A Hyperconnected Smart City Framework: Digital Resources Using Enhanced Pedagogical Techniques

Naureen Naqvi
School of Computing & Mathematics
Charles Sturt University
nnaqvi@csu.edu.au

Sabih ur Rehman
School of Computing & Mathematics
Charles Sturt University

Md Zahidul Islam
School of Computing & Mathematics
Charles Sturt University

Abstract

Recent technological advancements have given rise to the concept of hyper-connected smart cities being adopted around the world. These cities aspire to achieve better outcomes for citizens by improving the quality of service delivery, information sharing, and creating a sustainable environment. A smart city comprises of a network of interconnected devices also known as IoT (Internet of Things), which captures data and transmits it to a platform for analysis. This data covers a variety of information produced in large volumes also known as Big Data. From data capture to processing and storage, there are several stages where a breach in security and privacy could result in catastrophic impacts. Presently there is a gap in the centralization of knowledge to implement smart city services with a secure architecture. To bridge this gap, we present a framework that highlights challenges within the smart city applications and synthesizes the techniques feasible to solve them. Additionally, we analyse the impact of a potential breach on smart city applications and state-of-the-art architectures available. Furthermore, we identify the stakeholders who may have an interest in learning about the relationships between the significant aspects of a smart city. We demonstrate these relationships through force-directed network diagrams. They will help raise the awareness amongst the stakeholders for planning the development of a smart city. To complement our framework, we designed web-based interactive resources that are available from http://ausdigitech.com/smartcity/

Keywords: Smart Cities; Privacy; Security; IoT; Big Data

1 Introduction

The adoption and advancement in technology have given rise to smart cities that are acting as enablers to improve the liveability of cities by providing better outcomes for their residents.

To improve the quality of life of citizens, smart cities make use of information and communication technologies. It builds a seamlessly interconnected society of devices capturing data from multiple sources, analysing it, and supporting data-driven decisions (Achmad, Nugroho, Djunaedi, & Widyawan, 2018; Ismail, 2016). Over the last decade, the speed at which the population of cities is growing has reinforced the importance of using technology to improve service outcomes for citizens. For example, smart cities, with the help

of technological assistance, can save 30–300 lives each year, reduce crime by 30–40%, lower the disease burden by 8–15%. Additionally, the smart cities can help improve emergency response times by 20–35%, cut daily commutes by 15–30 minutes, and save 25–80 litres of water consumption per person per day (Shah & Patel, 2014). These areas are a part of the daily lives of city residents and improved efficiencies in these areas will result in greater quality of lives. and an improved governance framework. More compelling arguments suggest that a smart city is not only capable of improving the quality of services for citizens but also empowers governments for running public administration effectively (Sarker, Wu, & Hossin, 2018). Furthermore, according to studies from the United Nations (UN), the world population is expected to increase by close to 6 billion by 2050. This will lead to challenges that require a standard framework to help with the growth of cities in a sustainable manner (Okai, Feng, & Sant, 2019; Simonofski, Asensio, De Smedt, & Snoeck (2017)).

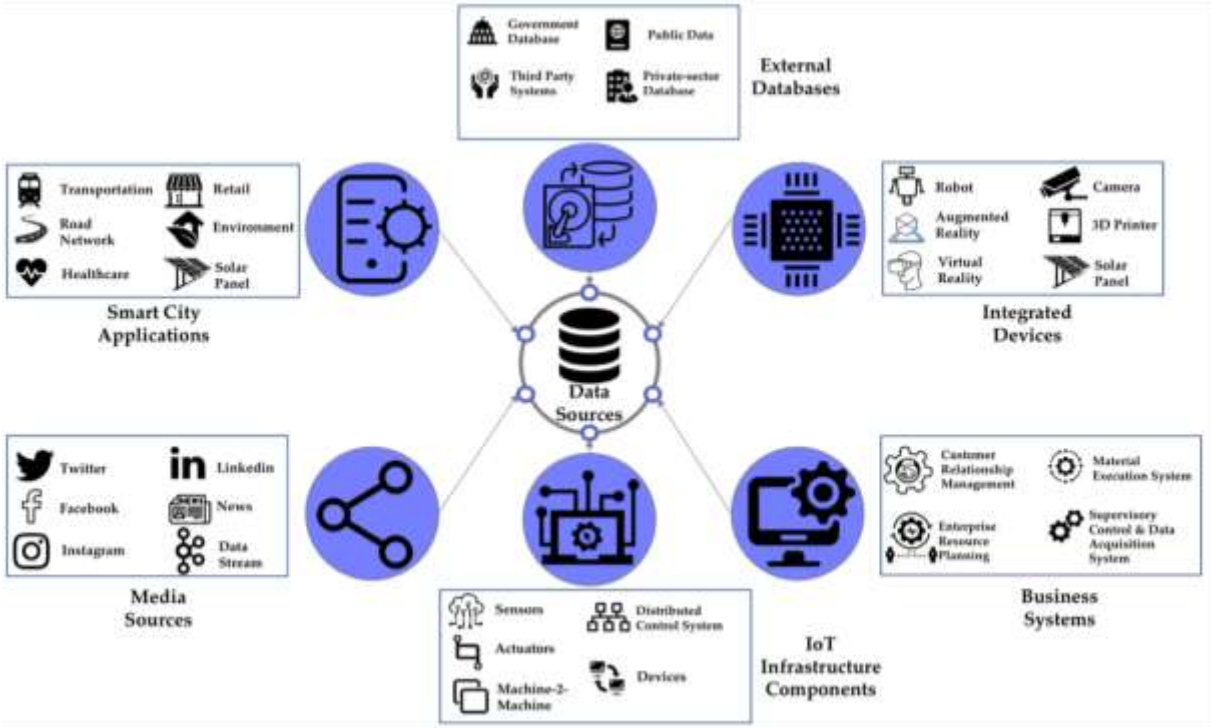

Figure 1 Sources for Data Collection – Smart City

The performance of smart cities and outcomes produced by them relies on the amount and the quality of data provided to them. To collect this data, smart cities use an integrated network

of closely webbed technologies that capture large volumes of data arriving at high speeds called the Internet of Things (IoT). Figure 1 illustrates the sources for data collection within a smart city. A smart city architecture has a fundamental layer of data collection where data is ingested from multiple sources. Within the smart city paradigm, data can be collected from core applications across the city. For example, external databases collecting data from stakeholder organisations, and integrated devices that are embedded in operations. Additionally, this data is also captured from the business systems that are used across the administration, and the IoT infrastructure that has been installed to gather insights and media sources, etc. Due to enormous data collection, often the boundaries of ethics with which the data has been acquired get blurred leading to trust issues among the citizens (Brauchli & Li, 2015). Post data acquisition by smart cities, there is often a lack of effective mechanisms in

place to ensure the protection from invading privacy and threatening civil liberties (Wang, Ali, & Kelly, 2015). This data is vulnerable and can be compromised by intruders, leading to compromised security of the city operations and the privacy of citizens' data posing a security threat.

Our work recognises current research gaps in the domain of smart cities and presents a holistic framework. We anticipate this framework to be pivotal in shaping a strategy for data privacy and security for the portfolio of smart city services. Our framework has been developed by keeping in view the stakeholders' requirements and the impact that data privacy and security have on the operations. Our framework focuses on synthesizing information within the most important areas of the smart city and highlighting the key relationships. Our work comprises a comprehensive literature review following a timeline of 2007-2018. The objective was to synthesize previous publications and analyse the relationship between the work that is already available. This work has then been overlaid with the current trends within a smart city, IoT, and big data analytics. We also study state-of-the art exemplary smart cities around the world to correlate their learnings with our findings. Our framework has been developed in the form of an open-source interactive digital resource. This will allow other researchers to benefit from this work and build future resources using the fundamental building blocks provided.

The framework follows a structured research methodology with the identification of theoretical concepts, gaps, and implementation via kinaesthetic learning methodology. Our broad literature review has resulted in a knowledge base consisting of commonly used terminology used in smart cities. These keywords are supported by definitions and publication references. To develop an interactive resource, we focused on a portfolio of services that fall under the remit of a smart city to fully comprehend the challenges pertaining to security and privacy. This has helped us in devising a targeted plan for addressing challenges. Furthermore, mapping the challenges to the available solutions and highlighting relationships between the key aspects delivered via pedagogical techniques. Our research offers the following contributions:

1. Developed a knowledge base of key terms, definitions, and relationships between important concepts relating to smart cities along with relevant references.
2. Analysed the learning of state-of-the-art exemplary smart cities around the world and identified key stakeholders within the smart city framework. This framework helps in demonstrating the key aspects of privacy & security within the smart city applications.
3. Presented a framework for privacy and security preserved data sharing in hyper-connected smart cities. The framework is delivered via open-source interactive digital resources highlighting fundamental building blocks and the key relationships between entities.

The paper is organized as follows: in section 2, a literature review of smart cities along with examples is provided. Section 3 describes our proposed framework. Section 4 explains the usefulness of our framework and a discussion on our designed interactive resources. Section 5 contains the conclusion of our work and proposes a future outlook of research within this domain.

2 Literature Review

The smart cities model presents an integrated concept of a sustainable environment, improved quality of life, and reduced cost of living, using technology to optimize services. It is a composite of people, infrastructure, technology, and services. Many cities around the world have adopted digital initiatives to establish smart governance. To achieve real-time data-driven decision making, the cities collect data from interconnected sensor-enabled devices, 'Things'. The Internet of Things (IoT) has been recognized as an efficient mechanism to achieve city urbanization. Emerging technologies provide reliable technology for real-time data collection and sharing using controlled architecture following standard processes for high-impact applications (Khan, Pervez, & Ghafoor 2014; Li, Cao, & Yao, 2015; Maheswaran & Misra, 2015; Popescul & Radu, 2016; Pacheco & Hariri 2016; Shahat, Elragal, & Bergvall-Kåreborn, 2017; Ati & Basmaji, 2018; Alias Balamurugan, Lilian, & Sasikala 2018; Manjunatha & Annappa, 2018; Alsafery, Alturki, Reiff-Marganiec, & Jambi, 2018; Puschmann, Barnaghi, & Tafazolli, 2018; Santos et. al, 2017; Lim, Kim, & Maglio, 2018; Harris 2014).

The synergy of these processes, standards, and emerging technologies will result in collecting data. This data could include sensitive information, such as health records, financial transactions, academic records, multimedia recordings, industrial grids, electricity, water systems, etc. With a hyper-connected, integrated network in place, datasets may not always be collected and in turn shared with the explicit consent of the citizens. A security breach within the smart city could allow intruders to infiltrate the network and gain access to controls. This could have a severe impact on the smart city operations, requiring the attack paths to be identified and stored by using Smart Infrastructures (SI) that provide autonomy and control. This further reinforces the impact that security and privacy have on the smart operations and must be considered when designing the reference architecture (Cárdenas & Safavi-Naini, 2012; Hashem et al., 2016; Berntzen & Johannessen, 2016; Doynikova & Kotenko, 2017; Ylmaz, Ciylan, Gönen, Sindiren, & Karacayilmaz, 2018; Ghirardello, Maple, Ng, & Kearney, 2018).

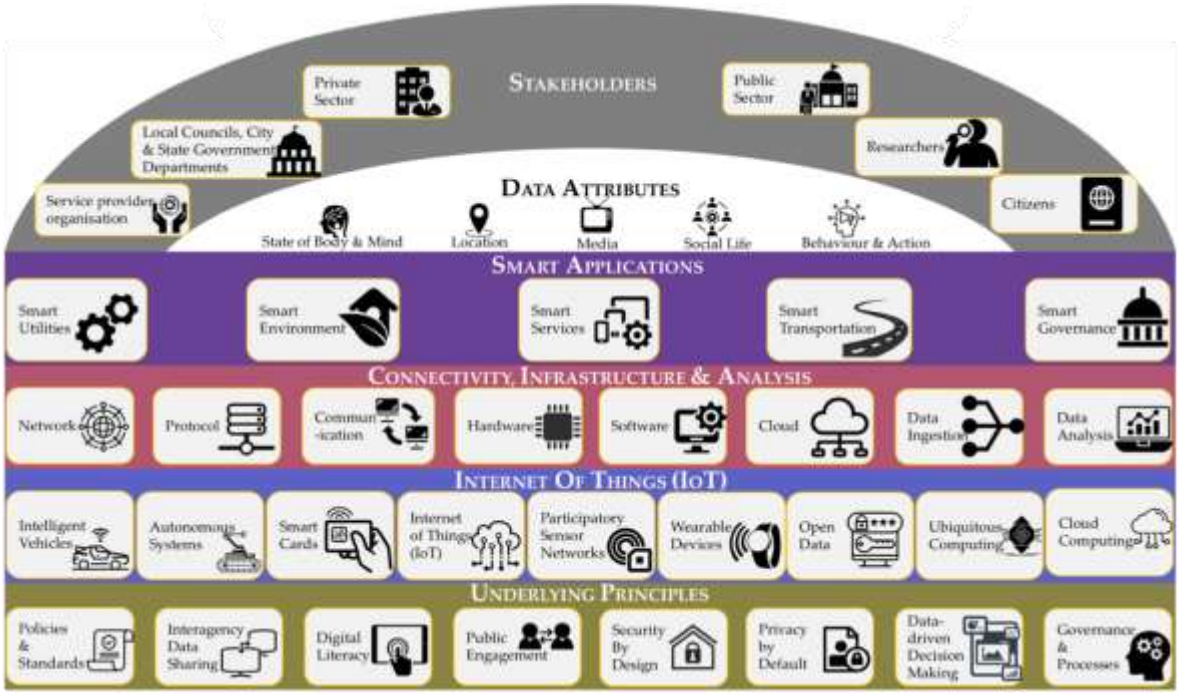

Figure 2: Smart City Framework

Our research observed that some of the key aspects of security concerns include unlawful access to information, and attacks causing physical service disruptions. On the other hand, privacy breaches include the interception of data in transit-related to the citizens' private life. These aspects must be planned contingently when designing a smart city, for example, by establishing business resiliency, service continuity planning, and appropriate accountability. A possible way in which accountability can be established is by storing the audit trail of operations in the form of tamper-proof digital patterns via Blockchain. Another measure of achieving resilience within the smart city business application is to host applications on critical infrastructure and classify them based on their risk score (Estevez & Janowski, 2013; Cam-Winget, Sadeghi, & Jin, 2016; Sankaran & Vishwa Vidyapeetham, 2017; Liu et al., 2017; Chan et al., 2018; Boban & Weber, 2018; Russell, Goubran, Kwamena, & Knoefel, 2018).

