	[22], [33], [38], [42]–[49]
Self-Control and Customization	[24], [26], [29], [34], [41], [46], [50]–[59]
Transparency	[21]–[27], [33], [37], [40], [41], [48], [57], [58], [60]–[63]
Reference Standards, Frameworks, and Rules	[24], [25], [27], [29]–[31], [34], [37], [40], [42], [48], [53], [55], [57], [61], [62], [64]–[76]
Data Management	[25], [43], [47], [58], [64], [69], [71], [77]–[80]
Security Requirements	[24]–[29], [37], [39], [42], [48], [53], [55], [57], [58], [61]–[63], [70], [71], [73], [79]–[91]
Risk and Risk Management	[21], [23], [35], [37], [66], [67]
Acceptance of Smart City Applications	[22], [33], [35], [36], [38], [40], [67]

In the fifth step, this study employed Cohen's kappa coefficient to control and evaluate the extracted dimensions. In this process, the extracted dimensions were presented to two experts to assess their importance based on their impact. Each expert rated the dimensions independently, without being aware of the other expert's evaluations. The Kappa statistic value, obtained using SPSS software, was 0.6. With a significant p-value of 0.033, this statistic is deemed acceptable. The results of the Kappa coefficient calculations can be found in Table 3.

Table 3
Kappa agreement coefficient

Criteria	value	Asymp. Std. Error	Approximate	sig
Kappa Agreement Metric	0.600	0.223	2.135	0.033
Number of Valid Cases	9			

In the upcoming subsections, each dimension listed in Table 2 will be thoroughly examined and discussed.

3.1.1 Awareness and Understanding

A fundamental challenge in ensuring privacy in smart cities is the insufficient level of public awareness among users. Users in smart cities need to be well-informed about how to safeguard themselves against different privacy threats. Increasing user awareness and knowledge regarding their rights to protect their privacy, as well as the associated risks and vulnerabilities, can be accomplished through the implementation of various smart city programs and technologies [24], [28], [29], [92]. Increasing this awareness poses a significant challenge, as it often falls outside the direct purview of researchers and is typically the responsibility of media and political authorities. Building awareness involves educating users about issues related to the collection of private data and the utilization of such data by security agencies [47], [70]. Raising awareness through initiatives for the secure deployment of IoT-equipped smart cities is of paramount significance. User unawareness can act as an indicator of security and privacy threats that may have consequences for other systems and users within a smart city [27], [93]. In addition to IoT, emerging technologies like cloud centers, blockchain, and artificial intelligence offer numerous innovations for smart cities [94]. Some of these technologies are still in their developmental stages, and concerns about potential "privacy loss" for users may arise. Therefore, stakeholders and smart city developers must inform users about their data handling behavior, security requirements, and privacy preservation related to the use of these technologies [40]. There are specific measures that can be implemented within a given system to enhance public awareness of privacy risks. Privacy and security alerts are designed to alert individuals to potential privacy threat. It is anticipated that privacy awareness systems and services will progressively adhere to frameworks, regulations, laws, ethical guidelines, and operational standards that are specific to this field [43]. Users need to better understand the value of personal data, and this understanding can lead to their informed use of the benefits inherent in the concept of a smart city [25], [26], [30], [32].

3.1.2 Trust

Trust plays a pivotal role in shaping people's decision-making and their willingness to embrace new technologies. Trust inherently entails a degree of acceptance of risk and vulnerability in relation to a trusted entity. This willingness to assume risk is rooted in the belief that the trusted party will undertake actions that are advantageous or meaningful for the party in a vulnerable position [49]. Building trust among users is of utmost importance for broadening the operational reach and efficiency of systems and infrastructure in smart cities. Without trust from all stakeholders, users are likely to abstain from participating in smart city systems and interfaces. In instances where users have apprehensions about security risks or privacy violations, their reluctance to engage during interactions can signify lower levels of trust [95]. Trust is a fundamental concern in smart cities, where sensors and various tools continuously collect data. Trust in key entities responsible for collecting and processing data is of utmost importance. The concepts of trust and privacy are interconnected and multifaceted, influenced by individuals' personal circumstances. Individuals using smart city services often have concerns about security vulnerabilities and privacy breaches. Perceived security and privacy directly impact the level of trust in using smart city services. Public trust must be a top priority in the development of smart cities [96], [97]. Trust from citizens and users in security and privacy policies in smart cities results in their satisfaction. Increasing this satisfaction will facilitate and enhance user engagement and interaction in the advancement of smart city development and implementation. Consequently, acceptance and satisfaction are prerequisites for lawful data collection and processing. The establishment of suitable trust-based mechanisms should ensure user satisfaction and participation in smart city projects. However, current disclosure and satisfaction practices, as demonstrated using privacy preservation policies, do not adequately address consumer needs concerning privacy priorities and trust. With the evolution of smart cities, consumer priorities regarding trust must be considered [47], [98].

3.1.3 Transparency

Sustaining user trust within a smart city necessitates that operations are observable and carried out with transparency. Transparency in this context implies that data is collected and stored by governments and companies, while individuals may not have complete awareness of the data being stored about them and possess limited control over their data [99]. When developing smart city programs, prioritizing data transparency is essential. This involves enabling users to comprehend the status of their data, understand what data is being collected, how it is processed, what types of data are stored, with whom it is shared, and how it is safeguarded. For example, cities can send regular reports to citizens outlining the data stored about them, allowing them to easily rectify or delete it. Transparency elevates citizens' levels of trust and, consequently, bolsters the acceptance of smart city programs [63]. Transparency, achieved through detailed explanations of the functions and processes of privacy protection systems, renders the level of privacy comprehensible for users. Users should receive clear responses to questions such as: Who can access their data? Is third-party access a possibility? What kind of information can be deduced from the data? Is their data shared internationally? Are there identified vulnerabilities in the device? Can their movements be traced through their data? What steps can be taken if their personal information is jeopardized? Is a copy of their user data retained? Therefore, developers of smart city initiatives and privacy designers must emphasize transparency, ensuring that citizens are informed about all aspects of their data's fate [43], [47], [70].

3.1.4 Self-control and Customization

The transition from existing traditional infrastructures to infrastructures that incorporate smart city innovations poses a significant risk to designers and planners unless sufficient focus is placed on user-related factors. Systems that collect user information without considering their privacy priorities can lead to privacy breaches, making user preferences a crucial consideration in designing a privacy-preserving model for smart city systems. Self-control entails that data owners can oversee and regulate their data, specifying particulars, data protection techniques, data gathering, and data storage durations. The finest smart services should provide a variety of options aligned with user preferences. These options should be modifiable by users according to their desires, including the adjustment of default device permissions and default settings, such as location access, images, and videos. Nonetheless, this procedure can be labor-intensive and demands a certain level of expertise. In cases where users have limited knowledge in this domain, the default settings chosen by privacy engineers assume even greater significance. Users are initially queried about overarching decisions (i.e., whether they grant permission), and subsequently, they are presented with more specific controls (e.g., what types of data can be collected). Elaborate settings could potentially result in the excessive collection of surplus information, rendering the user's decision-making process more complex. The utilization of statistical analysis techniques can enhance predictive accuracy and aid in the selection of the most suitable settings [54], [75], [100], [101]. One of the pressing issues with smart cities is the restricted control users have over their personal data. When smart city services incorporate features that empower users to manage their data and tailor services to their activities, it is anticipated that users will be more diligent in safeguarding their privacy. These services provide a range of choices to users in line with their preferences and interests, enabling the customization of security and privacy parameters in real-world situations when necessary. Users of smart cities may also need to build and customize their smart environment by choosing various hardware devices and software components. Furthermore, users should have the capability to grant or withdraw access permissions to both other users and service providers [24], [56]–[58], [100].

3.1.5 Data management

Data stands out as one of the most pivotal concerns in a smart city context. The findings from the meta-synthesis approach reveal that discussions pertaining to data and its privacy implications are prevalent across the majority of articles. These discussions encompass various aspects, such as data privacy, data confidentiality, data collection, storage, access, sharing, integration. Furthermore, a smaller subset of articles has delved into the concept of data governance. All these subjects can be indispensable within the realm of data management, and they wield substantial influence over user privacy. Consequently, this study regards this dimension as one of the pivotal facets of user privacy. Smart city services and applications generate a tremendous volume of data, underscoring the critical importance of effective data management. The data management framework encompasses a multitude of stakeholders, including policymakers, data creators, service providers, users, and consumers. The roles that these stakeholders assume in relation to smart city data can vary, encompassing functions such as data generation, data collection, data processing, data provision, and data consumption. [64]. Smart city developers and policy makers have put forth a range of initiatives, both technical and non-technical, for effective data management. These initiatives manifest as standards, frameworks, regulatory legislation, or data management architectures within smart cities. Data management encompasses the fundamental processes of data collection and acquisition, storage and processing, dissemination, maintenance, and, ultimately, data utilization. Each of these processes carries specific prerequisites for safeguarding user privacy [77]. Within these processes, there are also steps that can impact data abundance, quality, and security and potentially create challenges for user privacy, such as data integration, sharing, and data access. Considering various data collection platforms, data integration is a fundamental step in data management, as dealing with numerous data platforms and repositories may make it challenging to maintain user privacy. It is essential to note that data integration itself poses its own unique challenges, requiring corresponding approaches [78].

3.1.6 Security and privacy reference standards, frameworks and rules

Introducing smart city initiatives necessitates the establishment of policies, standards, regulations, and reference frameworks for their execution. One crucial aspect associated with smart cities, contingent upon these policies, is the safeguarding of data privacy, and by extension, the privacy of the users. Within this section, we will delve into concepts linked to the preservation of privacy, encompassing protective standards, certifications, public data protection laws and regulations, as well as the legal and supervisory dimensions. These non-technical mechanisms serve as a complement to technical mechanisms and should be meticulously devised within a comprehensive privacy protection framework, fully taken into account in the smart city's development. Developers of smart cities and designers of privacy frameworks face the challenge of not being able to establish a multitude of standards, regulations, and policies solely for the protection of data confidentiality and user privacy. The breadth of these policies and standards introduces a significant level of complexity and inundates stakeholders in smart cities with a multitude of rules and solutions. Currently, there are no universally accepted protocols, standards, or laws pertaining to user privacy in smart cities on a global scale. Even if there are regulations at the local level, they are typically crafted and enforced within specific local jurisdictions [102]. Adherence to standardized methods and techniques for smart city implementation is crucial. As an example, in order to guarantee the safe and efficient production and utilization of devices and technologies in smart cities, there are established standards that equipment manufacturers and developers are required to follow. Organizations such as the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU) have played a key role in formulating standards in this domain. Prominent standards in this field are provided by organizations like IEC, ITU, ISO, and IEEE [103]. Because of the diverse contexts and initiatives within smart cities, developers have devised and enforced their own regulations and policies tailored to their respective regions. For instance, the European Union, as well as various countries including the United States, India, China, Brazil, and Mexico have implemented their own supportive laws. In this context, the Organization for Economic Co-operation and Development (OECD) has introduced a framework for data protection, which restricts data collection and mandates user consent and awareness whenever feasible. The Asia-Pacific Economic Cooperation (APEC) has also established a framework that defines various aspects of harm prevention, warnings, restrictions on data collection, usage, and the integration of personal information, security safeguards, access, correction, and responsiveness. The European Union's General Data Protection Regulation (GDPR) has introduced a comprehensive framework for data protection, featuring new commitments for organizations and an extended scope. It grants legal rights to consumers, including the right to access personal data, the right to be forgotten, the right to rectification, and the right to restrict processing. Clear regulations govern data collection from users, access to personal data, non-automated profiling, modification and deletion, and the right to object. Non-compliance with these laws can lead to significant consequences, including fines that can reach up to 20 million euros or 4% of the global revenue, depending on which is higher [44], [104], [105].

3.1.7 Security requirements

Security is indeed a fundamental aspect of smart cities, and ensuring the safety and privacy of data and users is paramount. The fundamental security requirements that must be encompassed within smart city programs and initiatives consist of confidentiality, integrity, and availability (CIA). In addition to CIA, other pivotal security requirements encompass identity authentication, access control, user privacy preservation, and resilience against potential threats, as indicated in the findings derived from the meta-synthesis method. Apart from these security requirements, other aspects like anonymity, responsiveness, auditing, non-repudiation, and public and private keys also come into play. These security requirements should be integrated by service providers, equipment manufacturers, and application developers incorporated into their services and programs. Some of these requirements, such as access control, identity authentication, and public and private keys, possess technical aspects, while others, like accountability, responsiveness, and auditing pertain to non-technical aspects. One prominent example of security requirements that stakeholders in smart cities should adhere to is the security controls outlined in the Information Security Management System (ISMS) standard, ISO 27001. Security requirements, in addition to ensuring service integrity, play a critical role in safeguarding user privacy.

During the design of applications and services, it's essential to consider the specific system context and needs and determine which security requirements are necessary. For instance, consider secure data sharing, where requirements like identity authentication, accessibility, authorization, data integrity, data confidentiality, anonymity, and non-repudiation may be indispensable for data sharing. These requirements not only ensure secure data sharing but can also have an impact on safeguarding user privacy during the data sharing process [61], [87]. Violating any of these requirements or neglecting them could have negative consequences for user privacy. Research studies that provide various services and plans for smart cities have presented specific security requirements in their designs. To achieve an optimal and desirable level of security for these services, developers must adhere to important and common security requirements to ensure the security and privacy of users. Identifying and assessing these security requirements is crucial, although it falls beyond the scope of this study. For example, Kalloniatis et al. (2019) enumerated key attributes that affect data and user privacy and identified 17 concepts [39]. Apart from identifying these requirements, evaluating them can lead to desirable outcomes for smart city initiatives and their stakeholders. It's important to tailor these security requirements to the specific needs and contexts of smart city projects to ensure the highest level of security and user privacy.

3.1.8 Risk Management

Identifying and effectively managing the risks associated with the security and privacy of users in the implementation of smart city initiatives, as well as other related risks, is of paramount importance. This can aid researchers, professionals, stakeholders, and particularly users in gaining a comprehensive understanding of the primary privacy risks in the context of smart cities. Therefore, understanding how users react to the concept of "security and privacy in a smart city" necessitates the identification of these risks. In a study conducted by Ola et al. (2021), they delved into risk management in the governance of sustainable smart cities. This study is based on a framework known as the Technology-Organizational-Environmental (TOE) framework, which encompasses significant risks in three key categories: technological, organizational, and environmental [21]. To effectively manage these risks, it is crucial to understand users' reactions in the context of smart city implementations and use cases. Some of the identification of risks and users' reactions to smart city implementations and use cases can be found in previous studies, which can be related to the dimension of "acceptance" as derived from general information systems research. For example, the Unified Theory of Acceptance and Use of Technology (UTAUT) theory can be applied to examine users' perspectives on the adoption of specific technologies and innovations within a particular context, including security and privacy issues. For instance, Batot et al. (2020) applied the dimensions of the UTAUT theory to investigate Dutch citizens' views on the emerging concept of "smart city safety," which involves the advanced use of digital technologies and data for urban safety management. Their study focused on users' acceptance and risk perceptions, demonstrating the importance of understanding the capabilities and responsibilities of users concerning urban safety and managing certain risks. Moreover, the study highlighted that predicting the adverse effects of technologies in the realm of smart urban safety requires considering user responsibility and autonomy [35]. Moreover, risk management in smart city initiatives intersects with various other dimensions. It is the responsibility of designers, developers, and implementers to ensure that these initiatives do not compromise the privacy and security of their users. Transparency throughout the entire lifecycle of these projects, starting from their design through implementation and operation, is crucial for effective risk assessment, validation, and accountability. To accurately identify and manage these risks, transparency within smart city initiatives must be established, meeting the needs of all stakeholders, particularly the end-users. Elahi et al. (2019) demonstrated in their research how the lack of transparency in smart assistants within smart cities hinders communication and poses challenges in risk identification and implementation. This deficiency renders many risk assessment models and malware detection systems ineffective, as revealed by their findings. These findings underscore the significance of transparency in the design and execution of smart city products, highlighting the necessity of establishing standards and specifications for such products. These standards should be developed by independent institutions in collaboration with all relevant stakeholders [37].

3.1.9 Acceptance of smart city applications

The investigation and evaluation of user and stakeholder acceptance of smart city programs, particularly with a focus on privacy and security concerns, can help guide users toward accepting these initiatives with proper awareness and understanding. To promote the adoption of smart city programs, their connection with other dimensions can be examined. In other words, it can be stated that broader contexts can assist users in accepting these initiatives more readily, with a better grasp of their security and privacy implications in the smart city context. Previous research has explored the relationship of these factors to some extent. The more information users receive about smart city initiatives, privacy protection, and the use of their data, the more likely they are to trust the providers of these initiatives and be inclined to use and adopt them [22]. Several recent studies, based on the Technology Acceptance Model (TAM) and/or the Unified Theory of Acceptance and Use of Technology (UTAUT) approaches, have demonstrated that trust is crucial for the adoption of new digital technologies, including privacy-focused smart city initiatives. While most users may express criticism, acceptance significantly increases when the purpose and benefits have high personal and social value. A study conducted by Jolsrud and Krogstad (2020) indicates that the adoption of smart city technologies and the sharing of private data, including location data, depend on the context of use. In such cases, trust, assurance, and transparency must be established in advance to address user privacy concerns. User acceptance and privacy concerns vary in different situations [33]. In the discussion of the acceptance of smart city initiatives, stakeholders should organize users' responses to initiatives related to the establishment of a smart city. To examine and evaluate this acceptance, as mentioned above, one can employ approaches such as TAM and UTAUT [35]. For instance, in current research on the adoption of technologies like smart city initiatives based on the UTAUT approach, performance expectations have shown the strongest influence on intentions to use smart city services. Moreover, user trust in the stakeholders' ability to effectively manage these initiatives serves as a positive predictor and evaluative measure for the intentions of using such initiatives. These criteria should contribute to increased adoption and utilization of smart city programs. The seven dimensions mentioned earlier, along with social norms, may aid in promoting the adoption of smart city initiatives. This helps users understand that accepting such initiatives does not equate to a breach of their privacy. The adoption of these initiatives, in turn, enhances the performance of smart city beneficiaries and can lead to the protection of users' privacy. In a study by Habib et al. (2020), a smart city beneficiary acceptance model (SSA) was presented, based on the integrated theory of acceptance and use of technology (UTAUT2). Their results demonstrate that each factor in this theory significantly influences citizens' willingness to use smart city services. Additionally, perceived security and privacy are strong determinants of trust in smart city initiatives. Strengthening this trust by addressing user privacy concerns increases their intention to accept and use smart city services [38].

3.2 FF-SWARA Method

Multi-Criteria Decision-Making (MCDM) has become one of the most widely adopted decision-support paradigms for addressing complex problems involving multiple, often conflicting, criteria. Over the past decades, MCDM methods have been successfully applied across a broad range of disciplines, including supply chain management, transportation, healthcare, energy systems, environmental sustainability, urban planning, finance, digital services, and smart city development. Their flexibility in structuring decision problems and prioritizing alternatives has led to the continuous development of new weighting and ranking techniques, as well as numerous methodological extensions to improve decision quality and practical applicability. Recent advances, such as the Base Criterion Method (BCM) and its variants, including Stratified BCM, Nonadditive BCM, and BCM Tradeoff, further demonstrate the ongoing evolution of MCDM methodologies to address increasingly sophisticated decision environments [106]–[109]. Despite their effectiveness, conventional MCDM approaches often assume that decision-makers can express their preferences using precise numerical values. In practice, however, expert judgments are frequently characterized by uncertainty, vagueness, ambiguity, and incomplete information, particularly in real-world decision-making contexts. To overcome these limitations, fuzzy set theory has been extensively integrated with MCDM methods, enabling linguistic assessments and uncertain opinions to be represented more realistically. The integration of fuzzy approaches with MCDM has significantly enhanced the robustness and reliability of decision-making models and has been successfully employed in diverse applications, including customer experience evaluation, risk assessment, sustainability analysis, and intelligent data-driven systems. More recently, advanced fuzzy environments, such as Fermatean fuzzy sets, have attracted increasing attention because of their superior capability to model uncertainty and capture experts' imprecise judgments compared with earlier fuzzy extensions [110]–[112]

3.2.1 Preliminaries of the Fermatean Fuzzy Set (FFS)

The Fermatean Fuzzy Set (FFS) was introduced by [113] as an effective framework for representing uncertain and imprecise information in decision-making problems. Similar to the Intuitionistic Fuzzy Set (IFS) and the Pythagorean Fuzzy Set (PFS), FFS characterizes uncertainty using membership and non-membership degrees. However, unlike these earlier fuzzy models, FFS satisfies the constraint that the sum of the cubes of the membership and non-membership degrees must be less than 1. This constraint provides greater flexibility in representing uncertainty and enables FFS to capture experts' judgments more effectively than IFS and PFS. The fundamental mathematical definitions of the FFS are presented below [114].

Definition 1. Let X denote a non-empty universal set and let $\tilde{F}$ be an FFS defined on X. A Fermatean Fuzzy Number (FFN) can be expressed as Eq. (1):

$$\tilde{F} \cong x, \mu_{\tilde{F}}(x), \nu_{\tilde{F}}(x); x \in X \tag{1}$$

where $\mu_{\tilde{F}}(x)$ and $\nu_{\tilde{F}}(x)$ denote the membership and non-membership degrees of element x, respectively, with both values belonging to the interval [0,1]. These degrees must satisfy the Eq. (2):

$$0 \leq \mu_{\tilde{F}}(x)^3, \nu_{\tilde{F}}(x)^3 \leq 1 \tag{2}$$

Furthermore, the degree of hesitancy, denoted by $\pi_{\tilde{F}}(x)$, quantifies the uncertainty associated with the assessment and is computed by Eq. (3):

$$\pi_{\tilde{F}}(x) = \sqrt[3]{1 - \left(\mu_{\tilde{F}}(x)\right)^3 + \left(v_{\tilde{F}}(x)\right)^3} \tag{3}$$

Definition 2. The score function of an FFN is defined by Eq. (4):

$$S(\tilde{\alpha}) = \mu_{\tilde{\alpha}}^3 - v_{\tilde{\alpha}}^3 \tag{4}$$

Where $(\tilde{\alpha}) = (\mu_{\tilde{\alpha}}, v_{\tilde{\alpha}})$.

Definition 3. The positive score function for an FFN is given by Eq. (5):

$$S^+(\tilde{\alpha}) = 1 + S(\tilde{\alpha}) = 1 + \mu_{\tilde{\alpha}}^3 - v_{\tilde{\alpha}}^3 \tag{5}$$

Definition 4. The aggregated operation of FFNs is determined by Eq. (6):

$$Z_i = Y(\mu_i, v_i) = \left(\prod_{t=1}^{d} (\mu_{it})^{\psi_t}, \sqrt[3]{1 - \prod_{t=1}^{d} (1 - (v_{it})^3)^{\psi_t}}\right), i = 1,2, \dots, n \tag{6}$$

where Z_i denotes the aggregated fermatean fuzzy evaluation of criterion i, n is the total number of criteria, d is the number of decision-makers, and ψ_t represents the weight assigned to decision-maker t and is obtained by Eq. (7):

$$\psi_t = \frac{S^+(E_t)}{\sum_{t=1}^{d} S^+(E_t)} = \frac{1 + \mu_t^3 - v_t^3}{\sum_{t=1}^{d} 1 + \mu_t^3 - v_t^3} \tag{7}$$

where $S^+(E_t)$ represents the positive score function associated with decision maker t.

3.2.2 FFS linguistic terms and corresponding FFNs

The linguistic variables and their corresponding FFNs employed in this study are presented as follows. Table 4 is utilized to evaluate the relative importance of experts.

Table 4.
Linguistic terms used to assess the relative importance of experts [114]

Linguistic term	Abbreviate	Corresponding FFNs	
		μ	ν
Very Qualified	VQ	0.95	0.10
Qualified	Q	0.75	0.30
Medium Qualified	MQ	0.55	0.50
Less Qualified	LQ	0.30	0.75
Very Less Qualified	VLQ	0.10	0.95

Table 5 is applied to prioritize influential dimensions on user privacy in smart cities.

Table 5.
Linguistic terms used to evaluate the criteria [115]

Linguistic term	Abbreviate	Corresponding FFNs	
		μ	ν
Extremely Unimportant / Very Low	EU / VL	0.1	0.975
Not Important / Low	N / L	0.2	0.85
Slightly Important / Medium Low	SI / ML	0.35	0.70
Moderately Important / Medium	MI / M	0.55	0.5
Important / Medium High	I / MH	0.7	0.35
Very Important / High	VI / H	0.85	0.2
Extremely Important / Very High	EI / VH	0.975	0.1

3.2.3 Steps of SWARA method

SWARA is a an MCDM method developed by [116] for determining the subjective weights of evaluation criteria. This method requires fewer pairwise comparisons among criteria, which reduces the complexity of the decision-making process [117]. To address uncertainty and vagueness in real-world decision environments, SWARA has been extended by integrating it with different fuzzy set theories, resulting in various fuzzy SWARA variants, including intuitionistic fuzzy SWARA, hesitant fuzzy SWARA, and Pythagorean fuzzy SWARA. In this study, the Fermatean Fuzzy SWARA (FF-SWARA) approach is employed to determine the relative importance weights of influential dimensions on user privacy in smart cities. The computational steps of the proposed FF-SWARA method are described as follows [114].