This helps to map the relationship between applications and security essentials. It is also important to note that the legacy systems should be fully secure if they have any touchpoints with the systems using the IoT. Smart city stakeholders concerned about security should be vigilant when making a selection in hosting their IoT networks on edge or fog respectively. The design has to be in line with the principles of scalability as a smart city portfolio contains closely related applications. Finally, the security essentials should be applied at all levels of the smart city applications (Anthopoulos, 2015; Gyrard, Zimmermann, & Sheth, 2018; Oteafy & Hassanein, 2018; Pradhan, Suri, Fuchs, Bloebaum, & Marks, 2018). Figure 2 illustrates a smart city framework that captures the key elements of a smart city. The top layer includes the stakeholders who are the receivers of this information. Layer 2 highlights the applications of interest. Layer 3 demonstrates the important data attributes produced by the city. The following layer presents a number of IoT technologies used that helps collect the data. To summarize, all of the above layers revolve around Layer 5, the underlying principles within a smart city.

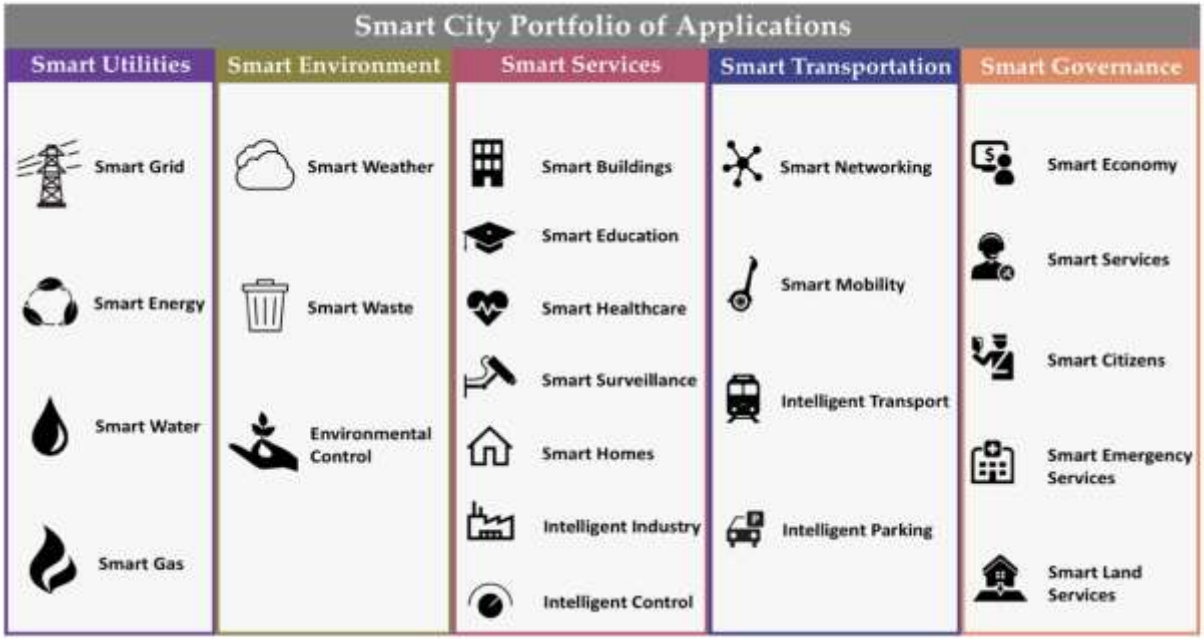

Figure 3: Smart City Framework Portfolio of Applications

From a stakeholder's perspective, our research is aimed at smart city planners, designers, specialists, privacy and security advocates, and decision-makers. These groups have been identified to have a significant impact on how interconnected cities are designed and function.

We identified real-life digital initiatives focusing on economic planning, governance, opportunities, environmental damage, and operational efficiencies. To evaluate our ideas and test them on practical benchmarks, we conducted a thorough analysis of the smart city applications, as illustrated in Figure 3. These applications have been listed based on their impact on the city's operation to learn from the lessons of the exemplary smart cities.

Now that we have defined the role of the portfolio of applications within the smart city framework and the types of applications that sit within the portfolio. We introduce Table 1, which summarizes state-of-the art exemplary smart cities that run smart applications around the world. The challenges faced by these initiatives have been cited in publications in reputed journals. We have grouped these applications in the form of the portfolio of services that relate to that group and experienced similar challenges (Foucault & Moulier-Boutang, 2015; Feng, Dawam, & Amin, 2017; Smolander, Rossi, & Pekkola 2017; De Carolis, Macchi, Negri, & Terzi 2017; Johannessen & Berntzen, 2018; Achmad, Nugroho, Djunaedi, & Widyawan, 2018).

Publications	Portfolio of Service	Smart City Applications	Exemplary Smart Cities
Okai, Feng, & Sant, 2019	**Smart Utilities**	Smart Grid	Barcelona, Spain
Eckhoff, & Wagner, 2018		Smart Energy	Zwolle, Netherlands Bristol, UK
El hendy, Miniaoui, Atalla, & Hashim, 2018		Smart Water	The Island city, state of Singapore
El hendy, Miniaoui, Atalla, & Hashim, 2018		Smart Gas	San Francisco, US
Bellini, Nesi, Paolucci, & Zaza, 2018; El hendy, Miniaoui, Atalla, & Hashim, 2018	**Smart Environment**	Smart Weather	Seattle, US San Francisco, US
Bellini, Nesi, Paolucci, & Zaza, 2018		Smart Waste	Helsinki, Finland
Eckhoff, & Wagner, 2018		Environment Control	Bristol, UK
Eckhoff, & Wagner, 2018; Bellini, Nesi, Paolucci, & Zaza, 2018	**Smart Services**	Smart Buildings	Aspern, Austria Milton Keynes, UK
Eckhoff, & Wagner, 2018		Smart Education	Almere, Netherlands Waseda, Japan
Eckhoff, & Wagner, 2018		Smart Healthcare	Rio De Janeiro The Island city, state of Singapore
Bellini, Nesi, Paolucci, & Zaza, 2018; Eckhoff, & Wagner, 2018		Smart Surveillance	Eindhoven, Netherlands Glasgow, Scotland California, US
Eckhoff, & Wagner, 2018		Smart Homes	Hague, Netherlands
Eckhoff, & Wagner, 2018		Intelligent Industry	European Union
Eckhoff, & Wagner, 2018		Intelligent Control	European Union
Eckhoff, & Wagner, 2018	**Smart Transportation**	Smart Networking	Oulu, Finland Estonia Copenhagen, Denmark Chicago, US

Publications	Portfolio of Service	Smart City Applications	Exemplary Smart Cities
Bellini, Nesi, Paolucci, & Zaza, 2018		Smart Mobility	Glasgow, Scotland
Bellini, Nesi, Paolucci, & Zaza, 2018		Intelligent Transport	Seattle, US
Okai, Feng, & Sant, 2019; Bellini, Nesi, Paolucci, & Zaza, 2018		Intelligent Parking	Barcelona, Spain Milton Keynes, UK
Eckhoff, & Wagner, 2018; Bellini, Nesi, Paolucci, & Zaza, 2018; Okai, Feng, & Sant, 2019	**Smart Government**	Smart Economy	Almere, Netherlands Dubai, UAE
Eckhoff, & Wagner, 2018		Smart Services	Sydney, Australia
Eckhoff, & Wagner, 2018		Smart Citizens	Zaragoza, Spain
Eckhoff, & Wagner, 2018		Smart Emergency Services	Hague, Netherlands Rio De Janeiro
Bellini, Nesi, Paolucci, & Zaza, 2018; Okai, Feng, & Sant, 2019		Smart Land Services	Dubai, UAE

Table 1: Smart City Data Model

Next, we discuss the intricate design and implementation details of the proposed framework.

3 The proposed framework

The learning gathered for the framework has been presented in the form of a purpose-built website with interactive resources. This section describes the artifacts produced to disseminate the knowledge. The resource development was inspired by the product development lifecycle with stages categorized as scope definition, requirements gathering, stakeholder identification, and implementation. We adopted the standard approach for building a framework by i) reviewing requirements, ii) analysing relationships, and iii) proposing a solution (Elmaghraby, 2013; Teoh & Mahmood, 2017; Yamakami, 2017; Puron-Cid, Gil-Garci, & Zhang, 2015; Wagner, & Eckhoff, 2018).

3.1 Design

To deliver an immersive learning experience through our digital resources, we focused on the following five dimensions of design:

i. Volume – reviewed a large number of publications per year.

ii. Domain – the study included the IoT, architecture, ontologies, privacy, security, big data, and data sharing.

iii. Object – challenges, solutions, architecture, and applications.

iv. Level – review against three dimensions i.e., smart city subject expertise, education resources, and design excellence.

v. Contribution – the type of contribution to the field such as best practice, field experience, policy recommendation, standard design, and empirical methods.

Design Principles	Standard	Our Resource
Useful	The content produced as a result of this research is original. The references to the source have been appropriately cited.	✓
Desirable	The website is light and has easy to use a color scheme to reduce strain on users' eyes. Consistent layout design and fonts have been used to give the website a unified, consistent look and feel.	✓
Findable	Search functionality is built to look for keywords without hassle.	✓
Accessible	The website is Web Content Accessibility Guidelines (WCAG) 2.0 compliant making the website inclusive to all users.	✓

Table 2: Digital Resource Design Principles

With the help of the above, we opted to use gamification techniques and methods for creating an immersive experience for developing our pedagogical resources (L'Heureux, Grolinger, Higashino, & Capretz, 2017). These resources stimulate a fast learning experience among users of resources by enabling kinaesthetic techniques. Next, we discuss the methodology including data collection, organization, and the presentation method used in this research. This section is followed by a discussion on the user experience.

3.1.1 Methodology

We reviewed literature from primary and secondary sources. A detailed spreadsheet of the relationships is available on the website. Presenting relationships between variables, reviewing the irregular hierarchies, positioning the citations, and listing the glossary were some of the biggest design challenges. Table 2 represents the design principles that we have used in the presentation of knowledge.

Design Elements	Standard	Our Resource
Mega menus	The website content is arranged in mega menus. It enables the content to be categorized reducing the page length.	✓
Usable Information	Bootstrap and jQuery have been used to make the website easy to use. Custom components have been used to present data and interrelationships. The website is cross-platform, compatible, and responsive, that is, usable on computers, tablets & phones.	✓
Vertical tab	Allows efficient maneuvers between two sub-topics and contains a significant amount of information in the form of switchable tabs.	✓
Accordion	The accordions are horizontally expandable collapsible boxes containing the content reducing the vertical scroll of the page.	✓
HTML	Standard elements are used for designing.	✓

Table 3: Page Design Elements

Our reviews yielded approximately 500 variables, in 38 categories, and over 143 references. We used the design principles in Table 2 to organize the data into simple user-friendly data-rich resources. Presenting data on different levels or hierarchies posed an implementation

challenge. Table 3 demonstrates the design elements used to render content dynamically – this required no added customisation to the code.

We selected the technology such that all the components reside on the client-side with reduced round trips to the server to fetch the data for each node. Our resources are cross-browser, cross-platform, and cross-devices. This means that they work effectively on four tested browsers (Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari), across both Microsoft and Apple OS platforms. The resources perform equally well on multiple devices such as computers and mobile devices. Table 4 shows the selected technology for our solution i.e., HTML5, Bootstrap, PHP, JSON, JavaScript jQuery, and amCharts. In the next section, we explain the user experience and usability of the resources.

Technology Stack	Standard	Our Resource
UX Specifications	• HTML5 for developing SEO-friendly web resource • PHP – HTML friendly object-orientation package • Mega Menus – ease of navigation with no scrolling • Vertical tabs – intuitive with better use of horizontal space • Accordions – responsive design, collapsible menus • Cross-browser – works responsively on all browsers (Chrome, Opera, Firefox, Edge, Safari and, IE onwards) • Cross-device – works on phones, tablets, and computers • Cross-platform – works on iOS, Android, and Windows • WCAG2.0 (World Content Accessibility Guidelines) by W3C (World Web Consortium).	✓
Technical Specifications	• Bootstrap – customizable look & feel for the plugins used • jQuery – SEO friendly, clean, extensible and libraries used • JSON (JavaScript Object Notification)–data stream sync • amCharts– building intuitive & intelligent digital resources	✓

Table 4: Technology Stack

3.1.2 User Experience

Usability, the transfer of knowledge, and ease of navigation have been the core principles behind designing this website. The website has been classified into five sections:

i. The "Overview" provides a holistic view.

ii. Sub-topics illustrate "Challenges", "Solutions", "Applications" and "Architecture".

iii. "Application Relationship" and "Security Relationships" include relationships derived from sources and anecdotal evidence.

iv. The "Definitions" page is a knowledge base of concepts used in smart cities.

v. The "Surveys" section captures the possible considerations that smart city stakeholders must plan for when introducing new technology within applications.

In the next section, we discuss the implementation details of our framework, including the areas of interest for the resource development and the benchmark set for the evaluation of resources.

3.2 Implementation

We classified the key aspects of the framework into the areas of interest. Later, we mapped the relationship between these aspects by highlighting the areas that would benefit stakeholders the most. As a preliminary step, we identified the key challenges, their solution, the applications they impact, and the technology used in the development of the city. We then moved onto understanding the relationships smart city stakeholders would benefit from the most.

3.2.1 Delivery Techniques

The visual interaction offered by our system has been developed using the following techniques.

i. **Tree Maps**: The tree maps provide a structured model for representing information in a layered fashion, highlighting the parent-child hierarchy between parameters of interest. We used tree maps to capture information on multiple levels from level 0 i.e., a high-level tree map to level 5, a low-level tree map demonstrating the children node under parent nodes. This is an effective method of organizing the information into categories.

ii. **Force Directed Trees**: The Force Directed Trees offer an effective mechanism of visualizing pre-organized information in the form of mind maps. It is easier to understand the hierarchical nature of information and it is used as a standard method of data visualization in the software development lifecycle to create valuable knowledge.

iii. **Force Directed Networks**: The Force Directed Networks is an extension of the Force Directed Trees and offer to map of relationships in the form of a network. They are used as a standard technique in the software development lifecycle to visualize relationships.

3.2.2 Areas of Interest within Smart City Framework

The development of the interactive resources available on our website has been aided by the literature review conducted. The learnings have been orchestrated in the form of a tree diagram before being converted to resources as illustrated in Figure 4. All tree diagrams have been drawn from the high-level (being level 0) to the lowest level, capturing granular details under section ii) and iii) above. The following are the four areas of interest that were used to develop the digital resources and understand the relationships.

Figure 4: Tree Map – Smart City Framework

i) The challenges regarding privacy-protected data sharing that emerge as a result of using new technologies within smart cities form the first area of interest. These challenges can be summarized into two categories – technical and functional challenges. Technical challenges emerge as connected devices within smart cities

require a non-conventional approach towards big data. This data has doubled in size every two years since 2011 and is predicted to increase from 130 exabytes in 2005 to 40,000 exabytes this year (a 300-fold increase). This can become a trigger for an increase in privacy-related issues. Functional challenges arise due to the dynamic nature of smart city applications that have seen exponential growth and require policies to be developed to protect privacy (Terzi, Terzi, & Sagiroglu, 2016; Kolozali et al., 2018; Nesi, Pantaleo, Paolucci, & Zaza, 2018; Siris, Fotiou, Mertzianis, & Polyzos, 2019). Our resource on challenges is available from http://ausdigitech.com/smartcity/challenges.html. Section 4.2 provides a detailed discussion on this topic.

ii) The second area of interest is the solutions that are available to tackle these challenges. However, it is interesting to note that there is no centralization of knowledge available at this stage. With our solution, we researched these areas and synthesized this information within a framework that the stakeholders can adopt and adapt when planning their smart city applications and related architecture. This solution has been derived from comparisons, expert views of prior studies, and questionnaires (Belgaum, Alansari, Jain, & Alshaer, 2018). We researched the key areas of big data, artificial intelligence (AI), and cloud automation along with their roles in the smart cities. Our resources on this solution is available from http://ausdigitech.com/smartcity/solutions.html. Section 4.3 has a detailed discussion.

iii) The third area of interest is identifying the portfolio of applications within the city. With the significant adoption of cloud computing, these applications are increasingly being hosted in the cloud. Under the transformative ecosystem, the use of the cloud to run smart city applications provides scalability, interoperability, elasticity, and maintainability at a low cost with fully encrypted data sharing (Alkhamisi, Nazmudeen, & Buhari, 2016; Venticinque & Amato, 2018; Abi Sen, Eassa, & Jambi 2018). Our resource on applications is available from http://ausdigitech.com/smartcity/applications.html with a detailed discussion in section 4.4.

iv) The fourth and the most important area of the smart city framework is its architecture. The planning and development of a smart city requires an architecture that can present a holistic picture of information systems, mission-critical, and distributed systems. This is key to building architectural resources in line with the services that need to be supported and consideration for architectural responses (Budhiputra & Putra, 2016; Sikora-Fernandez & Stawasz, 2016; Assante et al., 2018; Bass, Sutherland, & Symons, 2018; Cui et al., 2018; Sindhusha & Bharathi, 2018). Our resources on architecture are available from http://ausdigitech.com/smartcity/architecture.html. There is a detailed discussion in section 4.5.

Figure 5 illustrates the overview of our interactive resource on the high-level smart city framework, highlighting the areas of interest defined above.

Next, we evaluate our work against the key industry standards for assessing digital resources.

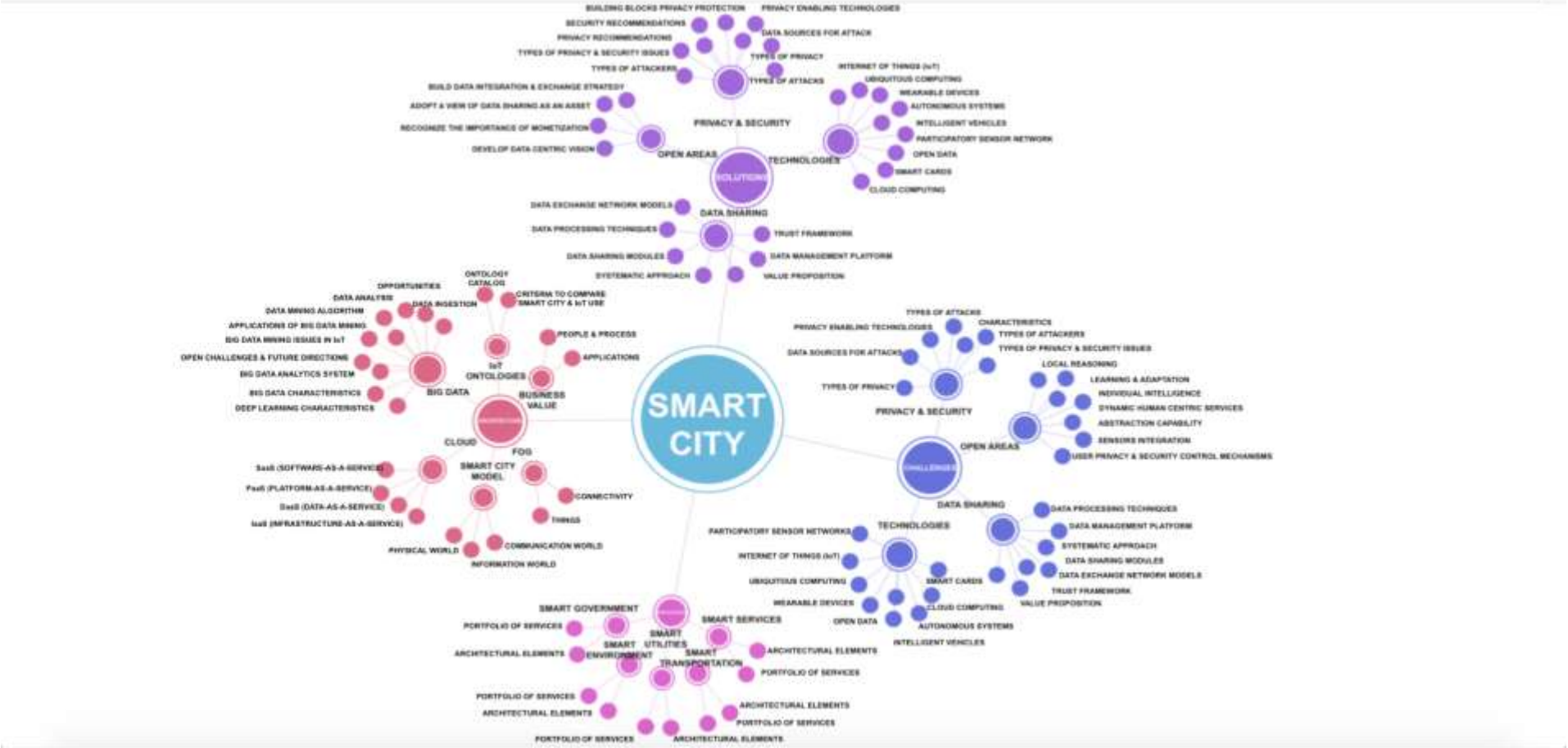

Figure 5: Force-directed Tree – Overview – Smart City

Table 5: Evaluation Criteria

3.2.3 Benchmark for Evaluation

Table 5 explains the high-level benchmarks for evaluating our framework design against the standard best practices.

i. The literary benchmark i.e. the discovery and analysis of various related concepts and their significance within smart cities (Liu, Choo, Huang, & Au, 2017).

ii. The functional benchmark includes the development of interactive digital resources. Furthermore, the presentation of complex information in the form of the tree maps, force-directed trees, and force-directed networks is another important measure of a functional fit (Ainane, Ouzzif, & Bouragba, 2018).

iii. The technical benchmark includes the technical quality of the open-source interactive resources. The system has the ability for the stakeholders to leverage the existing knowledge and scale the framework (Ahn, Lee, Kim, & Hwang, 2016).

Benchmark by Group	Measure of Evaluation	Our Resource
Literary benchmarks (findings of the research, their orchestration, and presentation within the website)	• IoT technologies • Privacy Enabling Technologies • Smart City Services • Smart City Paradigm • Architecture • Relationships • Associative relationships • Market Observations • Glossary	✓
Functional benchmarks (overall look and feel, ease of navigation, usability, accessibility and the empathy for the end-to-end stakeholder journey)	• User Experience • Colour confusion • The Golden Triangle • Feeding the imagination • Informative • Retention • Reading comprehension • Student achievements • Thinking and learning • Critical thinking • Pedagogical techniques • Design • Readability & Legibility • Accessibility • Clarity • Maintenance • Financially Viable • Easy to Maintain	✓
Technical benchmarks (the work to be made reproducible and extensible)	• Min. Server-side roundtrip • Dynamic Updates	✓

Next, we discuss the usefulness of our framework by describing the outputs of our research.

4 The Usefulness of our framework

While emerging technologies have shown immense promise to encourage the growth of smart cities, their reliability and full adaptability are yet to be seen. Additionally, their trust is yet to be matured, especially in government bodies and communities (Bajramovic, Waedt, Ciriello, & Gupta, 2016). Therefore, a trust framework needs to be established to offer best-practice knowledge on privacy-protected data sharing within smart cities (Hassanain et. al., 2019; Ferrer, Marquès, & Jorba, 2019). We have attempted to consolidate the knowledge areas where best practices and standards need to be developed. Table 6 presents a summary of our web system.

Page Configuration	Standard
Overview	The purpose of this project is to develop state of the art digital resources adopting newer ways of learning and introducing concepts of security and privacy for smart cities. This project dives deep into the challenges faced by smart cities on daily basis, offers solutions to the issues faced by the digitalization of the cities with a focus on a specific portfolio of services, in turn, shedding light on the architectural framework that is used for enabling privacy and security in smart cities. This project is a modern-day version of learning about the new concepts on smart city and is the version 1.0 with the intention that the team keeps contributing to the knowledge area - smart city focusing on IoT and Big Data.
Challenges	Smart cities face several challenges when it comes to keeping citizen's data private and secure from the time of collection and analysis. Our digital resources provide the challenges faced by cities classified into four categories: technological issues, privacy & security issues, data sharing issues, and open areas.
Solutions	Many smart cities have established smart city initiatives to meet the privacy and security requirements in turn protecting citizen's data. Our digital resources focus on providing a solution to the challenges defined. This has been classified into four main areas: solution on technological issues, privacy & security issues data-sharing issues, and solution recommendations for open areas.
Applications	Smart cities around the world have many service offerings such as transactional and consultative services which can be divided into five main smart categories: services, transportation, utilities, environment, and government.
Architecture	Smart cities focus on developing their intelligent assets and digital services on the back of architectural building blocks such as fog computing, cloud computing, smart city modeling, and IoT ontologies. This plays an important role in managing the privacy & security of the technologies involved in the city.
Applications Relationships	The application relationship diagram illustrates the fundamental building blocks of the application portfolio in a smart city. This diagram demonstrates the relationship between the building blocks such as privacy enabling technologies, IoT ontologies, and security techniques used in data sharing with the smart city. This includes analysis such as how data sharing takes place in smart governance application, which technologies are used, how can operational efficiencies be improved, how involving the citizens can have better outcomes. Here, a connection between these blocks can be seen with the ability to determine how these technologies can be used for preserving privacy and protecting security.

Page Configuration	Standard
Security Relationships	The security relationship diagram illustrates the fundamental building blocks of privacy protection and security in a smart city. This diagram demonstrates the relationship between these building blocks such as privacy elements, security design, privacy & security recommendations, smart technologies used in privacy protection, types of privacy and security issues, type of attacks and attackers, sources of data attacks, and privacy enabling technologies. Here, a connection between these blocks can be seen with the ability to dive deep into how security can be addressed in a smart city. This involves sense checking the entire data management lifecycle using IoT, big data, and inter-agency data sharing.

Table 6: Web-system Overview - Smart City Framework

Next, we identify the key stakeholders who will receive the maximum value from our framework. Furthermore, we define the interactive digital resources on the challenges related to privacy-protected data sharing, and a solution to mitigate these challenges. Additionally, we identify the smart city applications that this solution can be used on and architectural measures to ensure privacy-protected data sharing. To explain our framework in detail, we establish the relationship between privacy and security, and the impact on smart city operations.