Step 1: Ranking criteria in descending order

The experts evaluate the importance of criteria by applying the linguistic terms presented in Table 5. These linguistic assessments are transformed into their corresponding FFNs and aggregated through Equations (6) and (7). Subsequently, Eq. (4) is employed to obtain the score value of each FFN associated with the criteria. Finally, the criteria are arranged in descending order based on their calculated score values.

Step 2: Determining the significance coefficient of each criterion

Beginning with the second-ranked criterion, experts assess the relative significance of each criterion in comparison with its previous criterion based on the obtained ranking sequence. Subsequently, the significance coefficient (k_i) for each criterion is calculated using Eq. (8):

$$k_i = \begin{cases} 1, i = 1 \\ S^{+}(i) + 1 \,, i > 1 \end{cases} \tag{8}$$

Where, $S^{+}(i)$ is the significant of criterion j compared to its previous criterion.

Step 3: Calculating the significance weight of each criterion

Based on the obtained values from Step 2, the significance weight of each criterion (q_i) is determined by Eq. (9):

$$q_i = \begin{cases} 1, i = 1 \\ \frac{q_{i-1}}{k_i}, i > 1 \end{cases} \tag{9}$$

Step 4: Determining the relative weight of each criterion

Using the results obtained in Step 3, the relative weight of each criterion (w_i) is calculated according to Eq. (10):

$$w_i = \frac{q_i}{\sum_{i=1}^{n} q_i} \tag{10}$$

3.3 Clustering Methods

Today, researchers are facing an overwhelming volume of data, necessitating the utilization of knowledge discovery tools. Machine learning models and data mining, as a sophisticated capability, plays a vital role in data analysis, the exploration of extensive datasets, and the process of knowledge discovery. Various methods have been developed to suit specific purposes, and one of the most significant machine learning techniques is clustering, which finds extensive application in knowledge discovery. Clustering involves the grouping of similar data based on inherent similarities. Through this classification and similarity assessment, concealed patterns within the dataset are unveiled. The identification of these patterns significantly streamlines data management for diverse applications [118]. Clustering falls within the realm of unsupervised learning methods, where the target database comprises unlabeled data. Unsupervised learning, in general, aims to discern meaningful structures or patterns for data categorization. Clustering, specifically, entails the task of partitioning a set of objects into distinct groups, each known as a cluster. Objects within the same cluster exhibit a high degree of similarity based on their characteristics, while the similarity between clusters is minimized. Consequently, the primary objective of clustering is to assign labels to objects signifying their membership in a specific cluster. This process is a fundamental component of exploratory data mining and represents a commonly employed technique for statistical data analysis across various fields, including pattern recognition and machine learning. Recommender systems are designed to generate descriptions of new items based on user preferences. In certain cases, clustering algorithms are used to forecast a user's preferences by capitalizing on the preferences of other users within the same cluster as the target user [119], [120].

In the clustering method for a dataset with *n* observations and *d* dimensions, assuming the required number of k clusters, the primary objective is to divide the data into *k* groups or clusters denoted as {c=C1, C2, C3, …, Ck}. Each cluster has a representative, typically referred to as μ_i, which is commonly known as the mean or center of the cluster, in this context:

$$\mu_i = \frac{1}{n} \sum_{x_j \in ci} x_j \tag{11}$$

And the exact number of possible modes for clustering *n* data in *k* clusters is as follows [121]:

$$S(n,k) = \frac{1}{k!}\sum_{t=0}^{k}(-1)^t \binom{k}{t} (k-t)^n \tag{12}$$

In this research, we applied clustering techniques to our dataset. To start, we collected data obtained in the initial stage using the meta-synthesis method and presented it to users in the form of nine dimensions. These nine dimensions were provided to them based on two main questions in the form of a questionnaire. First, we asked users to prioritize these dimensions based on their importance for privacy protection (i.e., "How do you prioritize the following dimensions to protect your privacy?"). Additionally, we provided users with a question to select the most crucial dimensions for privacy protection from their perspective (i.e., "In your opinion, which of the following dimensions is the most important for protecting your privacy?"). After gathering and processing the questionnaires, we transformed the responses into a specific index that encompassed data from 53 users (53 samples) and 9 features (dimensions). Subsequently, we conducted analyses using two clustering techniques: K-means and K-modes. In this stage, we assessed the significance of each factor according to user preferences and ranked them based on user prioritization.

3.3.1 K-means clustering

While many clustering algorithms share a common foundation, there are variations in how they measure similarity or distance and how they assign labels to the objects within each cluster. Some algorithms utilize Euclidean distance, while others prefer Manhattan or Minkowski distances. The k-means clustering technique is one such method. The k-means algorithm stands out as one of the simplest and most widely used clustering algorithms, particularly in the realm of unsupervised learning. In this context, we are working with multidimensional data, where each dimension is typically referred to as a feature or attribute. Given this diversity, the use of various distance functions is recommended. Some object characteristics may be quantitative, while others are qualitative. The k-means algorithm falls under the category of discriminative clustering methods, and its computational complexity is *O(ndk+1)*, where *n* represents the number of objects, *d* denotes the dimension of features, and *k* signifies the number of clusters. This method relies on the optimization of an objective function [122]. The K-means algorithm consists of the following steps, which are iterated until a certain condition is met:

1. Randomly select *k* points as the initial cluster centers. These points will serve as the initial centroids for the clusters.

2. Form *k* clusters by assigning each point (data) to the cluster whose center is closest, which is determined by calculating the distance between the point and the cluster centers. The point is assigned to the cluster with the smallest distance. Mathematically, the function that calculates the distance of point *x* from the centers of cluster *C*, where the *i-th* point belongs to the *j-th* cluster, is used.

$$x_i \in c_j | j = argmin_{i=1}^{k}\{\|x_j - \mu_i\|\} \tag{13}$$

3. After assigning points (data) to the clusters, compute the new centroids by calculating the average of points within each cluster. These new centroids become the updated centers of the clusters. The above steps are repeated until the distance between the centroids in consecutive iterations falls below a specified sensitivity level.

$$\sum_{i=1}^{k} \left\| {\mu_j}^{t} - {\mu_{j-1}}^{t-1} \right\|^2 \leq \varepsilon \tag{14}$$

To evaluate or validate the results of clustering, the Davies-Bouldin index can be employed, which is computed using the following formula:

$$D = \frac{min_{1 \leq i < j \leq n} d(i,j)}{max_{1 \leq k \leq n} d'(k)} \tag{15}$$

where:

- *n* is the number of clusters.
- *cx* is the center of cluster *x*.
- *σx* is the average distance of all elements in cluster *x*.
- *d(ci, cj)* is the distance between the centers *ci* and *cj* of clusters *i* and *j*, respectively.

The Davies-Bouldin index is structured to favor clustering algorithms that generate clusters with minimal intra-cluster distances, indicating high similarity within clusters, and high inter-cluster distances, indicating low similarity between clusters. A lower Davies-Bouldin index signifies superior clustering outcomes. Consequently, a clustering algorithm that produces clusters with the smallest Davies-Bouldin index is regarded as the best algorithm according to this criterion [121].

3.3.2 K-means clustering

In the real world, data can take various forms, including numerical and categorical data. While the k-Means clustering algorithm is a powerful tool for analyzing large datasets, it is primarily suited for numerical data and is not well-suited for data that includes specific categorical variables. To address this limitation, Huang (1998) introduced an algorithm known as k-Modes, designed to handle clustering with categorical data. KModes clustering is an unsupervised machine learning algorithm used for clustering categorical variables. Unlike KMeans, which relies on distance measures for continuous data, KModes is better equipped to deal with categorical data. In this algorithm, the concept of "distance" is replaced by the difference (overall fit) between data points. The smaller the differences between data points, the more similar they are considered. The mathematical relationship of this algorithm involves calculating the distance between two data points, *X* and *Y*, by counting the number of observations in *X* and *Y* with differing values. The formula for this distance measure is given as equation (18), and it assesses the dissimilarity between categorical data points. This makes it a suitable choice for clustering categorical data effectively [123].

$$d_1(X,Y) = \sum_{i=1}^{n} \delta(x_i, y_i) \tag{16}$$

where

$$\delta(X,Y) = \begin{cases} 0, x_i = y_i \\ 1, x_i \neq y_i \end{cases} \tag{17}$$

The value or significance of the *i-th* observation in the data *X*, denoted as *X_i*, and the value or significance of the *i-th* observation in the data *Y*, denoted as *Y_i*, are used in the formula for calculating the distance between two data points in the KModes algorithm. The value of *n* represents the total number of observations or data points in the dataset. Additionally, to determine the optimal value of k (the number of clusters) in the KModes algorithm, the following formula is employed. This formula is used to guide the selection of an appropriate number of clusters based on the characteristics of the data and the clustering objectives.

$$WCD = \sum_{j=1}^{k} \sum_{i=1}^{m} d_1(x_i, y_c) \tag{18}$$

Here, *WCD* is the within-cluster difference, *k* is the number of clusters, *m* is the number of observations in each cluster, *c* is the cluster centroid, and d_1 is the sample dissimilarity measure.

4. Results

4.1 FF-SWARA Results

This section presents the findings obtained from applying the FF-SWARA method to determine the relative importance of influential dimensions on user privacy in smart cities. Based on the results of the meta-synthesis phase, nine key dimensions were identified as the evaluation criteria. Table 6 presents these nine dimensions together with their corresponding criterion codes (C1–C9).

Table 6.
List of influential dimensions on user privacy and their corresponding codes

No.	Symbol	Dimensions
1	C1	Awareness and understanding
2	C2	Trust
3	C3	Self-Control and Customization
4	C4	Transparency
5	C5	Reference Standards, Frameworks, and Rules
6	C6	Data Management
7	C7	Security Requirements
8	C8	Risk and Risk Management
9	C9	Acceptance of Smart City Applications

Subsequently, the opinions of seven domain experts were collected using fermatean fuzzy linguistic variables, and the FF-SWARA approach was employed to calculate the relative weights of these dimensions under uncertainty. The demographic characteristics of the participating experts are summarized in Table 7.

Table 7.

Demographic profile of the participating experts

No.	Symbol	Academic Degree	Field of Expertise	Years of Experience
1	E1	Ph.D.	Knowledge Management	11
2	E2	MSc	Smart City Applications	14
3	E3	Ph.D.	Smart Cities and Knowledge Management	10
4	E4	Ph.D.	Decision-Making and Smart Systems	15
5	E5	MSc	Information Systems	13
6	E6	Ph.D.	Data Management and Privacy Protection	16
7	E7	MSc	Information Systems	9

Table 8 presents the experts' assessments of the identified dimensions using the linguistic variables provided in Table 4.

Table 8.
Relative importance of the participating experts

No.	Symbol	Linguistic terms assessment	Corresponding FFNs		Importance weights of experts
			μ	ν	
1	E1	Q	0.75	0.3	0.151
2	E2	Q	0.75	0.3	0.151
3	E3	MQ	0.55	0.5	0.113
4	E4	VQ	0.95	0.1	0.202
5	E5	MQ	0.55	0.5	0.113
6	E6	VQ	0.95	0.1	0.202
7	E7	LQ	0.3	0.75	0.065

After identifying the evaluation dimensions and assessing the participating experts, the FF-SWARA method was implemented to calculate the relative importance of the identified dimensions. The findings are presented in the following subsections according to the sequential steps of the FF-SWARA methodology.

Step 1: Ranking influential dimensions on user privacy in descending order

Industrial experts evaluated the importance of the identified dimensions using the linguistic terms provided in Table 5. The linguistic assessments are summarized in Table 9.

Table 9.
Experts' linguistic assessments of the identified dimensions

Symbol	Experts						
	E1	E2	E3	E4	E5	E6	E7
C1	N/L	SI/ML	N/L	MI/M	SI/ML	MI/M	SI/ML
C2	N/L	SI/ML	N/L	N/L	SI/ML	N/L	SI/ML
C3	SI/ML	MI/M	SI/ML	SI/ML	MI/M	MI/M	MI/M
C4	SI/ML	MI/M	SI/ML	MI/M	MI/M	MI/M	MI/M
C5	EI/VH	VI/H	I/MH	VI/H	EI/VH	VI/H	EI/VH
C6	VI/H	EI/VH	VI/H	EI/VH	VI/H	EI/VH	EI/VH
C7	EI/VH	VI/H	EI/VH	VI/H	EI/VH	EI/VH	EI/VH
C8	MI/M	I/MH	MI/M	I/MH	MI/M	I/MH	MI/M
C9	N/L	SI/ML	N/L	N/L	N/L	N/L	N/L

These assessments were subsequently transformed into their corresponding FFNs and aggregated across the seven experts using Equations (6) and (7). The aggregated FFNs were then converted into crisp values by applying Eq. (4). Based on the obtained crisp values, the influential dimensions on user privacy were prioritized, and the ranking results are presented in Table 10.

Table 10.
Crisp values and ranking of the identified dimensions

Symbol	E1		E2		…	E7		Aggregate		Crisp number	Rank
	μ	ν	μ	ν	…	μ	ν	μ	ν		
C1	0.2	0.85	0.35	0.7	…	0.35	0.7	0.36	0.71	0.69	7
C2	0.2	0.85	0.35	0.7	…	0.35	0.7	0.24	0.81	0.47	8
C3	0.35	0.7	0.55	0.5	…	0.55	0.5	0.45	0.62	0.85	6
C4	0.35	0.7	0.55	0.5	…	0.55	0.5	0.49	0.57	0.93	5
C5	0.97	0.1	0.85	0.2	…	0.97	0.1	0.87	0.21	1.65	3
C6	0.85	0.2	0.97	0.1	…	0.97	0.1	0.93	0.15	1.79	2
C7	0.97	0.1	0.85	0.2	…	0.97	0.1	0.93	0.15	1.80	1
C8	0.55	0.5	0.7	0.35	…	0.55	0.5	0.63	0.43	1.17	4
C9	0.2	0.85	0.35	0.7	…	0.2	0.85	0.22	0.83	0.43	9

Step 2: Determining the significance coefficient of each dimension

Following the prioritization of the dimensions in Step 1, the industrial experts evaluated the relative significance of each dimension with respect to its immediately preceding dimension in the ranking sequence. The pairwise comparisons were conducted using the linguistic scale presented in Table 5. The evaluation process began with a comparison between the second- and first-ranked dimension and proceeded sequentially until all adjacent dimensions had been assessed. The linguistic judgments provided by the experts were then converted into their corresponding FFNs and aggregated using Equations (6) and (7). Subsequently, the aggregated FFNs were transformed into crisp values by applying Eq. (4). Based on these crisp values, the significance coefficient (k_i) for each dimension was computed using Eq. (8).

Step 3: Calculating the significance weight of each dimension.

The significance weight (q_i) of each dimension is determined using Eq. (9).

Step 4: Determining the relative weight of each dimension.

In the last step, the relative weight (w_i) of each dimension is computed using Eq. (10). The results of the last three steps can be seen in Table 11.

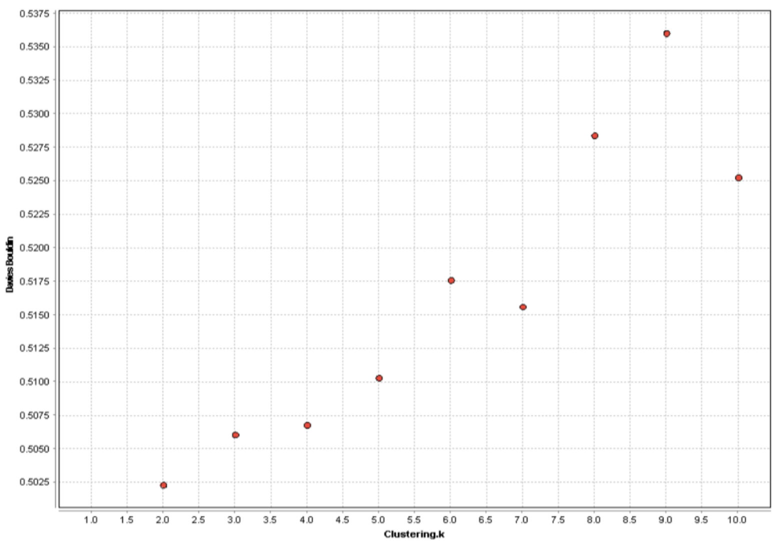
Table 11.
Crisp values and ranking of the identified dimensions

Symbol	Relative significance comparison with C_{i-1}	Fermatean linguistic terms	Aggregate		Crisp number	k_i	q_i	w_i
			μ	ν				
C7		-	-	-	-	1	1	0.385
C6	C7	N/L, N/L, N/L, N/L, N/L, MI/M, MI/M	0.26	0.80	0.50	1.50	0.67	0.257
C5	C6	I/MH, SI/ML, SI/ML, I/MH, SI/ML, MI/M, MI/M	0.50	0.57	0.94	1.94	0.34	0.132
C8	C5	N/L, N/L, MI/M, N/L, SI/ML, MI/M, SI/ML	0.30	0.77	0.58	1.58	0.22	0.084

C4	C8	N/L, SI/ML, N/L, N/L, SI/ML, SI/ML, SI/ML	0.27	0.79	0.53	1.53	0.14	0.055
C3	C4	N/L, N/L, SI/ML, N/L, N/L, N/L, N/L	0.21	0.84	0.42	1.42	0.10	0.038
C1	C3	I/MH, SI/ML, N/L, SI/ML, N/L, SI/ML, SI/ML	0.34	0.73	0.66	1.66	0.06	0.023
C2	C1	SI/ML, N/L, N/L, N/L, N/L, N/L, N/L	0.22	0.83	0.43	1.43	0.04	0.016
C9	C2	N/L, N/L, I/MH, N/L, SI/ML, MI/M, SI/ML	0.31	0.76	0.59	1.59	0.03	0.010

4.2 K-means Clustering Results

In order to implement the first approach, the data from the questionnaires for all users were collected and organized in an Excel file. The primary columns in this file included the user number and the user's evaluation of the importance of each dimension. The choice of the k-means algorithm for this approach was motivated by the suitability of the input matrix's dimensions and the desired output type for this method. The implementation of the k-means clustering algorithm was carried out using software tools like MATLAB and RapidMiner. An analytical comparison was conducted to determine the optimal values for k (the number of clusters) and the number of iterations. Through this analysis, it was found that the optimal value for *k* was 4, and the algorithm required 50 iterations to reach a stable solution. The algorithm's parameters were set according to these findings. Figure 4 in the research presentation illustrates the optimal value of *k*, which was determined through this process.



Loop Parameters (10 rows, 3 columns)

iteration	Clusteri...	Davies Bouldin
2	2	0.502
1	1	?
5	5	0.510
3	3	0.506
6	6	0.518
7	7	0.516
10	10	0.525
4	4	0.507
9	9	0.536
8	8	0.528

Fig. 4. The number of *k* obtained and the selection of the optimal *k*

Once the optimal parameters were determined, the k-means clustering algorithm was implemented with these settings. As a result, users were grouped into 4 clusters based on their varying degrees of importance assigned to their privacy. The output of this clustering process provided the results and the center of each category, as detailed in Table 12. This categorization allowed users to be placed into distinct clusters according to their individual privacy preferences and priorities.

Table 12.
Clustering of users

Attribute	Cluster_0	Cluster_1	Cluster_2	Cluster_3
User	34	7	20.500	46.500
Points	0.874	1.029	1.401	0.541

Also, this clustering is displayed on the graph in Figure 5 with different colors and coordinates of each user.

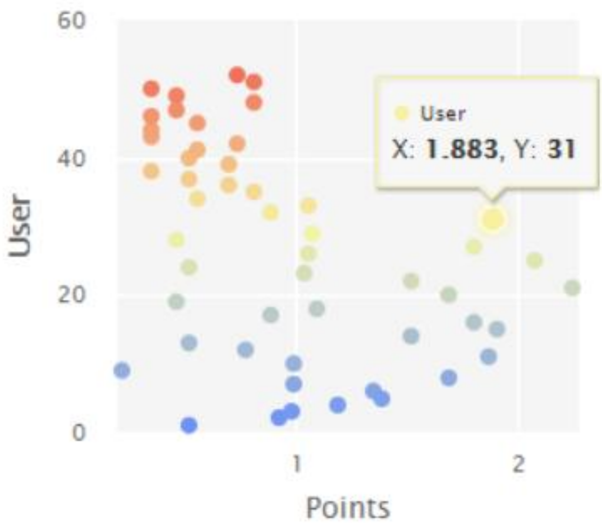


Fig. 5. Clustering of users and the placement of users in different clusters

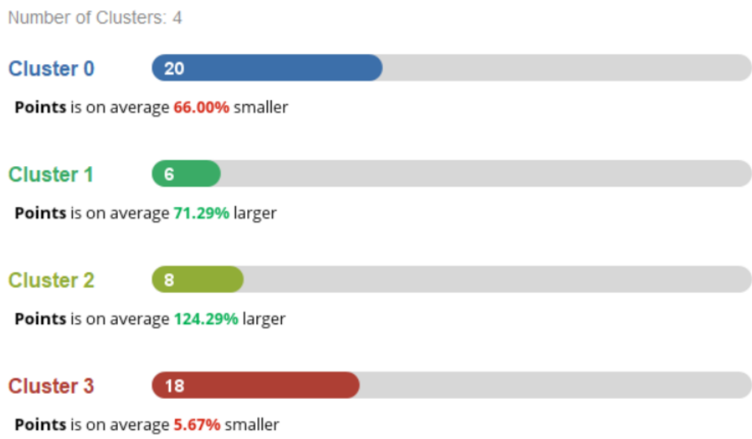


Fig. 6. Number of users in each cluster

Based on the output of this analysis, developers in each smart city can effectively cluster the citizens according to their security needs and privacy considerations, as assessed through surveys and questionnaires. By categorizing citizens into different clusters based on their privacy preferences and priorities, developers can tailor personalized suggestions and solutions for each cluster. This approach allows for the customization of privacy-enhancing recommendations that align with the specific desires and requirements of each group of citizens. It enables a more targeted and effective strategy for improving privacy and security in a smart city environment, ultimately enhancing the overall quality of life and satisfaction of its residents.

4.2 K-modes Clustering Results

In this study, the choice of the K-Modes algorithm was driven by the type of data, which includes both numerical data and categorical variables. Initially, it was calculated the optimal value for *k* (the number of clusters) for a dataset comprising 53 samples, and the resulting clusters are illustrated in Figure 7. The optimal number of clusters for this dataset is 4. It's observed that having 2 or 3 clusters increases the cost and doesn't yield significant efficiency improvements. Beyond *k=4*, the cost-optimality gradient becomes less pronounced, and there isn't a substantial difference between having 4 clusters and increasing it to 8 clusters. Increasing the number of clusters beyond a certain point can lead to less optimal and less efficient sample (user) clustering. Therefore, it was chosen the middle ground of 4 clusters as the optimal choice, balancing effectiveness and efficiency in the clustering of samples.

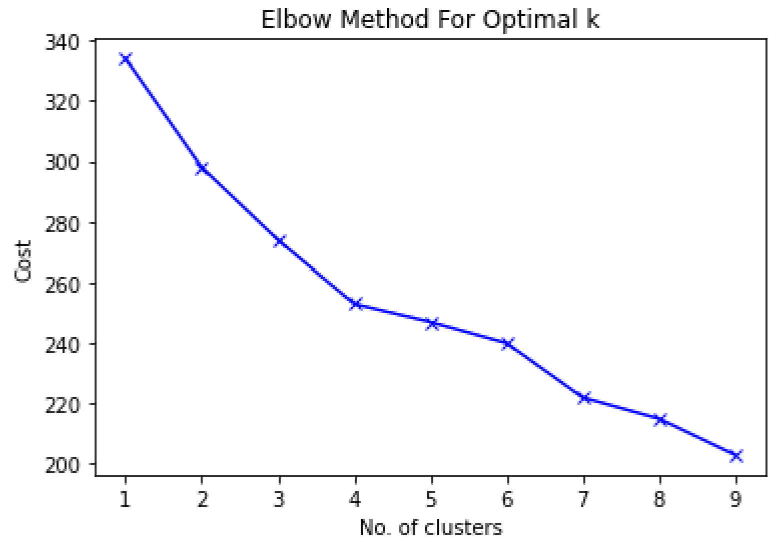


Fig. 7. Optimal k value in K-modes algorithm

The analysis of the results of this algorithm on the samples shows that the number of optimal clusters is equal to 4. Figure 8 shows the number of users in each cluster.