4.1 Identification of stakeholder for our interactive resources

This section provides an overview of the stakeholders identified in our research. These stakeholders have a primary interest in the smart city, its functions and frameworks, the overall experience, needs, pain points, and outcomes revolve around them. With our resources, we aim to create an impactful engagement among stakeholders through interactivity. The success criterion is to enhance the users' motivation, enabling them to achieve their goals.

In the initiation phase of this research, we tried to identify a target audience for the knowledge – primarily in the form of research that exists and resources we collated as we progressed through the project. This research presents an opportunity to engage with multidisciplinary stakeholders. Additionally, this enables collaboration with researchers who are authorities on the subject. In the past, frameworks were based on technology rather than people. We have observed that for smart cities, the framework must primarily serve people, or roles, mainly stakeholders. The key stakeholders identified were the IT experts, data custodians, domain experts, legitimate and malicious providers, consumers, and governing bodies (Sanseverino, Sanseverino, Vaccaro, Macaione, & Anello, 2017; Tay, Supangkat, Cornelius, & Arman, 2018; Andrisano et al., 2018, Yigitcanlar et. al., 2018; Kodali, Azman, & Panicker, 2018; and Rjab, Ben, & Mellouli, 2018).

Table 7 depicts the stakeholder map along with their key pain points when designing the smart city. Our resources are targeted at addressing the pain points and keeping in view the interests of these stakeholders throughout the process of implementing our digital resources.

Stakeholder Role	Profile	Pain Points	Interest
IoT Service Provider organisation (Alliance for Telecommunications Industry Solutions, 2018)	• Develops IoT devices and technologies	• Lack of visibility into client issues (Shah & Patel, 2014). • Limited understanding of other key aspects of the smart city (Nam & Pardo, 2011). • Limited time to perform research on case studies (Sanseverino et al., 2014).	The Smart City framework, in this research, will act as a reference guide keeping into consideration various security and privacy parameters, technologies, methods and processes of the smart city in the development of the interactive resources.
Local Councils, City & State Government Departments (Jiong & Gubbi et al., 2014)	• Manages cities resources in order to achieve the best outcomes and living environment for citizens in a sustainable manner • Consumes IoT technologies and various data analytics methods to develop a Smart city.	• Lack of knowledge of Smart City practices, models, and challenges. (Berntzen, & Johannessen, 2016) • Limited time to perform research on case studies (Sanseverino et al., 2017) • Limited access to the domain expertise summarised for a business case. (Lim, Kim, & Maglio, 2018)	The Smart City framework, in this research, provides a measure of quality assurance, for benchmarking purposes, and will act as the reference guide for systems development and business case development.
Other organisations (Private sector/ Public-sector) (IoT Alliance Australia, 2017)	• Operates on businesses across various industry verticals such as healthcare, shopping centre, utilities, transportation, etc. • Consumes IoT technologies and various data analytics methods to develop a Smart city	• Lack of visibility into privacy and security related issues for citizens (Puron-Cid, Gabriel, 2015) • Lack of knowledge on Smart City practices, models and challenges (Yigitcanlar et al., 2018) • Limited time to perform research on case studies (Sanseverino et al., 2017) • Limited access to the domain expertise summarised for a business case. (Lim, Kim & Maglio, 2018)	The Smart City framework, in this research, provides a measure of quality assurance, for benchmarking purposes, in performing technology assessment and evaluation of options and will act as the reference guide for systems development and business case development.
Researchers (Ismail 2016)	• Consumes knowledge and domain expertise that has been established in the context of Smart City • Reproduce, modify existing knowledge and develop new knowledge on Smart City	• Limited amount of well-orchestrated knowledge and domain expertise available in the context of a Smart City (Anthopoulos, 2015) • Time must be expensed in order to develop a relationship between key areas of the Smart City (Sikora-Fernandez, Dorota, Stawasz, & Danuta, 2016)	The Smart City framework, in this research, will act as a one-stop-shop of the key areas under Smart City Incl. Privacy, Security, and Big Data providing details on the key challenges, implemented solutions, possible applications, and architecture).

Stakeholder Role	Profile	Pain Points	Interest
Citizens (Simonofski, Asensio, De Smedt, & Snoeck, 2017)	• Consumer of services in a Smart City that employs various complex tools, methods, and technologies	• Lack of transparency and visibility within processes leading to their apprehensions in the use of the tools available in a Smart city (Johannessen, & Berntzen, 2018). • Concerns for Privacy and Security issues and lack of understanding to establish trust (Elmaghraby, & Adel, 2013).	The Smart City framework, aids in breaking down complex concepts into simple understanding providing subject matter knowledge and domain expertise to establish a transparent process and assure quality measures adopted in the Security & Privacy of citizens.

Table 7: Stakeholder Map – Smart City Framework

In the next section, we provide a detailed explanation of our digital resources.

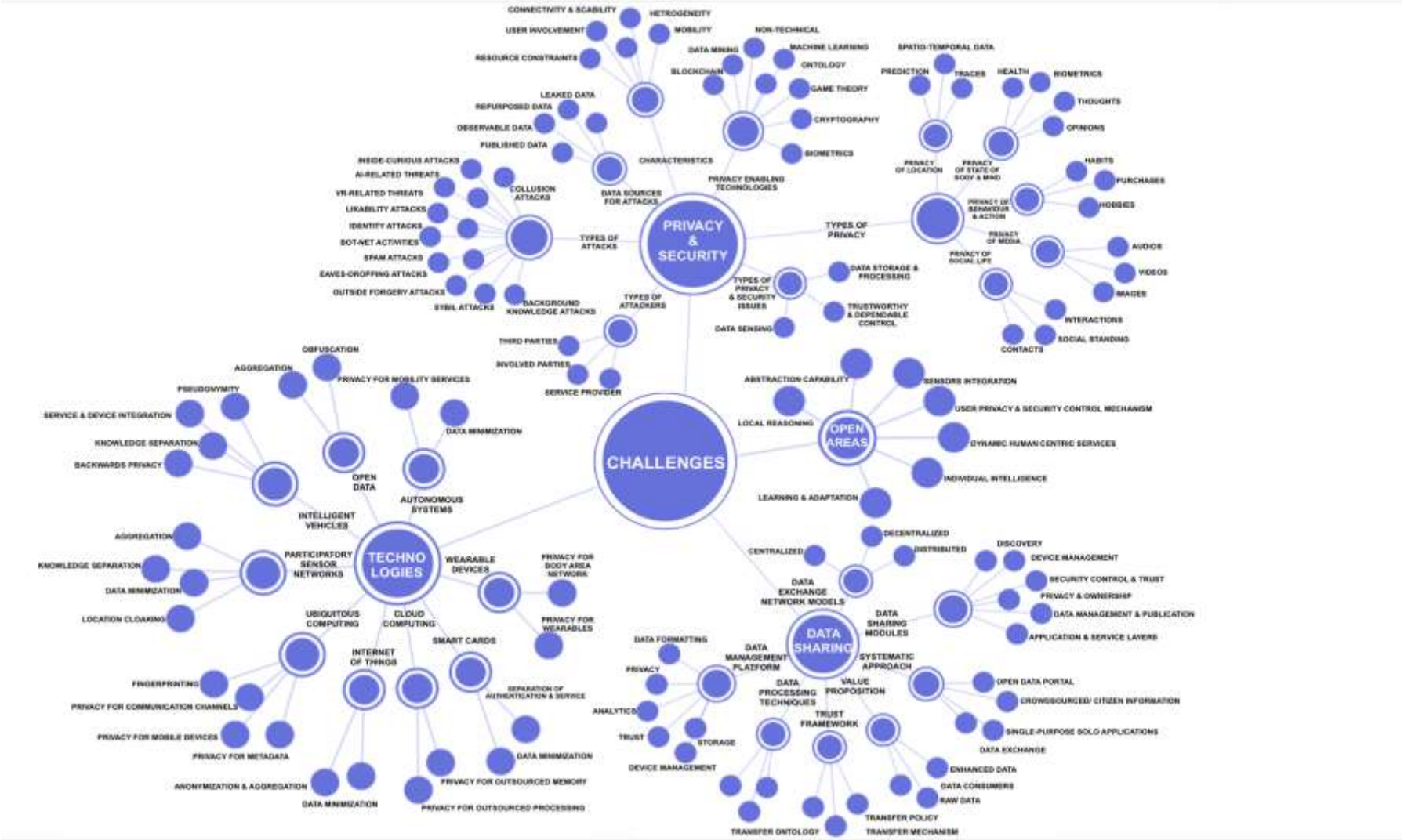

Figure 6: Force-directed Tree – Challenges – Smart City Framework

4.2 Challenges related to privacy-protected data sharing within smart cities

Emerging technologies are forming the building blocks of smart cities, but there is a lack of a comprehensive and established framework for sharing data with relevant bodies within a smart city. As part of our research, we attempt to establish the relationships between core concepts of privacy and security in the context of smart cities. Privacy is a state in which an individual is not observed by others, while security is a state of being free from threat. Privacy protection is delivered into two steps, i) Privacy by Design (PbD) focused on which data to secure, where to store it and who to authorize access, ii) Privacy Enhancing Technologies (PET) – an implementation approach offering tools to preserve privacy by reducing personal data, coupled with an inability to identify individuals. Security is often followed by enforcing legislation and policies to avoid breaches. The data sharing exposes citizens' data, including personally identifiable information, and possible attacks to the smart city systems. Secure data transfer is another important area requiring attention as it occurs in many smart city applications. The over-collection of data may also lead to ethical concerns (Alohali, Merabti, & Kifayat, 2014; Memmi, Kapusta, & Qiu, 2015; Cao et al., 2016; Moreno et al., 2017; Moura & Serrao, 2016; Steuer, Benabbas, Kasrin, & Nicklas, 2016; Elmisery, Sertovic, & Gupta, 2017; Tawalbeh, Tawalbeh, Song, & Jararweh, 2017; Mohammadi, Al-Fuqaha, Guizani, & Oh, 2018; Tanaka, de Barros, & de Souza Mendes, 2018; Liu, Zhang, & Fang, 2018; Soultatos et al., 2018; Rastogi, Singh, & Singh, 2018; Essa, Al-Shoura, Al-Nabulsi, Al-Ali, & Aloul, 2018).

To understand these issues, we created an interactive resource illustrated in Figure 6 that consolidates these issues so that the best practices may be proposed, keeping data security and citizens' privacy at the heart of the design of this framework.

4.3 Solutions to achieve privacy protected data sharing within smart cities

In light of the challenges outlined in the previous section, the introduction of emerging technology in smart cities brings an increase in ethical issues related to the stage of data. Since the technologies used for data capture are ubiquitous in nature, it is important to ensure that the cloud they are hosted on is fully secured via encryption, with traceability via a cryptosystem. The next issue is data sharing – all interagency systems must be interoperable, fully secured, and have a strong audit mechanism in place. Other elements that focus on ensuring a secure architecture with privacy by design to consider are measures for integration and abstraction capability, individual intelligence and local reasoning, learning and adaptation, and human-centric services (Luo, Ren, Hu, Wu, & Lou, 2017; Masduki, Ramli, & Salman, 2017; Fernandes, Rahmati, Eykholt, & Prakash, 2017; Esposito et. al., 2018; Xie, Wang, Wang, & Chang, 2018; Zhang & Zahng, 2018; Alketbi, Nasir, & Talib, 2018; Bellini, Nesi, Paolucci, & Zaza, 2018; Pradhan, Fuchs, & Johnsen, 2018; Sinaeepourfard, Krogstie, & Peterse, 2018; Badii et al., 2018; Siddiqui, Tayan, & Khan, 2018). To synthesize these solution measures, we derived our resource through mapping the key challenges and solution e.g., ethical challenges, lessons learned, approaches. We identified the solution to the pain points of the various types of stakeholders within the smart city. We also investigated smart city best practices for the adoption of new technology. Additionally, through our knowledgebase, we offer an explanation on entities to provide a guidance to the stakeholders, available from http://ausdigitech.com/smartcity/definitions.html.