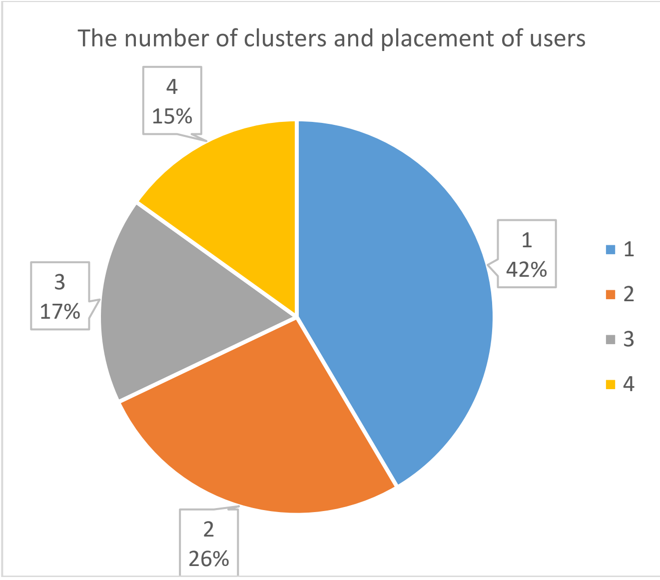


Fig. 8. Clustering of users based on the K-modes algorithm and the number of users in each cluster

In the first cluster, which includes the largest number of users (22 out of 53), the findings indicate that 15 users prioritize dimensions related to reference standards, frameworks, and rules as their first to third priorities for safeguarding their privacy. Additionally, 12 users have acknowledged that security requirements are among their top three priorities, while 10 users consider transparency as an important aspect within their first to third priorities for protecting their privacy. Moving on to the second cluster, which consists of 14 users, 12 of them prioritize both transparency and trust as their top three priorities. Furthermore, 9 users in this cluster consider awareness and understanding as their primary concerns for maintaining privacy.

In the third cluster, comprising 9 users, 8 of them place transparency as one of their top three priorities for safeguarding their privacy. Additionally, 5 users within this cluster prioritize dimensions such as reference standards, frameworks, and rules, as well as self-control and customization, as their top three priorities. Finally, in the fourth cluster, which includes 8 users, 6 individuals emphasize data management and control as one of their three most important priorities for protecting their privacy. Furthermore, 4 users consider security requirements and awareness and understanding as their top priorities for privacy protection in the context of the smart city. An analysis of the above results reveals that transparency is the most significant dimension for smart city users when it comes to protecting their privacy. This dimension consistently ranks among the first to third priorities across various clusters. Following transparency, "security requirements," " reference standards, frameworks, and rules," and "awareness and understanding" emerge as the top three priorities for users in different clusters.

To provide an integrated view of the study, Figure 9 presents a schematic overview of the research findings. It summarizes the proposed knowledge management-based framework by illustrating the sequential stages of the research, including knowledge acquisition through meta-synthesis, expert evaluation using FF-SWARA, knowledge sharing and application based on the SECI model, user clustering, and the resulting practical outcomes for smart city user privacy preservation.

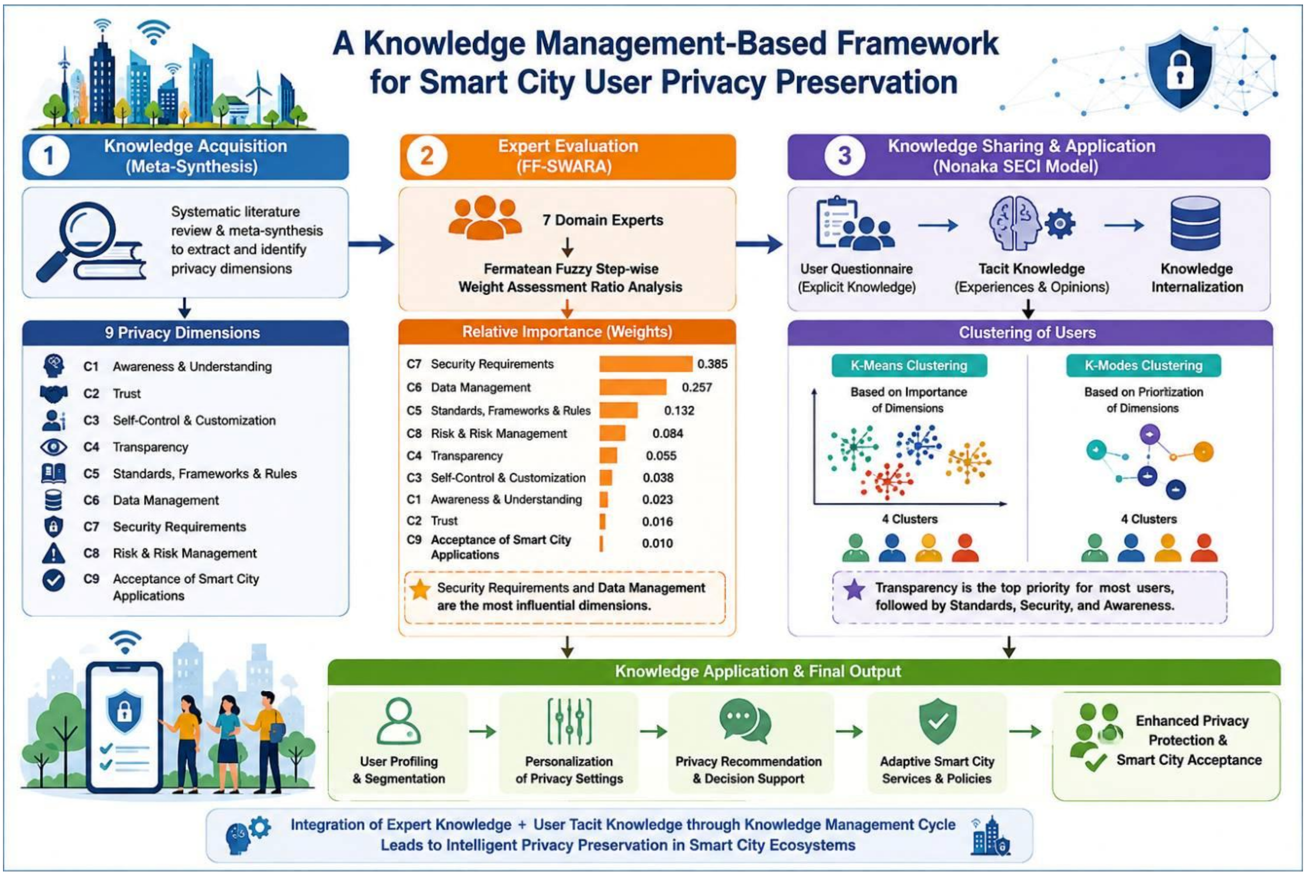


Fig. 9. Integrated framework of the proposed approach and research findings.

5. Conclusion

With the advent of the age of information and the rise of digital technologies, the concept of the smart city stands out as one of the most innovative and influential developments in this transformative era. It has introduced a multitude of initiatives and advantages for its users. In this context, users actively participate in these initiatives and reap their advantages, while a substantial volume of data and information is consistently collected, stored, processed, and utilized. A critical concern that significantly influences the acceptance of smart city initiatives is the preservation of user security and privacy, especially their personal data. To tackle these concerns, it is imperative to put in place specific measures during the implementation of smart city initiatives. Among these measures is the identification and evaluation of factors and indicators that affect user privacy within the smart city ecosystem. Recognizing these factors and deriving insights from them serves as the basis for making informed decisions and effectively safeguarding user privacy. To acquire this vital knowledge, it is imperative to manage and collect data, information, and explicit knowledge in line with the overarching context. This study employs a two-step approach to identify these factors and extract valuable insights from them.

Prior to commencing the steps based on Wiig's knowledge management cycle (knowledge creation and acquisition, knowledge integration and sharing, as well as application and utilization of knowledge), this study aims to investigate the knowledge collected across all three stages of knowledge management and how this knowledge, comprising both explicit and latent knowledge, is stored and utilized to create a new knowledge model. This process also seeks to understand how acquired knowledge and creativity should be disseminated and ultimately put into practice. To address the above questions, the initial step involved the extraction, acquisition, and identification of dimensions influencing user privacy. This process was carried out through the meta-synthesis approach, yielding 9 acquired dimensions: "Awareness and Understanding" (C1), "Trust" (C2), "Self-Control and Customization" (C3), "Transparency" (C4), "Reference Standards, Frameworks, and Rules" (C5), "Data Management" (C6), "Security Requirements" (C7), "Risk and Risk Management" (C8), and "Acceptance of Smart City Applications" (C9).

In the second step, the relative importance of these identified dimensions was determined using the FF-SWARA method, based on the judgments of seven domain experts. This approach effectively captured the uncertainty inherent in experts' assessments. The findings revealed that Security Requirements (C7) emerged as the most influential dimension affecting user privacy with a weight of 0.385, followed by Data Management (C6) with a weight of 0.257, Reference Standards, Frameworks, and Rules (C5) with a weight of 0.132, Risk and Risk Management (C8) with a weight of 0.084, Transparency (C4) with a weight of 0.055, Self-Control and Customization (C3) with a weight of 0.038, Awareness and Understanding (C1) with a weight of 0.023, Trust (C2) with a weight of 0.016, and Acceptance of Smart City Applications (C9) with a weight of 0.010. The dominance of security requirements and data management underscores the critical importance of robust technical safeguards and proper data governance in smart city ecosystems.

In the third step, the findings from the first step were shared with smart city users through a questionnaire, following Nonaka and Takeuchi's theory and the knowledge creation cycle. This explicit knowledge was shared among users to extract tacit knowledge, experiences, and opinions. The output of this stage was considered as input for the knowledge application stage. Here, clustering techniques were employed to analyze and extract tacit knowledge from users, categorizing it into specific groups and clusters. This knowledge was then utilized for personalization and profiling of other users, becoming internalized. In this step, two clustering techniques, K-means, and K-modes, were employed for different purposes. K-means was used to cluster users based on the importance of dimensions in safeguarding their privacy. The results revealed the significance of the set of dimensions for each user, resulting in users being grouped into 4 clusters based on their assigned scores. Users in the first cluster found these dimensions very important, suggesting that smart city developers should consider additional dimensions to address their needs. Conversely, users in the fourth cluster attached less importance to these dimensions, allowing developers to take suitable actions to address their concerns.

K-modes, on the other hand, was used to cluster users based on the prioritization of relevant dimensions according to their preferences and opinions. The analysis showed that users were clustered into 4 groups based on the similarity and priority of their dimension categorization. Cluster 1 exhibited the highest similarity in categorizing users, representing 42% of the total, indicating the most common categorization among users. The overall clustering results indicated that the "transparency" dimension ranked among the top 3 priorities for users in all clusters, followed by dimensions such as " reference standards, frameworks, and rules," "security requirements," and "awareness and understanding" in the priorities of other users. Notably, while the FF SWARA expert analysis placed security requirements as the most critical dimension, the user clustering revealed that transparency was the most frequently prioritized dimension among end users. This divergence highlights an important gap between expert and user perspectives, suggesting that citizens may value clear and open communication about data practices even more than technical security measures.

This clustering indicates that knowledge obtained from users' implicit knowledge can be applied to profiling, personalization, and future user recommendations. It can provide a suitable outcome and application for preserving their privacy and making relevant suggestions. The integration of the FF-SWARA results with the clustering outcomes creates a comprehensive knowledge framework: the expert-driven weights inform the design of privacy policies and technical infrastructures, while the user-driven clusters guide the customization of privacy interfaces and communication strategies. This dual approach ensures that both technical robustness and user-centricity are addressed in smart city privacy preservation efforts.

Within the scope of this study, one of the limitations lies in the relatively small number of participants or the restricted sample size. This limitation might affect the extent to which the research findings can be generalized, and the broader applicability of the knowledge framework developed for safeguarding smart city user privacy. Also, the following suggestions align with the discoveries made in this study and offer insights into potential avenues for future research:

- **Ethical Frameworks for Smart Cities**: As this study mentions the importance of laws and frameworks, future research could delve into the development of comprehensive ethical frameworks specific to smart city environments.
- **User-Centric Design and Customization**: Building on clustering analysis and FF SWARA findings, further research can explore the development of user centric smart city systems that adapt to individual preferences and privacy concerns. This may involve AI driven customization and personalization and the development of user-friendly interfaces that allow users to customize their data sharing settings based on their cluster membership.
- **Long-term User Trust and Engagement**: Investigating how trust and engagement with smart city initiatives evolve over time. Longitudinal studies could track user attitudes, behaviors, and concerns as they interact with these technologies, helping policymakers and developers adapt to changing user needs.
- **User-Generated Data Governance**: Researching how smart cities can involve citizens in the governance of the data they generate. This participatory approach could lead to more transparent and user-friendly data management systems.
- **Legal and Regulatory Challenges**: Investigate the legal and regulatory challenges that may hinder the protection of user privacy in smart cities, with particular attention to how different regulatory frameworks (such as GDPR) interact with user expectations and expert identified priorities.
- **Comparative Studies**: Future research could compare the relative importance of privacy dimensions across different smart city contexts, cultures, and geographical regions, using the FF SWARA methodology to understand how contextual factors influence both expert and user perceptions of privacy requirements.

Author Contributions

Author Contributions: Conceptualization, M.Z.N. and M.M.; methodology (meta-synthesis and clustering), M.Z.N., M.M., and A.Z.; methodology (FF-SWARA), J.N.-J. and T.S.; software, M.Z.N. and T.S.; validation, M.Z.N., A.Z., J.N.-J., and T.S.; formal analysis, M.Z.N., A.Z., and J.N.-J.; investigation, A.Z., and T.S.; resources, M.M. and J.N.-J.; data curation, M.Z.N., A.Z., and T.S.; writing—original draft preparation, A.Z., and J.N.-J.; writing—review and editing, M.Z.N. and T.S.; visualization, M.Z.N. and J.N.-J.; supervision, M.M. and J.N.-J.; project administration, M.Z.N. and J.N.-J. All authors have read and agreed to the published version of the manuscript.

Funding
This research received no external funding

Conflicts of Interest
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement
This research was not funded by any grant.

References

[1] Ghazal, Taher M., Mohammad Kamrul Hasan, Haitham M. Alzoubi, Muhammad Alshurideh, Munir Ahmad, and Syed Shehryar Akbar. 2023. "Internet of Things Connected Wireless Sensor Networks for Smart Cities." Pp. 1953–68 in *The Effect of Information Technology on Business and Marketing Intelligence Systems*. Springer. https://doi.org/10.1007/978-3-031-12382-5_107

[2] Pramanik, Sabyasachi, Digvijay Pandey, Subhankar Joardar, M. Niranjanamurthy, Binay Kumar Pandey, and Jaspinder Kaur. 2023. "An Overview of IoT Privacy and Security in Smart Cities." in *AIP Conference Proceedings*. Vol. 2495. https://doi.org/10.1063/5.0123511

[3] Banciu, Claudia, and Adrian Florea. 2026. "AIoT at the Frontline of Climate Change Management: Enabling Resilient, Adaptive, and Sustainable Smart Cities." *Climate* 14(1):19. https://doi.org/10.3390/cli14010019

[4] Novotn\`y, Radovan, Radek Kuchta, and Jaroslav Kadlec. 2014. "Smart City Concept, Applications and Services." *Journal of Telecommunications System & Management* 3(2):1–5. https://doi.org/10.4172/2167-0919.1000117

[5] Dameri, Renata Paola. 2013. "Searching for Smart City Definition: A Comprehensive Proposal." *International Journal of Computers & Technology* 11(5):2544–51. https://doi.org/10.24297/ijct.v11i5.1142

[6] Zhang, K., J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen. 2017. "Security and Privacy in Smart City Applications: Challenges and Solutions." *IEEE Communications Magazine* 55(1):122–29. doi: 10.1109/MCOM.2017.1600267CM. https://doi.org/10.1109/MCOM.2017.1600267CM

[7] Manshour, Shiva, and Steffen Lehmann. 2026. "A Systematic Review of Passive Cooling Strategies Integrating Traditional Wisdom and Modern Innovations for Sustainable Development in Arid Urban Environments." *Discover Cities* 3(1):42. https://doi.org/10.1007/s44327-026-00204-4

[8] Wiig, Karl M. 1994. *Knowledge Management Foundations: Thinking about Thinking-How People and Organizations Represent, Create, and Use Knowledge*. Schema Press, Limited.

[9] Von Krogh, Georg, Kazuo Ichijo, Ikujiro Nonaka, and others. 2000. *Enabling Knowledge Creation: How to Unlock the Mystery of Tacit Knowledge and Release the Power of Innovation*. Oxford University Press on Demand.

[10] Zareeihemat, Pourya, Samira Mohamadi, Jamal Valipour, and Seyed Vahid Moravvej. 2025. "Forecasting Stock Market Volatility Using Housing Market Indicators: A Reinforcement

Learning-Based Feature Selection Approach." *IEEe Access* 13:52621–43. https://doi.org/10.1109/ACCESS.2025.3554224

[11] Israilidis, John, Kayode Odusanya, and Muhammad Usman Mazhar. 2021. "Exploring Knowledge Management Perspectives in Smart City Research: A Review and Future Research Agenda." *International Journal of Information Management* 56:101989. https://doi.org/10.1016/j.ijinfomgt.2019.07.015

[12] de Borba, Darci, Rosiane Alves Palacios, Edimara Mezzomo Luciano, and Marcirio Silveira Chaves. 2020. "The Contribution of Knowledge Management to Smart Cities for Innovation: Proposal for a Prescriptive Framework and a Research Agenda." *International Journal of Innovation* 8(3):516–40. https://doi.org/10.5585/iji.v8i3.18543

[13] Roblek, Vasja, and Maja Meško. 2020. "Smart City Knowledge Management: Holistic Review and the Analysis of the Urban Knowledge Management." Pp. 52–60 in *The 21st Annual International Conference on Digital Government Research*. https://doi.org/10.1145/3396956.3398263

[14] Abdoli Mohamadabadi, Tayebeh, Mahmood Ahmadpour Daryani, Asef Karimi, and Zohreh Amiri Sardari. 2024. "A Conceptual Model for Antecedents of Dynamic Capability Development in New Ventures (Case Study: IT Business)." *Interdisciplinary Journal of Management Studies* 17(2):625–38. https://doi.org/10.22059/ijms.2023.348938.675388

[15] Laurini, Robert. 2021. "A Primer of Knowledge Management for Smart City Governance." *Land Use Policy* 111:104832. https://doi.org/10.1016/j.landusepol.2020.104832

[16] Asadzadeh, S., O. Rahmani Seryasat, and S. Moshrefzadeh. 2018. "Intelligent Transportation in the Prevention of Accidents." *Transactions on Machine Intelligence* 1(1):49–56. https://doi.org/10.47176/TMI.2018.49

[17] Abdalla, Wala, Suresh Renukappa, and Subashini Suresh. 2023. "Managing COVID-19-Related Knowledge: A Smart Cities Perspective." *Knowledge and Process Management* 30(1):87–109. https://doi.org/10.1002/kpm.1706

[18] Chang, Daniel Lage, Jamile Sabatini-Marques, Eduardo Moreira Da Costa, Paulo Mauricio Selig, and Tan Yigitcanlar. 2018. "Knowledge-Based, Smart and Sustainable Cities: A Provocation for a Conceptual Framework." *Journal of Open Innovation: Technology, Market, and Complexity* 4(1):5. https://doi.org/10.1186/s40852-018-0087-2

[19] Sandelowski, Margarete, and Julie Barroso. 2006. *Handbook for Synthesizing Qualitative Research*. springer publishing company.

[20] Sandelowski, Margarete, Julie Barroso, and Corrine I. Voils. 2007. "Using Qualitative Metasummary to Synthesize Qualitative and Quantitative Descriptive Findings." *Research in Nursing & Health* 30(1):99–111. https://doi.org/10.1002/nur.20176

[21] Ullah, Fahim, Siddra Qayyum, Muhammad Jamaluddin Thaheem, Fadi Al-Turjman, and Samad M. E. Sepasgozar. 2021. "Risk Management in Sustainable Smart Cities Governance: A TOE Framework." *TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE* 167. doi: 10.1016/j.techfore.2021.120743.

[22] Wiencierz, Christian, and Marco Luenich. n.d. "Trust in Open Data Applications through Transparency." *NEW MEDIA & SOCIETY*. doi: 10.1177/1461444820979708

[23] Vasileva, Roza, Lucelia Rodrigues, Nancy Hughes, Chris Greenhalgh, Murray Goulden, and Jeni Tennison. 2018. "What Smart Campuses Can Teach Us about Smart Cities: User Experiences and Open Data." *INFORMATION* 9(10). doi: 10.3390/info9100251.

[24] Bernal Bernabe, J., J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A.

Skarmeta. 2019. "Privacy-Preserving Solutions for Blockchain: Review and Challenges." *IEEE Access* 7:164908–40. doi: 10.1109/ACCESS.2019.2950872.

[25] Anisetti, M., C. Ardagna, V. Bellandi, M. Cremonini, F. Frati, and E. Damiani. 2018. "Privacy-Aware Big Data Analytics as a Service for Public Health Policies in Smart Cities." *Sustainable Cities and Society* 39:68–77. doi: 10.1016/j.scs.2017.12.019.

[26] Eckhoff, D., and I. Wagner. 2018. "Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions." *IEEE Communications Surveys and Tutorials* 20(1):489–516. doi: 10.1109/COMST.2017.2748998.

[27] Hernandez-Ramos, J. L., J. A. Martinez, V. Savarino, M. Angelini, V. Napolitano, A. F. Skarmeta, and G. Baldini. 2021. "Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and Future Directions." *IEEE Security and Privacy* 19(1):12–23. doi: 10.1109/MSEC.2020.3012353.

[28] Lytras, Miltiadis D., and Anna Visvizi. 2018. "Who Uses Smart City Services and What to Make of It: Toward Interdisciplinary Smart Cities Research." *SUSTAINABILITY* 10(6). doi: 10.3390/su10061998.

[29] Abi Sen, A. A., F. A. Eassa, K. Jambi, and M. Yamin. 2018. "Preserving Privacy in Internet of Things: A Survey." *International Journal of Information Technology (Singapore)* 10(2):189–200. doi: 10.1007/s41870-018-0113-4.

[30] Khatoun, R., and S. Zeadally. 2017. "Cybersecurity and Privacy Solutions in Smart Cities." *IEEE Communications Magazine* 55(3):51–59. doi: 10.1109/MCOM.2017.1600297CM.

[31] Javed, M. A., E. B. Hamida, and W. Znaidi. 2016. "Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice." *Sensors (Switzerland)* 16(6). doi: 10.3390/s16060879.

[32] Li, Yibin, Wenyun Dai, Zhong Ming, and Meikang Qiu. 2016. "Privacy Protection for Preventing Data Over-Collection in Smart City." *IEEE TRANSACTIONS ON COMPUTERS* 65(5):1339–50. doi: 10.1109/TC.2015.2470247.

[33] Julsrud, Tom Erik, and Julie Runde Krogstad. 2020. "Is There Enough Trust for the Smart City? Exploring Acceptance for Use of Mobile Phone Data in Oslo and Tallinn." *TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE* 161. doi: 10.1016/j.techfore.2020.120314.

[34] Hassan, A. M., and A. I. Awad. 2018. "Urban Transition in the Era of the Internet of Things: Social Implications and Privacy Challenges." *IEEE Access* 6:36428–40. doi: 10.1109/ACCESS.2018.2838339.

[35] Butot, Vivien, Petra Saskia Bayerl, Gabriele Jacobs, and Freek de Haan. 2020. "Citizen Repertoires of Smart Urban Safety: Perspectives from Rotterdam, the Netherlands." *TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE* 158. doi: 10.1016/j.techfore.2020.120164.

[36] Hou, Jinghui (Jove), Laura Arpan, Yijie Wu, Richard Feiock, Eren Ozguven, and Reza Arghandeh. 2020. "The Road toward Smart Cities: A Study of Citizens' Acceptance of Mobile Applications for City Services." *ENERGIES* 13(10). doi: 10.3390/en13102496.

[37] Elahi, Haroon, Guojun Wang, Tao Peng, and Jianer Chen. 2019. "On Transparency and Accountability of Smart Assistants in Smart Cities." *APPLIED SCIENCES-BASEL* 9(24). doi: 10.3390/app9245344.

[38] Habib, Abdulrahman, Duha Alsmadi, and Victor R. Prybutok. 2020. "Factors That Determine Residents' Acceptance of Smart City Technologies." *BEHAVIOUR & INFORMATION TECHNOLOGY* 39(6, SI):610–23. doi: 10.1080/0144929X.2019.1693629.

[39] Kalloniatis, Christos, Dimitris Kavroudakis, Amalia Polidoropoulou, and Stefanos Gritzalis. 2019. "Designing Privacy-Aware Intelligent Transport Systems: A Roadmap for Identifying the Major Privacy Concepts." *INTERNATIONAL JOURNAL OF APPLIED GEOSPATIAL RESEARCH* 10(1):73–91. doi: 10.4018/IJAGR.2019010104.

[40] de Wijs, Lisanne, Patrick Witte, and Stan Geertman. 2016. "How Smart Is Smart? Theoretical and Empirical Considerations on Implementing Smart City Objectives - a Case Study of Dutch Railway Station Areas." *INNOVATION-THE EUROPEAN JOURNAL OF SOCIAL SCIENCE RESEARCH* 29(4):424–41. doi: 10.1080/13511610.2016.1201758.