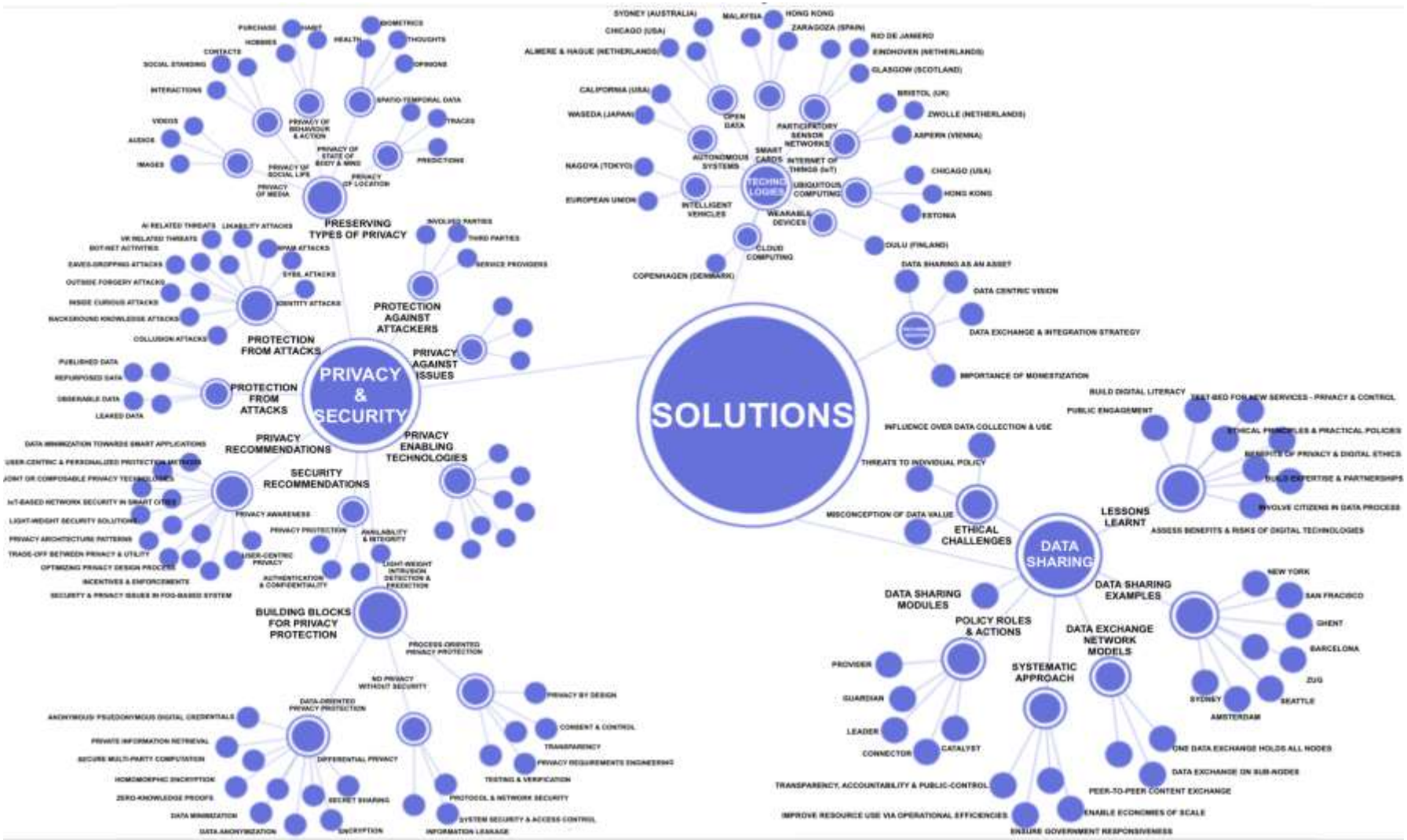

Figure 7: Force-directed Tree – Solution – Smart City Framework

Figure 7 illustrates our resource related to the solution we have synthesized and proposed as part of the smart city framework. This resource addresses solutions for the challenges associated with the increased use of emerging technologies focusing on privacy, security, data sharing, and open areas, such as scalability and extensive use of things.

4.4 Portfolio of Applications within the smart city using technology for data sharing

Countries have different goals for the adoption of technology to improve the quality of service, achieve operational efficiencies, interagency data exchange, and data-driven decision making by the administration. In India, the government has a mission to develop 100 smart cities by 2020. This can be achieved by adopting a wide range of emerging technologies offering an opportunity for agencies to collaborate. With time, citizens have moved from passive to active roles by conducting transactions, consulting with government online, and participating through digital forums. Smart city applications help with managing day-to-day aspects of life in an integrated fashion. This helps to provide not only excellent service delivery for citizens but also to drive great stakeholder outcomes (Layne & Lee, 2001; Haiyan, 2016; Chakrabarty & Engels, 2016; Kor, Pattinson, Yanovsky, & Kharchenko, 2016; Agarwal & Tripathi, 2017; Bibri & Krogstie, 2017; Beleuta & Delgado Merce, 2017; Liu, Zhang, & Fang, 2018; Kesswani & Kumar, 2018; Alliance for Telecommunications Industry Solutions, 2018; Ryu, Sharma, Jo, & Park, 2019).

Figure 8 illustrates our contribution to the synthesis of information on how technology is embedded within the smart city with the following suite of applications.

1. **Smart services**: focused on improving the quality of life by delivering digital services.
2. **Smart transportation**: offers an efficient road network, traffic mobility, and predictability, and shipping value chain (Swarnkar & Bhadoria, 2017; Feibert, Hansen, & Jacobsen, 2017).
3. **Smart environment**: reduce the carbon footprint, monitor air quality and manage waste (De Carolis, Macchi, Negri, & Terzi, 2017; Borges et al., 2017; Lokuliyana et al., 2018).
4. **Smart utilities**: offer transactional services accessible via digital channels to achieve sustainable water quality, telephone, mobile network, and electricity (Hong & Liu, 2019).
5. **Smart government**: allows citizens to interact with the government digitally (West, 2004).

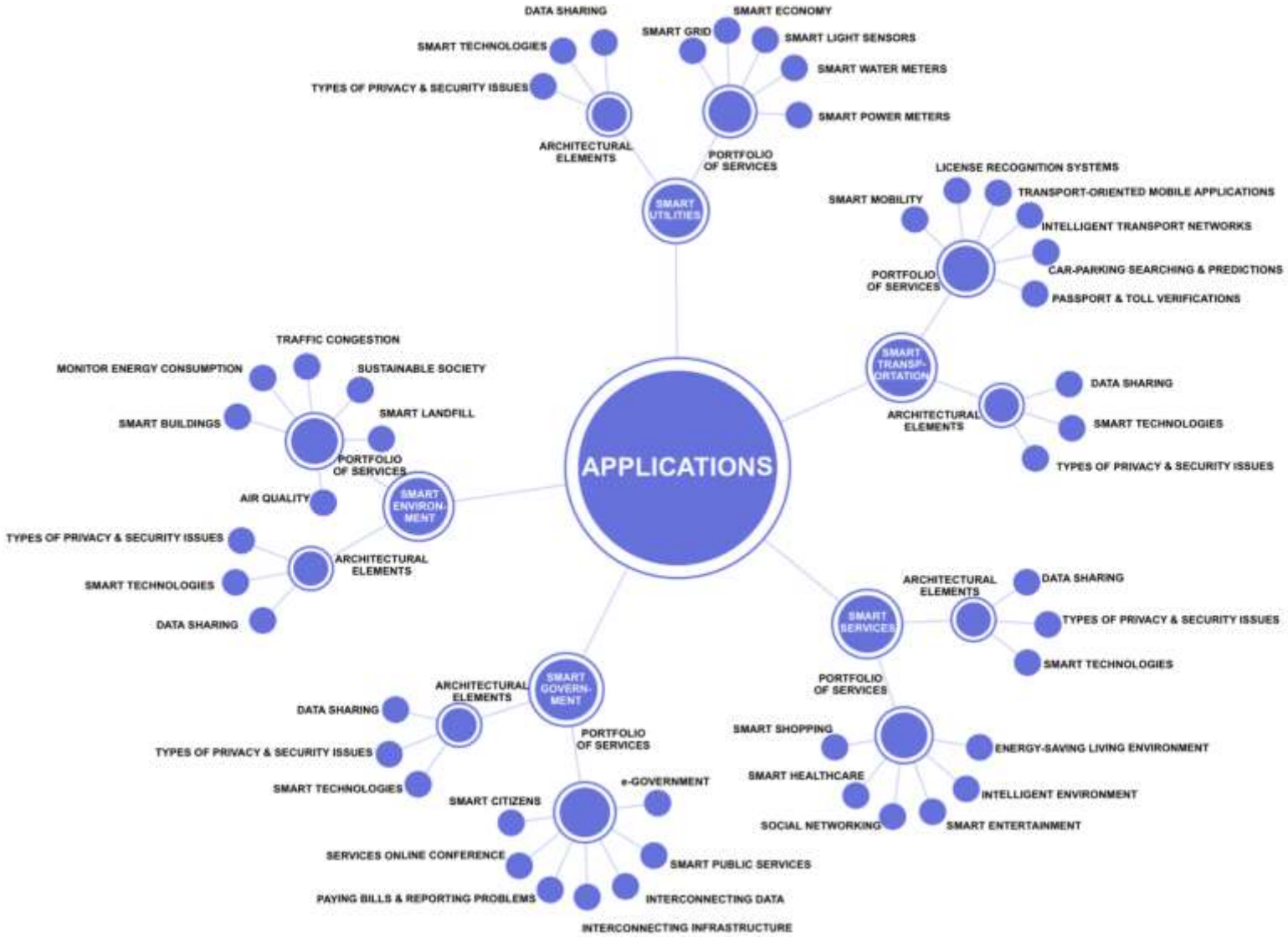

Figure 8: Force-directed Tree – Applications – Smart City Framework

4.5 Architectural considerations to ensure privacy-protected data sharing

Research suggests that by this year the number of connected "machine to machine" devices will be about 50 billion. When a smart city is designed, the architectural framework of existing systems and the modern-day technologies to be adopted by the city, play a significant role in its planning. There are several layers of abstraction involved from data collection to its use in a smart city application. These layers include the data collection layer, data ingestion layer, data processing, data analysis layer and data presentation layer. Sensors, network, and connectivity play a critical role in the data collection and ingestion layers. Big data analysis plays a significant role in the data processing and analysis layers, for knowledge extraction to actionable insights. Data sharing and exchange channels play a major role in the data presentation layer within the smart city application (Tragos, Fragkiadakis, Angelakis, & Pöhls, 2016; Marjani et al., 2017; Elsaeidy et al., 2017; Achmad, Nugroho, & Djunaedi, 2018; Riboni, 2019).

The other significant areas of consideration when designing smart city architecture are to ensure interoperability, resilience, fault-tolerance, scalability, and modularity. Figure 9 represents our resource representing smart city architectural considerations. The smart city applications are hosted in the cloud using either fog, or edge computing. In fog computing, the data is aggregated, processed and analysed away from sensor whereas, in edge computing, all functions are performed closer to the sensors. Researchers prescribe to use multi-factor authentication for privacy protection and security mitigation techniques such as encryption and security by design. The architectural considerations vary for the range of smart city applications having high to low impact on operations by maintaining the availability and integrity, authentication and confidentiality (Inukollu, Arsi, & Rao Ravuri, 2014; Yan, Yu, & Ding, 2017; Wang, Yang, Xavier, & Li, 2018; IoT Alliance Australia, 2017; Alromaihi, Elmedany, & Balakrishna, 2018; Falco, Viswanathan, Caldera, & Shrobe, 2018; Yadav & Vishwakarma, 2018).

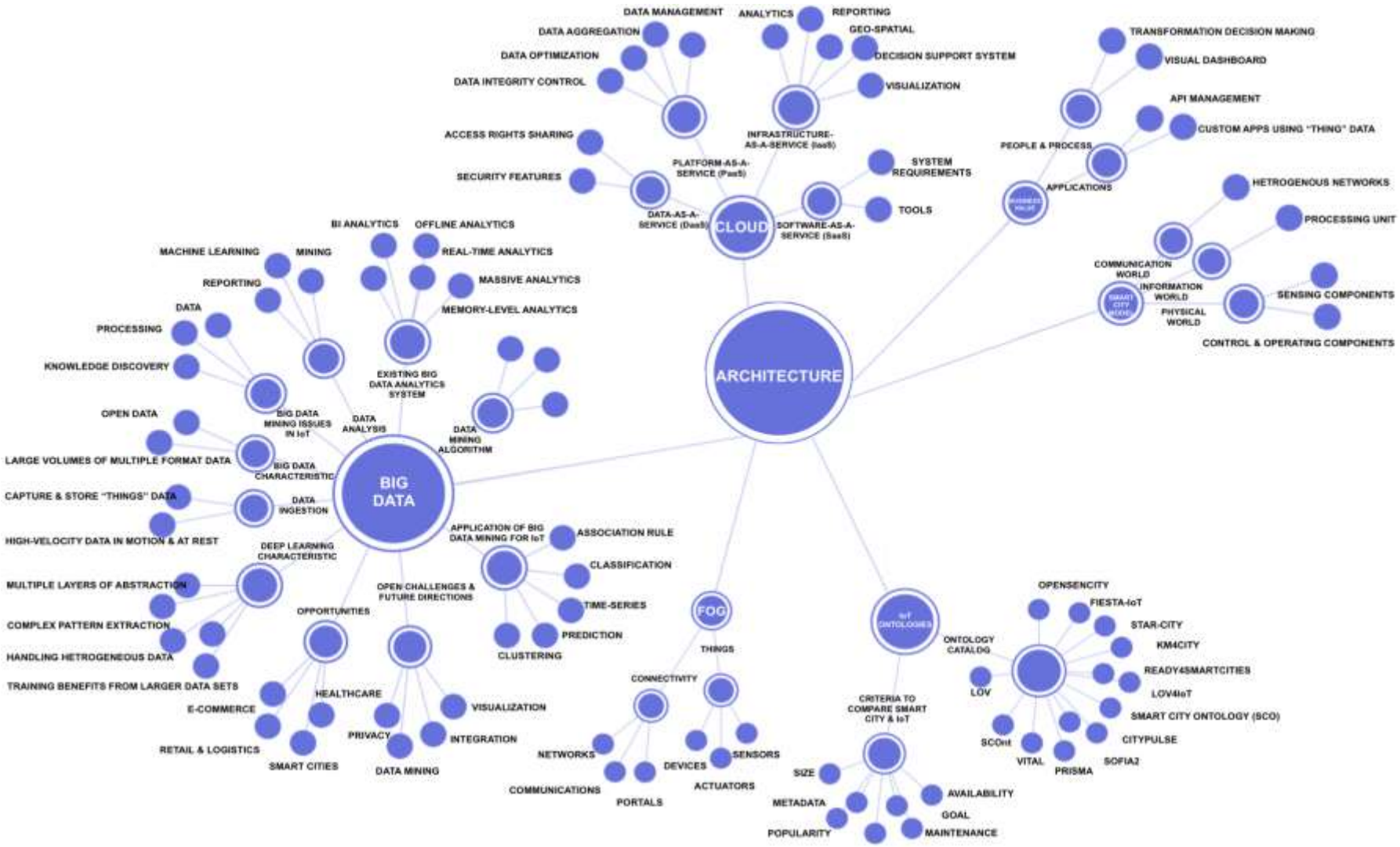

Figure 9: Force-directed Tree – Architecture – Smart City Framework

4.6 Smart city applications relationship model with the aspects of data sharing

The smart city application relationship model demonstrates relationships between the portfolio of applications and key aspects of data sharing in a privacy-preserving fashion. The smart city application portfolio comprises applications, and services provided by the city resulting in generating, analysing and sharing a large volume of data. With this relationship diagram, we intend to understand the impact that technology has on each of these applications and the techniques to mitigate privacy, security, and data sharing related issues. This will enable smart city stakeholders to consider and plan for these elements at the time of designing smart city architecture (Fernandez Molanes, Amarasinghe, Rodriguez-Andina, & Manic, 2018; Mohammadi & Al-Fuqaha, 2018). Since numerous relationships exist among nodes within a relationship model illustrated in Figure 10, for the ease of demonstration, we elaborate "Smart Governance" highlighted in black in the figure below. The interactive resource for this relationship model is available from http://ausdigitech.com/smartcity/apps-relationship.html.