[41] Belanche, Daniel, Luis V Casalo-Arino, and Alfredo Perez-Rueda. 2015. "Determinants of Multi-Service Smartcard Success for Smart Cities. Development: A Study Based on Citizens' Privacy and Security Perceptions." *GOVERNMENT INFORMATION QUARTERLY* 32(2):154–63. doi: 10.1016/j.giq.2014.12.004.

[42] Sánchez Alcón, J. A., L. López, J. F. Martínez, and G. R. Cifuentes. 2015. "Trust and Privacy Solutions Based on Holistic Service Requirements." *Sensors (Switzerland)* 16(1). doi: 10.3390/s16010016.

[43] Kumar, P., G. P. Gupta, and R. Tripathi. 2021. "TP2SF: A Trustworthy Privacy-Preserving Secured Framework for Sustainable Smart Cities by Leveraging Blockchain and Machine Learning." *Journal of Systems Architecture* 115. doi: 10.1016/j.sysarc.2020.101954.

[44] Cottrill, C. D., N. Jacobs, M. Markovic, and P. Edwards. 2020. "Sensing the City: Designing for Privacy and Trust in the Internet of Things." *Sustainable Cities and Society* 63. doi: 10.1016/j.scs.2020.102453.

[45] Chatterjee, S. 2020. "The Safety of IoT-Enabled System in Smart Cities of India: Do Ethics Matter?" *International Journal of Ethics and Systems* 36(4):601–18. https://doi.org/10.1108/IJOES-05-2019-0085

[46] Chatterjee, Sheshadri, and Arpan Kumar Kar. 2018. "Effects of Successful Adoption of Information Technology Enabled Services in Proposed Smart Cities of India: From User Experience Perspective." *JOURNAL OF SCIENCE AND TECHNOLOGY POLICY MANAGEMENT* 9(2, SI):189–209. https://doi.org/10.1108/JSTPM-03-2017-0008.

[47] Braun, T., B. C. M. Fung, F. Iqbal, and B. Shah. 2018. "Security and Privacy Challenges in Smart Cities." *Sustainable Cities and Society* 39:499–507. https://doi.org/10.1016/j.scs.2018.02.039.

[48] Alandjani, G. 2018. "Features and Potential Security Challenges for IoT Enabled Devices in Smart City Environment." *International Journal of Advanced Computer Science and Applications* 9(8):231–38. https://doi.org/10.14569/ijacsa.2018.090830.

[49] Yeh, Hsiaoping. 2017. "The Effects of Successful ICT-Based Smart City Services: From Citizens' Perspectives." *GOVERNMENT INFORMATION QUARTERLY* 34(3):556–65. https://doi.org/10.1016/j.giq.2017.05.001.

[50] Beltran, V., A. F. Skarmeta, and P. M. Ruiz. 2017. "An ARM-Compliant Architecture for User Privacy in Smart Cities: SMARTIE-Quality by Design in the IoT." *Wireless Communications and Mobile Computing* 2017. https://doi.org/10.1155/2017/3859836.

[51] Khan, Z., Z. Pervez, and A. G. Abbasi. 2017. "Towards a Secure Service Provisioning Framework in a Smart City Environment." *Future Generation Computer Systems* 77:112–35. https://doi.org/10.1016/j.future.2017.06.031.

[52] Avgerou, Artemis, Panayotis E. Nastou, Dimitra Nastouli, Panos M. Pardalos, and Yannis C. Stamatiou. 2016. "On the Deployment of Citizens' Privacy Preserving Collective Intelligent EBusiness Models in Smart Cities." *INTERNATIONAL JOURNAL OF SECURITY AND*

ITS APPLICATIONS 10(2):171–84. https://doi.org/10.14257/ijsia.2016.10.2.16.

[53] Ahmed, S. 2020. "Security and Privacy in Smart Cities: Challenges and Opportunities." *International Journal of Engineering Trends and Technology* 68(2):1–8. https://doi.org/10.14445/22315381/IJETT-V68I2P201.

[54] Moustaka, V., Z. Theodosiou, A. Vakali, A. Kounoudes, and L. G. Anthopoulos. 2019. "Enhancing Social Networking in Smart Cities: Privacy and Security Borderlines." *Technological Forecasting and Social Change* 142:285–300. https://doi.org/10.1016/j.techfore.2018.10.026.

[55] Cui, L., G. Xie, Y. Qu, L. Gao, and Y. Yang. 2018. "Security and Privacy in Smart Cities: Challenges and Opportunities." *IEEE Access* 6:46134–45. https://doi.org/10.1109/ACCESS.2018.2853985.

[56] Elahi, Haroon, Aniello Castiglione, Guojun Wang, and Oana Geman. 2021. "A Human-Centered Artificial Intelligence Approach for Privacy Protection of Elderly App Users in Smart Cities." *NEUROCOMPUTING* 444:189–202. https://doi.org/10.1016/j.neucom.2020.06.149.

[57] Omar, A. A., A. K. Jamil, A. Khandakar, A. R. Uzzal, R. Bosri, N. Mansoor, and M. S. Rahman. 2021. "A Transparent and Privacy-Preserving Healthcare Platform with Novel Smart Contract for Smart Cities." *IEEE Access* 9:90738–49. https://doi.org/10.1109/ACCESS.2021.3089601.

[58] Sookhak, M., H. Tang, Y. He, and F. R. Yu. 2019. "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges." *IEEE Communications Surveys and Tutorials* 21(2):1718–43. https://doi.org/10.1109/COMST.2018.2867288.

[59] Martinez, Juan A., Jose L. Hernandez-Ramos, Victoria Beltran, Antonio Skarmeta, and Pedro M. Ruiz. 2017. "A User-Centric Internet of Things Platform to Empower Users for Managing Security and Privacy Concerns in the Internet of Energy." *INTERNATIONAL JOURNAL OF DISTRIBUTED SENSOR NETWORKS* 13(8). https://doi.org/10.1177/1550147717727974.

[60] Fernandez, Javier D., Marta Sabou, Sabrina Kirrane, Elmar Kiesling, Fajar J. Ekaputra, Amr Azzam, and Rigo Wenning. 2020. "User Consent Modeling for Ensuring Transparency and Compliance in Smart Cities." *PERSONAL AND UBIQUITOUS COMPUTING* 24(4, SI):465–86. https://doi.org/10.1007/s00779-019-01330-0.

[61] Makhdoom, Imran, Ian Zhou, Mehran Abolhasan, Justin Lipman, and Wei Ni. 2020. "PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities." *COMPUTERS & SECURITY* 88. https://doi.org/10.1016/j.cose.2019.101653.

[62] Daoudagh, S., E. Marchetti, V. Savarino, J. B. Bernabe, J. García-Rodríguez, R. T. Moreno, J. A. Martinez, and A. F. Skarmeta. 2021. "Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal." *Sensors* 21(21). https://doi.org/10.3390/s21217154.

[63] Singh, S. K., Y. S. Jeong, and J. H. Park. 2020. "A Deep Learning-Based IoT-Oriented Infrastructure for Secure Smart City." *Sustainable Cities and Society* 60. https://doi.org/10.1016/j.scs.2020.102252.

[64] Lupi, Lucia. 2019. "City Data Plan: The Conceptualisation of a Policy Instrument for Data Governance in Smart Cities." *URBAN SCIENCE* 3(3). doi: 10.3390/urbansci3030091.

[65] Abosaq, Nasser H. 2019. "Impact of Privacy Issues on Smart City Services in a Model Smart City." *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS* 10(2):177–85.

[66] Badii, Claudio, Pierfrancesco Bellini, Angelo Difino, and Paolo Nesi. 2020. "Smart City IoT Platform Respecting GDPR Privacy and Security Aspects." *IEEE ACCESS* 8:23601–23.

https://doi.org/10.1109/ACCESS.2020.2968741.

[67] Bennati, Stefano, Ivana Dusparic, Rhythima Shinde, and Catholijn M. Jonker. 2018. "Volunteers in the Smart City: Comparison of Contribution Strategies on Human-Centered Measures." *SENSORS* 18(11). https://doi.org/10.3390/s18113707.

[68] Shaffer, G. 2021. "Applying a Contextual Integrity Framework to Privacy Policies for Smart Technologies." *Journal of Information Policy* 11:222–65. https://doi.org/10.5325/jinfopoli.11.2021.0222.

[69] Bannerman, S., and A. Orasch. 2020. "Privacy and Smart Cities: A Canadian Survey." *Canadian Journal of Urban Research* 29(1):17–38.

[70] Habibzadeh, H., B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata. 2019. "A Survey on Cybersecurity, Data Privacy, and Policy Issues in Cyber-Physical System Deployments in Smart Cities." *Sustainable Cities and Society* 50. https://doi.org/10.1016/j.scs.2019.101660.

[71] Curzon, J., A. Almehmadi, and K. El-Khatib. 2019. "A Survey of Privacy Enhancing Technologies for Smart Cities." *Pervasive and Mobile Computing* 55:76–95. https://doi.org/10.1016/j.pmcj.2019.03.001.

[72] Yang, F., and J. Xu. 2018. "Privacy Concerns in China's Smart City Campaign: The Deficit of China's Cybersecurity Law." *Asia and the Pacific Policy Studies* 5(3):533–43. https://doi.org/10.1002/app5.246.

[73] Chatterjee, S, A. K. Kar, and M. P. Gupta. 2018. "Alignment of IT Authority and Citizens of Proposed Smart Cities in India: System Security and Privacy Perspective." *Global Journal of Flexible Systems Management* 19(1):95–107. https://doi.org/10.1007/s40171-017-0173-5.

[74] Lim, H. S. M., and A. Taeihagh. 2018. "Autonomous Vehicles for Smart and Sustainable Cities: An in-Depth Exploration of Privacy and Cybersecurity Implications." *Energies* 11(5). https://doi.org/10.3390/en11051062.

[75] van Zoonen, L. 2016. "Privacy Concerns in Smart Cities." *Government Information Quarterly* 33(3):472–80. https://doi.org/10.1016/j.giq.2016.06.004.

[76] Seto, Y. 2015. "Application of Privacy Impact Assessment in the Smart City." *Electronics and Communications in Japan* 98(2):1427–35. https://doi.org/10.1002/ecj.11661.

[77] Gharaibeh, Ammar, Mohammad A. Salahuddin, Sayed Jahed Hussini, Abdallah Khreishah, Issa Khalil, Mohsen Guizani, and Ala Al-Fuqaha. 2017. "Smart Cities: A Survey on Data Management, Security, and Enabling Technologies." *IEEE Communications Surveys & Tutorials* 19(4):2456–2501.

[78] Qi, Lianyong, Chunhua Hu, Xuyun Zhang, Mohammad R. Khosravi, Suraj Sharma, Shaoning Pang, and Tian Wang. 2021. "Privacy-Aware Data Fusion and Prediction With Spatial-Temporal Context for Smart City Industrial Environment." *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS* 17(6):4159–67. https://doi.org/10.1109/TII.2020.3012157.

[79] Chen, J., L. Ramanathan, and M. Alazab. 2021. "Holistic Big Data Integrated Artificial Intelligent Modeling to Improve Privacy and Security in Data Management of Smart Cities." *Microprocessors and Microsystems* 81. https://doi.org/10.1016/j.micpro.2020.103722.

[80] Guan, Zhitao, Guanlin Si, Xiaosong Zhang, Longfei Wu, Nadra Guizani, Xiaojiang Du, and Yinglong Ma. 2018. "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities." *IEEE COMMUNICATIONS MAGAZINE* 56(7):82–88. https://doi.org/10.1109/MCOM.2018.1700401.

[81] Fang, Liming, Hanyi Zhang, Minghui Li, Chunpeng Ge, Liang Liu, and Zhe Liu. 2020. "A Secure and Fine-Grained Scheme for Data Security in Industrial IoT Platforms for Smart City."

IEEE INTERNET OF THINGS JOURNAL 7(9):7982–90. https://doi.org/10.1109/JIOT.2020.2996664.

[82] Wu, Fan, Xiong Li, Lili Xu, Saru Kumari, Dingbao Lin, and Joel J. P. C. Rodrigues. 2020. "An Anonymous and Identity-Trackable Data Transmission Scheme for Smart Grid under Smart City Notion." *ANNALS OF TELECOMMUNICATIONS* 75(7–8, SI):307–17. https://doi.org/10.1007/s12243-020-00765-4.

[83] Chaturvedi, Kanishk, Andreas Matheus, Son H. Nguyen, and Thomas H. Kolbe. 2019. "Securing Spatial Data Infrastructures for Distributed Smart City Applications and Services." *FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE* 101:723–36. https://doi.org/10.1016/j.future.2019.07.002.