Smart governance is a branch of a smart city that focuses on providing services to citizens via digital channels from the submission of an application, to the termination of that service. The applications that form part of smart governance are interconnecting frameworks of data sharing for smart citizen services via online portals, mobile applications, QR codes, and online payment gateways. Smart technologies that are used for the enablement of smart governance include smart cards, cloud, open data, ubiquitous computing, and other IoT devices for sensing data. These methods of data collection trigger privacy concerns, which can be mitigated by using security preserving methods and privacy protection techniques such as privacy by design, i.e. to weave privacy in the DNA of the application. To ensure that data is analysed, various methods of data sharing can be used. For example, just enough data collection, establishing secure exchanges and applying ethical principles when undergoing peer-to-peer exchange.

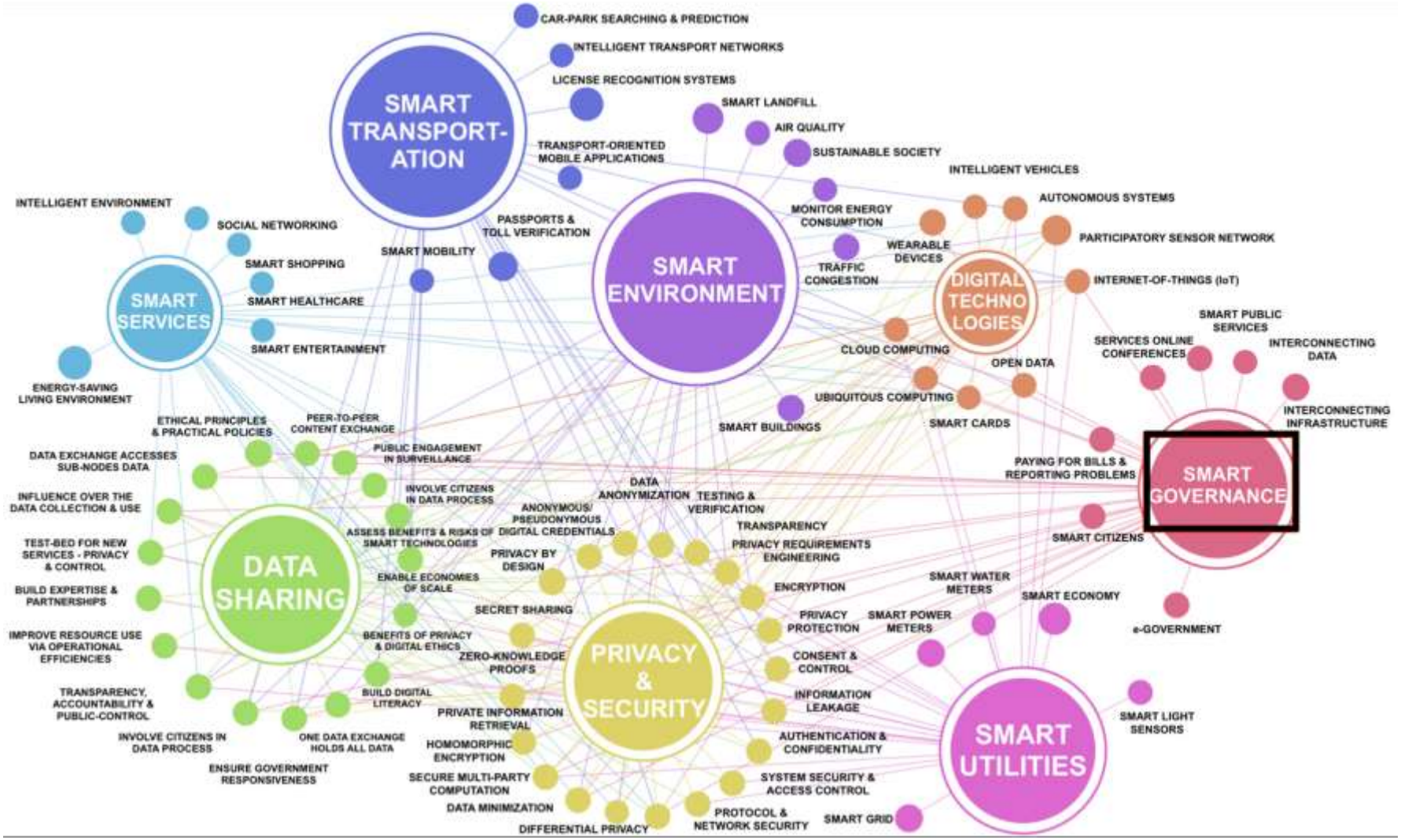

Figure 10: Force-directed Network – Smart City Application Relationship – Smart City Framework

4.7 Privacy and security relationship model with aspects of smart city applications

Privacy and security must be considered as fundamental building blocks of data collected, processed, and shared by the smart cities. The privacy and security relationship model helps stakeholders understand the areas to focus on when designing architecture. Through our relationship model, we highlight the relationship between the technology used in smart cities and the types of attacks attributed to privacy and security within a smart city. Additionally, we correlate this to the types of attackers involved, the data sources they can breach, and the privacy enabling technologies used. We offer the privacy and security recommendations that can help save the cities from those attacks or take appropriate measures for mitigation (Luo et. al., 2019; Liu, Nakauchi, & Shoji, 2018; Zhang et al., 2015; Feng, & Zhao, 2018; Kuan et al., 2017). Since numerous relationships exist within a relationship model as illustrated in Figure 11. For the ease of demonstration, we elaborate on "Data sources for an attack" highlighted in black in the figure below, also available from http://ausdigitech.com/smartcity/security-relationship.html.

Data sources for attack provide information on four types of data sources that can be attacked including:

- attacks based on the data that has been leaked during a data exchange;
- data that has been used for observation purposes;
- data that has been repurposed, i.e. it was used for one purpose and later on disposed of or reused for other purposes; and finally
- data that has been published but has exposed too much information about the information that has not been published.

We demonstrate how data sources for attack can be interrelated to profiles of attackers – this helps trace back to the data source where the breach took place. Based on the relationship of data sources to types of data, it is possible to determine the type of attacks that various types of data sources can trigger. For example, repurposed data is likely to undergo a collusion attack or background knowledge attack, whereas published data is likely to undergo an identity attack or outside forgery attack. The profile of an attacker can be determined once the source of data is identified, i.e., an attack on observable data is most likely to be carried out by the service provider, whereas, an attack caused due to leaked data pragmatically relates to third parties involved.

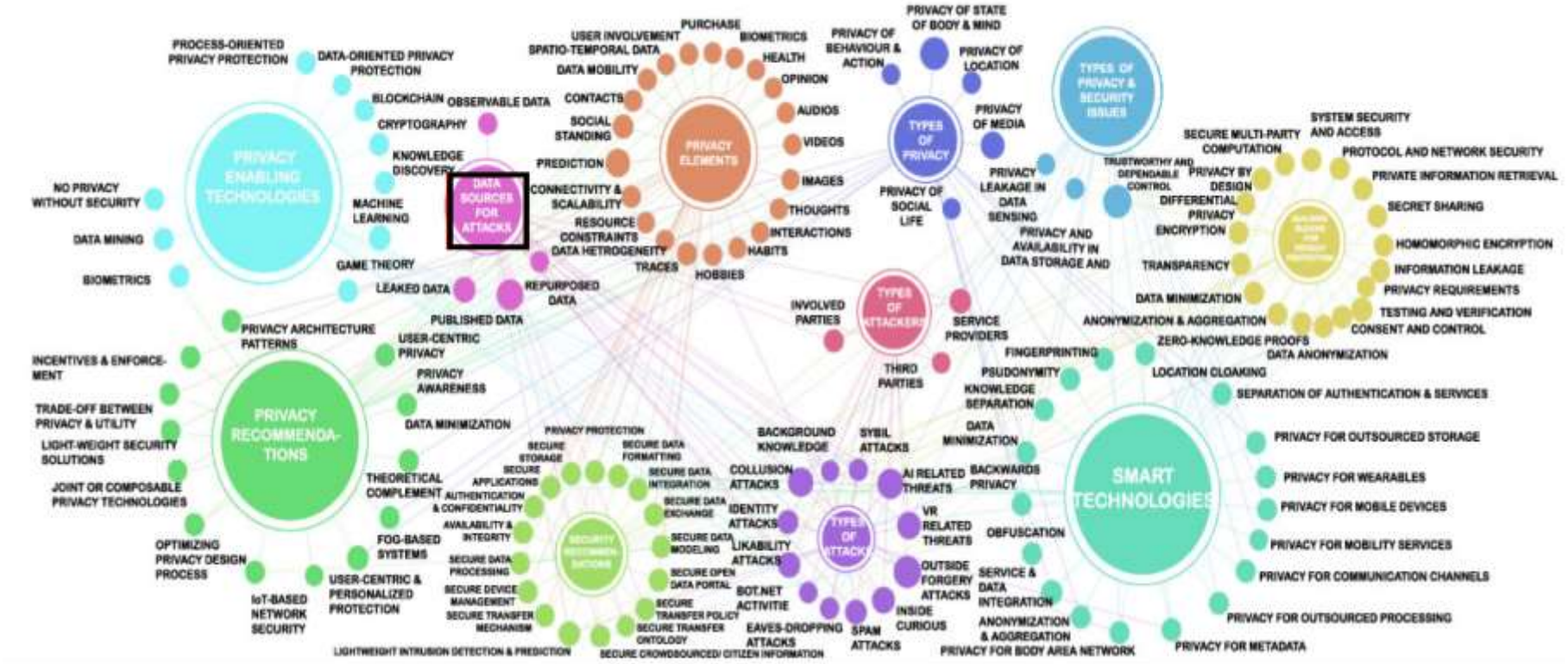

Figure 11: Force-directed Network – Smart City Security Relation – Smart City Framework

5 Conclusion

Smart city operations thrive on the data collected within the city. We identified that the security and privacy of this data are paramount in the real-time decision-making process. A security or privacy breach can have a significant impact not only on the operations of the city and quality of service outcomes but can also result in trust issues among the citizens and the administration. To address this challenge, we designed a holistic smart city framework that provides the building blocks and highlights the relationship between them. These building blocks are focused on the important aspects of a city, including the challenges faced, solutions offered, applications in consideration, and architectural recommendations. We also derived a knowledge base with several terms used in the context of smart cities to help future researchers and smart city stakeholders to navigate through the problem areas effectively. Furthermore, to deliver an impactful learning experience, we adopted pedagogical techniques to present our framework using web-based interactive resources, which impart on-demand knowledge to users.

We intend to undertake further research to explore the evolving trends within smart city domains and update the digital resources periodically. Additionally, we intend to extend our website, which contains interactive resources in the form of a content delivery platform so that researchers and smart city stakeholders can contribute towards the knowledge. This adaptation of our website into a centralized portal will offer a platform for researchers to digitally configure resources. This will further enable them to focus on the targeted delivery of content according to the role and interests of the stakeholder focusing on emerging technologies within smart cities.

Acknowledgements

The researchers would like to thank and acknowledge the School of Computing and Mathematics, Charles Sturt University for its support in making this research possible.