[84] Huang, Cheng, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. 2018. "Secure Automated Valet Parking: A Privacy-Preserving Reservation Scheme for Autonomous Vehicles." *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY* 67(11):11169–80. https://doi.org/10.1109/TVT.2018.2870167.

[85] Nikooghadam, Mahdi, Haleh Amintoosi, S. K. Hafizul Islam, and Mostafa Farhadi Moghadam. 2021. "A Provably Secure and Lightweight Authentication Scheme for Internet of Drones for Smart City Surveillance." *JOURNAL OF SYSTEMS ARCHITECTURE* 115. https://doi.org/10.1016/j.sysarc.2020.101955.

[86] Zhou, Rang, Xiaosong Zhang, Xiaofen Wang, Guowu Yang, Nadra Guizani, and Xiaojiang Du. 2021. "Efficient and Traceable Patient Health Data Search System for Hospital Management in Smart Cities." *IEEE INTERNET OF THINGS JOURNAL* 8(8):6425–36. https://doi.org/10.1109/JIOT.2020.3028598.

[87] Cha, Jeonghun, Sushil Kumar Singh, Tae Woo Kim, and Jong Hyuk Park. 2021. "Blockchain-Empowered Cloud Architecture Based on Secret Sharing for Smart City." *JOURNAL OF INFORMATION SECURITY AND APPLICATIONS* 57. https://doi.org/10.1016/j.jisa.2020.102686.

[88] Hundera, Negalign Wake, Chuanjie Jin, Muhammad Umar Aftab, Dagmawit Mesfin, and Sachin Kumar. 2021. "Secure Outsourced Attribute-Based Signcryption for Cloud-Based Internet of Vehicles in a Smart City." *ANNALS OF TELECOMMUNICATIONS* 76(9–10, SI):605–16. https://doi.org/10.1007/s12243-021-00833-3.

[89] Alotaibi, Saud S. 2019. "Registration Center Based User Authentication Scheme for Smart E-Governance Applications in Smart Cities." *IEEE ACCESS* 7:5819–33. https://doi.org/10.1109/ACCESS.2018.2884541.

[90] Kumar, A., K. Abhishek, X. Liu, and A. Haldorai. 2021. "An Efficient Privacy-Preserving ID Centric Authentication in IoT Based Cloud Servers for Sustainable Smart Cities." *Wireless Personal Communications* 117(4):3229–53. https://doi.org/10.1007/s11277-020-07979-8.

[91] Elmaghraby, A. S., and M. M. Losavio. 2014. "Cyber Security Challenges in Smart Cities: Safety, Security and Privacy." *Journal of Advanced Research* 5(4):491–97. https://doi.org/10.1016/j.jare.2014.02.006.

[92] Bagheri, Rouholla, Mahmoud Zahedian Nezhad, and Mohammad Hosein Panahi. 2023. "Identifying and Evaluating Factors Affecting User Privacy in the Smart City Using the Meta-Synthesis Method and the Fuzzy DEMATEL Technique." *International Journal of Information Technology and Decision Making*. https://doi.org/10.1142/S0219622023500530

[93] Ravaei, B., S. Ravaei, S. MoshrefZadeh, and O. Rahmani Seryasat. 2022. "An Efficient and Load Balanced Task Offloading in Vehicular Internet of Things." *Transactions on Machine*

Intelligence 5(1):46–56. https://doi.org/10.47176/TMI.2022.46

[94] Pishdar, M., Bahaghighat, M., Kumar, R., & Xin, Q. (2025). "Major vulnerabilities in Ethereum smart contracts: Investigation and statistical analysis". EAI Endorsed Transactions on Internet of Things, 11. https://doi.org/10.4108/eetiot.5120

[95] Truong, Nguyen B., Tai-Won Um, and Gyu Myoung Lee. 2016. "A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things." *Innovations in Clouds, Internet and Networks (ICIN), Paris, France* 104–11. https://researchonline.ljmu.ac.uk/id/eprint/2599

[96] Zhang, Hui, Muhammad Babar, Muhammad Usman Tariq, Mian Ahmad Jan, Varun G. Menon, and Xingwang Li. 2020. "SafeCity: Toward Safe and Secured Data Management Design for IoT-Enabled Smart City Planning." *IEEE Access* 8:145256–67. https://doi.org/10.1109/ACCESS.2020.3014622

[97] Fattahdizaji, Ali, Mohammad Pishdar, and Zarina Shukur. 2024. "Investigating Cyber Threats against Proof-of-Work Blockchain Networks." Pp. 1–14 in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. https://doi.org/10.1109/ICBDS61829.2024.10837146

[98] Chatterjee, Sheshadri, Arpan Kumar Kar, and M. P. Gupta. 2018. "Success of IoT in Smart Cities of India: An Empirical Analysis." *Government Information Quarterly* 35(3):349–61. https://doi.org/10.1016/j.giq.2018.05.002

[99] Albino, Vito, Umberto Berardi, and Rosa Maria Dangelico. 2015. "Smart Cities: Definitions, Dimensions, Performance, and Initiatives." *Journal of Urban Technology* 22(1):3–21. https://doi.org/10.1080/10630732.2014.942092

[100] Eckhoff, David, and Isabel Wagner. 2017. "Privacy in the Smart City – Applications, Technologies, Challenges and Solutions." *IEEE Communications Surveys & Tutorials* PP:1. https://doi.org/10.1109/COMST.2017.2748998.

[101] Navaei, Reza Lotfi, Mohammad Safarzadeh, and Seyed Mohammad Jafar Sobhani. 2025. "Optimizing Flamelet Generated Manifold Models: A Machine Learning Performance Study." *ArXiv Preprint ArXiv:2507.01030*. https://doi.org/10.48550/arXiv.2507.01030

[102] Rizi, Mohammad Hosein Panahi, and Seyed Amin Hoseini Seno. 2022. "A Systematic Review of Technologies and Solutions to Improve Security and Privacy Protection of Citizens in the Smart City." *Internet of Things* 100584. https://doi.org/10.1016/j.iot.2022.100584

[103] Lai, Chun Sing, Youwei Jia, Zhekang Dong, Dongxiao Wang, Yingshan Tao, Qi Hong Lai, Richard T. K. Wong, Ahmed F. Zobaa, Ruiheng Wu, and Loi Lei Lai. 2020. "A Review of Technical Standards for Smart Cities." *Clean Technologies* 2(3):290–310. https://doi.org/10.3390/cleantechnol2030019.

[104] Allam, Zaheer, and David Jones. 2020. "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* 8:46. https://doi.org/10.3390/healthcare8010046.

[105] van den Broek, Tijs, and Anne Fleur van Veenstra. 2017. "Governance of Big Data Collaborations: How to Balance Regulatory Compliance and Disruptive Innovation." *Technological Forecasting and Social Change* 129. https://doi.org/10.1016/j.techfore.2017.09.040.

[106] Haseli, Gholamreza, Muhammet Deveci, and Mostafa Hajiaghaei-Keshteli. 2026. *Encyclopedia of Multi-Attribute Decision Making (MADM)*. Morgan Kaufmann.

https://doi.org/10.1016/C2025-0-01339-X

[107] Haseli, Gholamreza, Reza Sheikh, and Shib Sankar Sana. 2020. "Base-Criterion on Multi-Criteria Decision-Making Method and Its Applications." *International Journal of Management Science and Engineering Management* 15(2):79–88. https://doi.org/10.1080/17509653.2019.1633964.

[108] Nazarian-Jashnabadi, Javad, and Samuel Yousefi. 2026. "Stratified BCM: Stratified Base Criterion Method for Multi-Attribute Decision-Making." Pp. 403–19 in *Encyclopedia of Multi-Attribute Decision Making (MADM)*. Elsevier. https://doi.org/10.1016/B978-0-443-33275-3.00008-7

[109] Nazarian-Jashnabadi, Javad, Tahereh Sepahi, and Dragan Pamucar. 2026. "Nonadditive BCM: Nonadditive Base-Criterion Method for Multi-Attribute Decision-Making." Pp. 435–49 in *Encyclopedia of Multi-Attribute Decision Making (MADM)*. Elsevier. https://doi.org/10.1016/B978-0-443-33275-3.00028-2

[110] Mohamadabadi, Tayebeh Abdoli, Javad Nazarian-Jashnabadi, Mahmoud Ahmadpour Daryani, Muhammad Ahmad Al-Rashid, and Tiziana Campisi. 2025. "Factors Affecting Online Customer Experience of Food Delivery Services during Crisis: TISM and Delphi Techniques." *Sustainable Futures* 9:100408. https://doi.org/10.1016/j.sftr.2024.100408

[111] Poorakbari, Pooria, Samira Mohamadi, Zahra Najafabadipour, Majid Talebpoor, Linda Manokians, and Hero Isavi. 2026. "Fuzzy Growing Map for Analyzing Cryptocurrency Market Trends." *Computational Methods for Differential Equations*. https://doi.org/10.22034/cmde.2025.69796.3445

[112] Nazarian-Jashnabadi, Javad, and Erfan Babaee Tirkolaee. 2026. "BCM Tradeoff (BCT): Base Criterion Tradeoff for Multi-Attribute Decision-Making." Pp. 421–34 in *Encyclopedia of Multi-Attribute Decision Making (MADM)*. Elsevier. https://doi.org/10.1016/B978-0-443-33275-3.00085-3

[113] Senapati, Tapan, and Ronald R. Yager. 2020. "Fermatean Fuzzy Sets: T. Senapati, RR Yager." *Journal of Ambient Intelligence and Humanized Computing* 11(2):663–674. https://doi.org/10.1007/s12652-019-01377-0

[114] Sumrit, Detcharat, and Jirawat Keeratibhubordee. 2025. "An Integrated SWARA-QFD under Fermatean Fuzzy Set Approach to Assess Proactive Risk Mitigation Strategies in Recycling Supply Chain: Case Study of Plastic Recycling Industry." *Journal of Engineering Research* 13(2):492–510. https://doi.org/10.1016/j.jer.2023.11.007

[115] Seker, Sukran, and Nezir Aydin. 2023. "Fermatean Fuzzy Based Quality Function Deployment Methodology for Designing Sustainable Mobility Hub Center." *Applied Soft Computing* 134:110001. https://doi.org/10.1016/j.asoc.2023.110001

[116] Keršuliene, Violeta, Edmundas Kazimieras Zavadskas, and Zenonas Turskis. 2010. "Selection of Rational Dispute Resolution Method by Applying New Step-Wise Weight Assessment Ratio Analysis (SWARA)." *Journal of Business Economics and Management* 11(2):243–58.

[117] Stanujkic, Dragisa, Darjan Karabasevic, and Edmundas Kazimieras Zavadskas. 2015. "A Framework for the Selection of a Packaging Design Based on the SWARA Method." *Engineering Economics* 26(2):181–87.

[118] Likas, Aristidis, Nikos Vlassis, and Jakob J. Verbeek. 2003. "The Global K-Means Clustering Algorithm." *Pattern Recognition* 36(2):451–61. https://doi.org/10.1016/S0031-3203(02)00060-2

[119] Pfitzner, Darius, Richard Leibbrandt, and David Powers. 2009. "Characterization and Evaluation of Similarity Measures for Pairs of Clusterings." *Knowledge and Information Systems* 19(3):361–94. https://doi.org/10.1007/s10115-008-0150-6

[120] Keser, Reyhan Kevser, Aydin Ayanzadeh, Omid Abdollahi Aghdam, Caglar Kilcioglu, Behcet Ugur Toreyin, and Nazim Kemal Ure. 2023. "Pursuhint: In Search of Informative Hint Points Based on Layer Clustering for Knowledge Distillation." *Expert Systems with Applications* 213:119040. https://doi.org/10.1016/j.eswa.2022.119040

[121] Kanungo, Tapas, David M. Mount, Nathan S. Netanyahu, Christine D. Piatko, Ruth Silverman, and Angela Y. Wu. 2002. "An Efficient K-Means Clustering Algorithm: Analysis and Implementation." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 24(7):881–92. https://doi.org/10.1109/TPAMI.2002.1017616

[122] Zhang, Yu-Fang, Jia-Li Mao, and Zhong-Yang Xiong. 2003. "An Efficient Clustering Algorithm." Pp. 261–65 in *Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 03EX693)*. Vol. 1. https://doi.org/10.1109/ICMLC.2004.1382013

[123] Huang, Zhexue. 1998. "Extensions to the K-Means Algorithm for Clustering Large Data Sets with Categorical Values." *Data Mining and Knowledge Discovery* 2(3):283–304. https://doi.org/10.1023/A:1009769707641