References

Abi Sen, A. A., Eassa, F. A., & Jambi, K. (2018). Preserving privacy of smart cities based on the fog computing. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, LNICST, 224, pp. 185–191. https://doi.org/10.1007/978-3-319-94180-6_18

Achmad, K. A., Nugroho, L. E., & Djunaedi, A. (2018). Smart City Model: A Literature Review. 2018 *10th International Conference on Information Technology and Electrical Engineering* (ICITEE) Smart, pp. 488–493. https://www.researchgate.net/publication/328982472_Smart_City_Model_a_Literature_Review

Achmad, K. A., Nugroho, L. E., Djunaedi, A., & Widyawan. (2018). Smart City for Development: Towards a Conceptual Framework. Proceedings – 2018 *4th International Conference on Science and Technology*, ICST 2018. https://doi.org/10.1109/ICSTC.2018.8528677

Agarwal, N., & Tripathi, A. (2017). Big Data Security and Privacy Issues: A Review. *International Journal of Innovative Computer Science & Engineering*, 2(4), pp. 12–15. Retrieved from www.ijicse.in

Ahn, J., Lee, J. S., Kim, H. J., & Hwang, D. J. (2016). *Smart City Interoperability Framework Based on City Infrastructure Model and Service Prioritization*. ICUFN 2016, 337–342. Retrieved from https://doi.org/10.1109/icufn.2016.7537044

Ainane, N., Ouzzif, M., & Bouragba, K. (2018). *Data security of smart cities*. ACM, pp. 1–13. https://doi.org/10.1145/3286606.3286866

Alias Balamurugan, A., Lilian, J. F., & Sasikala, S. (2018). The Future Of India Creeping Up In Building A Smart City: Intelligent Traffic Analysis Platform. *Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies* (ICICCT 2018) IEEE, pp. 518–522. https://doi.org/10.1109/ICICCT.2018.8473194

Alketbi, A., Nasir, Q., & Talib, M. A. (2018). Blockchain for government services – Use cases, security benefits and challenges. 2018 *15th Learning and Technology Conference*, L and T 2018, 112–119. https://doi.org/10.1109/LT.2018.8368494

Alkhamisi, A., Nazmudeen, M. S. H., & Buhari, S. M. (2016). A cross-layer framework for sensor data aggregation for IoT applications in smart cities. *IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life*, ISC2 2016 – Proceedings. https://doi.org/10.1109/ISC2.2016.7580853

Alliance for Telecommunications Industry Solutions. (2018). *Smart Cities Data Sharing Framework*. Retrieved from www.atis.org/01_legal/patent-policy/

Alohali, B., Merabti, M., & Kifayat, K. (2014). A cloud of things (CoT) based security for home area network (HAN) in the smart grid. Proceedings – 2014 *8th International Conference on Next Generation Mobile Applications, Services and Technologies*, NGMAST 2014. https://doi.org/10.1109/NGMAST.2014.50

Alromaihi, S., Elmedany, W., & Balakrishna, C. (2018). Cyber security challenges of deploying IoT in smart cities for healthcare applications. Proceedings – 2018 *IEEE 6th International Conference on Future Internet of Things and Cloud Workshops, W-Fi Cloud* 2018, 140–145. https://doi.org/10.1109/W-FiCloud.2018.00028

Alsafery, W., Alturki, B., Reiff-Marganiec, S., & Jambi, K. (2018). Smart Car Parking System Solution for the Internet of Things in Smart Cities. *1st International Conference on Computer Applications and Information Security*, ICCAIS 2018. https://doi.org/10.1109/CAIS.2018.8442004

Andrisano, O., Bartolini, I., Bellavista, P., Boeri, A., Bononi, L., Borghetti, A., Borghetti, A., Brath, A., Corazza, G., Corradi, A., De Miranda, S., Fava, F., Foschini, L., Leoni, G., Longo, D., Milano, M., Napolitano, F., Nucci, C., Pasolini, G., Patella, M., Cinotti, T., Tarchi, D., Ubertini, F., & Vigo, D. (2018). The Need of Multidisciplinary Approaches and Engineering Tools for the Development and Implementation of the Smart City Paradigm. *Proceedings of the IEEE*, 106(4), pp. 738–760. https://doi.org/10.1109/JPROC.2018.2812836

Anthopoulos, L. (2015). Understanding the Smart City Domain: A Literature Review. *Transforming City Governments for Successful Smart Cities*, Part of the Public Administration and Information Technology book series (PAIT, 8). pp 9-21. https://doi.org/10.1007/978-3-319-03167-5_2

Assante, D., Romano, E., Flamini, M., Castro, M., Martin, S., Lavirotte, S., Rey, G., Leisenberg, M., Migliori, M., Bagdoniene, I., Gallo, R., Pascoal, A., & Spatafora, M. (2018). Internet of Things education: Labor market training needs and national policies. *IEEE Global Engineering Education Conference*, EDUCON, 1846–1853. https://doi.org/10.1109/EDUCON.2018.8363459

Ati, M., & Basmaji, T. (2018). Framework for managing smart cities security and privacy applications. ISCAIE 2018 – 2018 *IEEE Symposium on Computer Applications and Industrial Electronics*, pp. 191–194. https://doi.org/10.1109/ISCAIE.2018.8405468

Badii, C., Belay, E. G., Bellini, P., Cenni, D., Marazzini, M., Mesiti, M., Nesi, P., Pantaleo, G., Paolucci, M., Valtolina, S., Soderi, M., & Zaza, I. (2018). Snap4City: A Scalable IOT/IOE Platform for Developing Smart City Applications. *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation* (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp. 2109–2116. https://doi.org/10.1109/SmartWorld.2018.00353

Bajramovic, E., Waedt, K., Ciriello, A., & Gupta, D. (2016). Forensic Readiness of Smart Buildings Preconditions for Subsequent Cybersecurity Tests. *2016 IEEE International Smart Cities Conference* (ISC2), Trento, 2016, pp. 1-6. https://doi.org/10.1109/ISC2.2016.7580754

Bass, T., Sutherland, E., & Symons, T. (2018). Reclaiming the Smart City: Personal data, trust and the new commons. decode. *European Commission*. https://decodeproject.eu/file/380/download

Beleuta, V., & Delgado Merce, J. M. (2017). *Data privacy and security in Business Intelligence and Analytics.* https://www.semanticscholar.org/paper/Data-privacy-and-security-in-business-intelligence-Beleuta/93adc50037259b66127d5bf1ea6d15ee7dc1b893

Belgaum, M. R., Alansari, Z., Jain, R., & Alshaer, J. (2018). A Framework for Evaluation of Cyber Security Challenges in Smart Cities. *Smart Cities Symposium 2018*, Bahrain, 2018, pp. 1-6. https://ieeexplore.ieee.org/document/8643178

Bellini, P., Nesi, P., Paolucci, M., & Zaza, I. (2018). Smart city architecture for data ingestion and analytics: Processes and solutions. Proceedings: *IEEE 4th International Conference on Big Data Computing Service and Applications*, BigDataService 2018, pp. 137–144. https://doi.org/10.1109/BigDataService.2018.00028

Berntzen, L., & Johannessen, M. (2016). The Role of Citizens in "Smart Cities". *Conference: Management – international conference, at Slovakia: Faculty of Management, University of Presov. October 2016*. https://www.researchgate.net/publication/309040628_The_Role_of_Citizens_in_Smart_Cities

Bibri, S. E., & Krogstie, J. (2017). The core enabling technologies of big data analytics and context-aware computing for smart sustainable cities: A review and synthesis. *Journal of Big Data*, 4(1). https://doi.org/10.1186/s40537-017-0091-6

Boban, M., & Weber, M. (2018). Internet of Things, legal and regulatory framework in digital transformation from smart to intelligent cities. 2018 *41st International Convention on*

Information and Communication Technology, Electronics and Microelectronics (MIPRO). https://doi.org/10.23919/MIPRO.2018.8400245

Borges, M. A., Melo, G. F., De Massaki, C., Igarashi, O., Lopes, P. B., & Silva, L. A. (2017). An architecture for the internet of things and the use of big data techniques in the analysis of carbon monoxide. Proceedings – *2017 IEEE International Conference on Information Reuse and Integration*, IRI 2017, 184–191. https://doi.org/10.1109/IRI.2017.76

Brauchli, A., & Li, D. (2015). A solution-based analysis of attack vectors on smart home systems. *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications*, SSIC 2015 – Proceedings. https://doi.org/10.1109/SSIC.2015.7245682

Budhiputra, P. M., & Putra, K. P. (2016). Smart City Framework Based on Business Process re-engineering approach. *2016 International Conference on ICT For Smart Society*, pp. 69–73. https://doi.org/10.1109/ICTSS.2016.7792851

Cam-Winget, N., Sadeghi, A, & Jin, Y. (2016). Invited - Can IoT Be Secured: Emerging Challenges in Connecting the Unconnected. *Proceedings of the 53rd Annual Design Automation Conference. DAC '16*, Austin, TX, 122, pp. 6. https://doi.org/10.1145/2897937.2905004

Cao, Q. H., Khan, I., Farahbakhsh, R., Madhusudan, G., Lee, G. M., & Crespi, N. (2016). A trust model for data sharing in smart cities. *2016 IEEE International Conference on Communications*, ICC 2016. https://doi.org/10.1109/ICC.2016.7510834

Cárdenas, A. A., & Safavi-Naini, R. (2012). Security and Privacy in the Smart Grid. In *Handbook on Securing Cyber-Physical Critical Infrastructure* (pp. 637–654). https://doi.org/10.1016/b978-0-12-415815-3.00025-x

Chakrabarty, S., & Engels, D. W. (2016). A secure IoT architecture for Smart Cities. 2016 *13th IEEE Annual Consumer Communications and Networking Conference*, CCNC 2016. https://doi.org/10.1109/CCNC.2016.7444889

Chan, A. L., Chua, G. G., Chua, D. Z. L., Guo, S., Lim, P. M. C., Mak, M. T., & Ng, W. S. (2018). Practical experience with smart cities platform design. *IEEE World Forum on Internet of Things*, WF-IoT 2018 – Proceedings, 2018-January, pp. 470–475. https://doi.org/10.1109/WF-IoT.2018.8355181

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access*, 6, pp. 46134–46145. https://doi.org/10.1109/access.2018.2853985

De Carolis, A., Macchi, M., Negri, E., & Terzi, S. (2017). Guiding manufacturing companies towards digitalization: A methodology for supporting manufacturing companies in defining their digitalization roadmap. *IEEE Access*, pp. 487–495. https://doi.org/10.1109/ICE.2017.8279925

Doynikova, E., & Kotenko, I. (2017). Enhancement of probabilistic attack graphs for accurate cyber security monitoring. In 2017 *IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*

(SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). http://doi.org/10.1109/UIC-ATC.2017.8397618

Eckhoff, D., & Wagner, I. (2018). Privacy in the Smart City – Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys and Tutorials*, 20(1), pp. 489–516. https://doi.org/10.1109/COMST.2017.2748998

El hendy, M., Miniaoui, S., Atalla, S., & Hashim, K. (2017). A Survey on Smart City Technologies, Initiatives and Global Technology Providers. Association for Computing Machinery. *Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing*. ICC '17, 84, pp. 7. https://doi.org/10.1145/3018896.3025132

Elmaghraby, A. (2013). Security and Privacy in The Smart City. *6th Ajman International Urban Planning Conference* AIUPC 6: "City and Security" At: Ajman, UAE. March 2013. https://www.researchgate.net/publication/269874307_SECURITY_AND_PRIVACY_IN_THE_SMART_CITY

Elmisery, A. M., Sertovic, M., & Gupta, B. B. (2017). Cognitive Privacy Middleware for Deep Learning Mashup in Environmental IoT. *IEEE Access*, pp. 1–12. https://doi.org/10.1109/ACCESS.2017.2787422

Elsaeidy, A., Elgendi, I., Munasinghe, K. S., Sharma, D., & Jamalipour, A. (2017). A smart city cyber security platform for narrowband networks. 2017 *27th International Telecommunication Networks and Applications Conference*, ITNAC 2017. https://doi.org/10.1109/ATNAC.2017.8215388

Esposito, C., Castiglione, A., Frattini, F., Cinque, M., Yang, Y., & Choo, K. K. R. (2018). On Data Sovereignty in Cloud-based Computation Offloading for Smart Cities Applications. *IEEE Internet of Things Journal*, pp. 1–15. https://doi.org/10.1109/JIOT.2018.2886410

Essa, A., Al-Shoura, T., Al Nabulsi, A., Al-Ali, A. R., & Aloul, F. (2018). Cyber Physical Sensors System Security: Threats, Vulnerabilities, and Solutions. *2nd International Conference on Smart Grid and Smart Cities*, ICSGSC 2018, pp. 62–67. https://doi.org/10.1109/ICSGSC.2018.8541316

Estevez, E., & Janowski, T. (2013). Electronic governance for sustainable development – Conceptual framework and state of research. *Government Information Quarterly*, 30 (2013), S94–S109. https://doi.org/10.1016/j.giq.2012.11.001

Falco, G., Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities. *IEEE Access*, 6, 48360–48373. https://doi.org/10.1109/ACCESS.2018.2867556

Feibert, D. C., Hansen, M. S., & Jacobsen, P. (2017). An Integrated Process and Digitalization Perspective on the Shipping Supply Chain – A Literature Review. *Proceedings of the 2017 IEEE IEEM*, pp. 1352–1356. https://doi.org/10.1109/IEEM.2017.8290113

Feng, X., & Zhao, Y. (2018). Digital forensics challenges to big data in the cloud. Proceedings – 2017 IEEE International Conference on Internet of Things, *IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data*, IThings-GreenCom-CPSCom-SmartData 2017. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.132

Feng, X., Dawam, E. S., & Amin, S. (2017). A New Digital Forensics Model of Smart City Automated Vehicles. Proceedings – *2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Dat*a, IThings-GreenCom-CPSCom-SmartData 2017, pp. 274–279. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.47

Fernandes, E., Rahmati, A., Eykholt, K., & Prakash, A. (2017). Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? *IEEE Security & Privacy*, 15(1), pp. 79–84. https://doi.org/10.1109/MSP.2017.3151346

Fernandez Molanes, R., Amarasinghe, K., Rodriguez-Andina, J., & Manic, M. (2018). Deep learning and reconfigurable platforms in the internet of things: Challenges and opportunities in algorithms and hardware. *IEEE Industrial Electronics Magazine*. https://doi.org/10.1109/MIE.2018.2824843

Ferrer, A. J., Marquès, J. M., & Jorba, J. (2019). Towards the Decentralised Cloud. *ACM Computing Surveys*, 51(6), 1–36. https://doi.org/10.1145/3243929

Foucault, J., & Moulier-Boutang, Y. (2015). Towards economic and social "sensors": Condition and model of governance and decision-making for an organological Smart City. *2015 International Conference on Smart and Sustainable City and Big Data* (ICSSC), Shanghai, 2015, pp. 106-112. https://ieeexplore.ieee.org/document/7446445

Ghirardello, K., Maple, C., Ng, D., & Kearney, P. (2018). Cyber security of smart homes: Development of a reference architecture for attack surface analysis. Proceedings: *IEEE. Living in the Internet of Things: Cybersecurity of the IoT* – 2018. https://ieeexplore.ieee.org/document/8379732

Gyrard, A., Zimmermann, A., & Sheth, A. (2018). Building IoT based applications for Smart Cities: How can ontology catalogs help? *IEEE Internet of Things Journal*, pp. 1–22. https://doi.org/10.1109/JIOT.2018.2854278

Haiyan, S. C. (2016). Digital education resource configuration mode transformation from the co-construction and sharing to the public to be shared. *2016 Eighth International Conference on Measuring Technology and Mechatronics Automation*. https://doi.org/10.1109/ICMTMA.2016.64

Harris, S. (2014). Securing Big Data in our Future Intelligent Cities. *IET Conference on Future Intelligent Cities*. pp. 1–4. https://www.researchgate.net/publication/300490699_Securing_Big_Data_in_our_Future_Intelligent_Cities

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., & Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management*, 36(5), pp. 748–758. https://doi.org/10.1016/j.ijinfomgt.2016.05.002

Hassanain, E., Rahman, M. A., Alhamid, M. F., Hossain, M. S., Guizani, M., & Rashid, M. M. (2019). Blockchain and IoT-based Cognitive Edge Framework for Sharing Economy Services in a Smart City. *IEEE Access*. https://doi.org/10.1109/access.2019.2896065.

Hong, J., & Liu, C. C. (2019). Intelligent Electronic Devices with Collaborative Intrusion Detection Systems. *IEEE Transactions on Smart Grid*, pp. 1–11. https://doi.org/10.1109/TSG.2017.2737826

Inquiry into the Australian Government's role in the development of cities Submission 37. IoT and Government's Role in The Development of Cities; Submission to The Standing Committee on Infrastructure. Transport and Cities. *IoT Alliance Australia* July 2017. https://www.aph.gov.au/DocumentStore.ashx?id=229cdb32-7586-4867-8e40-d43158edf35f&subId=514420

Inukollu, V. N., Arsi, S., & Rao Ravuri, S. (2014). Security Issues Associated with Big Data in Cloud Computing. *International Journal of Network Security & Its Applications*, 6(3), pp. 45–56. https://doi.org/10.5121/ijnsa.2014.6304

Ismail, N. (2016). Determining the Internet of Things (IOT) Challenges on Smart Cities: A Systematic Literature Review. *Journal of Information Systems Research and Innovation* 10(3), pp. 56–63,

Johannessen, M., & Berntzen, L. (2018). The Transparent Smart City. Smart Technologies for Smart Governments, *Public Administration and Information Technology book series* (PAIT, 24), pp 67-94. https://doi.org/10.1007/978-3-319-58577-2_5

Kesswani, N., & Kumar, S. (2018). The Smart-X Model for Smart Cities. Proceedings: *2018 IEEE 42nd Annual Computer Software and Applications Conferenc*e (COMPSAC). https://doi.org/10.1109/COMPSAC.2018.00112

Khan, Z., Pervez, Z., & Ghafoor, A. (2014). Towards cloud based smart cities data security and privacy management. Proceedings – *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, UCC 2014, pp. 806–811. https://doi.org/10.1109/UCC.2014.131

Kodali, R. K., Azman, M., & Panicker, J. G. (2018). Smart Control System Solution for Smart Cities. *2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (CyberC), Zhengzhou, China, 2018, pp. 89-893. https://doi.org/10.1109/CyberC.2018.00027

Kolozali, S., Bermudez-Edo, M., Davar, N. F., Barnaghi, P., Gao, F., Ali, M. I., … Tonjes, R. (2018). Observing the Pulse of a City: A Smart City Framework for Real-time Discovery, Federation, and Aggregation of Data Streams. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2872606

Kor, AL., Pattinson, C., Yanovsky, M., & Kharchenko, V. (2018). *IoT-enabled smart living. Technology for Smart Futures*, Springer, Cham, pp. 3-28. https://doi.org/10.1007/978-3-319-60137-3_1

Kuan, Z., Jianbing, N., Yang, K., Xiaohui, L., Ren, J., & Shen, X. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, pp. 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM

L'Heureux, A., Grolinger, K., Higashino, W. A., & Capretz, M. A. M. (2017). A gamification framework for sensor data analytics. Proceedings – *2017 IEEE 2nd International Congress on Internet of Things*, ICIOT 2017, pp. 74–81. https://doi.org/10.1109/IEEE.ICIOT.2017.18

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly*. 18, pp. 122–136. https://doi.org/10.1016/S0740-624X(01)00066-1

Li, D., Cao, J., & Yao, Y. (2015). Big data in smart cities. *Science China Information Sciences*, 58(10), 1–12. https://doi.org/10.1007/s11432-015-5396-5

Li, Y., Dai, W., Ming, Z., & Qiu, M. (2016). Privacy Protection for Preventing Data Over-Collection in Smart City. *IEEE Transactions on Computers*, 65(5), pp. 1339–1350. https://doi.org/10.1109/TC.2015.2470247

Lim C., Kim K., & Maglio P. (2018). *Smart cities with big data: Reference models, challenges, and considerations.* Elsevier, Volume 82, December 2018, pp. 86-99. https://doi.org/10.1016/j.cities.2018.04.011

Lin, H., Hu, J., Ma, J., Xu, L., & Yu, Z. (2017). A Secure Collaborative Spectrum Sensing Strategy in Cyber-Physical Systems. *IEEE Access*, 5, pp. 27679–27690. https://doi.org/10.1109/ACCESS.2017.2767701

Liu, J. K., Choo, K.-K. R., Huang, X., & Au, M. H. (2017). Erratum to: Special issue on security and privacy for smart cities. *Personal and Ubiquitous Computing*, 21(5), pp. 777–777. https://doi.org/10.1007/s00779-017-1062-9

Liu, J., Zhang, C., & Fang, Y. (2018). EPIC: A Differential Privacy Framework to Defend Smart Homes Against Internet Traffic Analysis. *IEEE Internet of Things Journal*, 1–12. https://doi.org/10.1109/JIOT.2018.2799820

Liu, W., Nakauchi, K., & Shoji, Y. (2018). A neighbor-based probabilistic broadcast protocol for data dissemination in mobile IoT networks. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2808356

Liu, Y., Weng, X., Wan, J., Yue, X., Song, H., & Vasilakos, A. V. (2017). Exploring data validity in transportation systems for smart cities. *IEEE Communications Magazine*. 55(5), pp. 26–33. https://doi.org/10.1109/MCOM.2017.1600240

Lokuliyana, S., Jayakody, A., Dabarera, G. S. B., Ranaweera, R. K. R., Perera, P. G. D. M., & Panangala, P. A. D. V. R. (2018, August 8-11). Location Based Garbage Management System with IoT for Smart City. *The 13th International Conference on Computer Science & Education* (ICCSE 2018), pp. 699–703. http://doi.org/10.1109/ICCSE.2018.8468682

Luo, C., et al. (2019). Predictable Privacy-Preserving Mobile Crowd Sensing: A Tale of Two Roles. *IEEE/ACM Transactions on Networking*, 27(1), pp. 361-374, Feb. 2019. https://doi.org/10.1109/TNET.2019.2890860

Luo, X., Ren, Y., Hu, J., Wu, Q., & Lou, J. (2017). Privacy-preserving identity-based file sharing in smart city. *Personal and Ubiquitous Computing*, 21(5), pp. 923–936. https://doi.org/10.1007/s00779-017-1051-z

Maheswaran, M., & Misra, S. (2015). Towards a Social Governance Framework for Internet of Things. *2015 IEEE 2nd World Forum on Internet of Things* (WF-IoT). Dec 2015. https://doi.org/10.1109/WF-IoT.2015.7389156

Manjunatha, & Annappa B. (2018). Real Time Big Data Analytics in Smart City Applications. *International Conference on Communication, Computing and Internet of Things* (IC3IoT), pp. 279–284. https://doi.org/10.1109/IC3IoT.2018.8668106

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. *IEEE Access*. https://doi.org/10.1109/ACCESS.2017.2689040

Masduki, B. W., Ramli, K., & Salman, M. (2017). Leverage Intrusion Detection System Framework for Cyber Situational Awareness System. *2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems* (ICON-SONICS), Yogyakarta, 2017, pp. 64-69. https://doi.org/10.1109/ICON-SONICS.2017.8267823

Memmi, G., Kapusta, K., & Qiu, H. (2015). Data Protection: Combining Fragmentation, Encryption, and Dispersion. *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications* (SSIC). https://doi.org/10.1109/SSIC.2015.7245680

Mohammadi, M., & Al-Fuqaha, A. (2018). Enabling Cognitive Smart Cities Using Big Data and Machine Learning: Approaches and Challenges. *IEEE Communications Magazine*, 56(2), pp. 94–101. https://doi.org/10.1109/MCOM.2018.1700298

Mohammadi, M., Al-Fuqaha, A., Guizani, M., & Oh, J. S. (2018). Semisupervised Deep Reinforcement Learning in Support of IoT and Smart City Services. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2017.2712560

Moreno, M. V., Terroso-Saenz, F., Gonzalez-Vidal, A., Valdes-Vela, M., Skarmeta, A. F., Zamora, M. A., & Chang, V. (2017). Applicability of Big Data Techniques to Smart Cities Deployments. *IEEE Transactions on Industrial Informatics*, pp. 1–10. https://doi.org/10.1109/TII.2016.2605581

Moura, J., & Serrão, C. (2015). Security and Privacy Issues of Big Data. *Handbook of Research on Trends and Future Directions in Big Data and Web Intelligence*, pp 33. https://doi.org/10.4018/978-1-4666-8505-5.ch002

Nam, T., & Pardo, T. A. (2011). Smart city as urban innovation: Focusing on management, policy, and context. *ACM International Conference Proceeding Series*. 185-194. https://dl.acm.org/doi/10.1145/2072069.2072100

Nesi, P., Pantaleo, G., Paolucci, M., & Zaza, I. (2018). Auditing and assessment of data traffic flows in an IoT architecture. Proceedings – *4th IEEE International Conference on Collaboration and Internet Computing*, CIC 2018, pp. 388–391. https://doi.org/10.1109/CIC.2018.00058

Okai, E., Feng, X., & Sant, P. (2019). Smart Cities Survey. Proceedings – *20th International Conference on High Performance Computing and Communications, 16th International Conference on Smart City and 4th International Conference on Data Science and Systems,* HPCC/SmartCity/DSS 2018, pp. 1726–1730. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00282

Oteafy, S. M. A., & Hassanein, H. S. (2018). IoT in the Fog: A Roadmap for Data-Centric IoT Development. *IEEE Communications Magazine*, 56(3), pp. 157–163. https://doi.org/10.1109/MCOM.2018.1700299

Pacheco, J., & Hariri, S. (2016). IoT security framework for smart cyber infrastructures. Proceedings – *IEEE 1st International Workshops on Foundations and Applications of Self-Systems*, FAS-W 2016, 242–247. https://doi.org/10.1109/FAS-W.2016.58

Popescul, D., & Radu, L. D. (2016). Data Security in Smart Cities: Challenges and Solutions. *Informatica Economica*, 20(1/2016), pp. 29–38. https://doi.org/10.12948/issn14531305/20.1.2016.03

Pradhan, M., Fuchs, C., & Johnsen, F. T. (2018). A survey of applicability of military data model architectures for smart city data consumption and integration. *IEEE World Forum on Internet of Things*, WF-IoT 2018 – Proceedings, pp. 129–134. https://doi.org/10.1109/WF-IoT.2018.8355226

Pradhan, M., Suri, N., Fuchs, C., Bloebaum, T. H., & Marks, M. (2018). Toward an Architecture and Data Model to Enable Interoperability between Federated Mission Networks and IoT-Enabled Smart City Environments. *IEEE Communications Magazine*, pp. 163–169. https://doi.org/10.1109/MCOM.2018.1800305

Puron-Cid G., Gil-Garci J.R., & Zhang J. (2015). Smart Cities, Smart Governments and Smart Citizens: A Brief Introduction. *International Journal of E-Planning Research.* 4. iv-vii. https://www.researchgate.net/publication/295850218_Smart_Cities_Smart_Governments_and_Smart_Citizens_A_Brief_Introduction

Puschmann, D., Barnaghi, P., & Tafazolli, R. (2018). Using LDA to Uncover the Underlying Structures and Relations in Smart City Data Streams. *IEEE Systems Journal*. https://doi.org/10.1109/JSYST.2017.2723818

Rastogi, N., Singh, S. K., & Singh, P. K. (2018). Privacy and Security issues in Big Data: Through Indian Prospective. Proceedings – *2018 3rd International Conference on Internet of Things: Smart Innovation and Usages*, IoT-SIU 2018. https://doi.org/10.1109/IoT-SIU.2018.8519858

Riboni, D. (2019). Opportunistic pervasive computing: Adaptive context recognition and interfaces. *CCF Transactions on Pervasive Computing and Interaction*. https://doi.org/10.1007/s42486-018-00004-9

Rjab, A. Ben, & Mellouli, S. (2018). Smart cities in the era of artificial intelligence and internet of things. 2018 *Association for Computing Machinery*, pp. 1–10. https://doi.org/10.1145/3209281.3209380

Russell, L., Goubran, R., Kwamena, F., & Knoefel, F. (2018). Agile IoT for Critical Infrastructure Resilience: Cross-modal Sensing as Part of a Situational Awareness Approach. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2818113

Ryu, J. H., Sharma, P. K., Jo, J. H., & Park, J. H. (2019). A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *Springer Journal of Supercomputing*. https://doi.org/10.1007/s11227-019-02779-9

Sankaran, S., &Vishwa Vidyapeetham, A. (2017). Securing Networked Control Systems: Modeling Attacks and Defenses. *2017 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia) Securing*, pp. 7–11. https://doi.org/10.1109/ICCE-ASIA.2017.8309317

Sanseverino, E., Sanseverino, R., Vaccaro, V., Macaione, I., & Anello, E. (2017). Smart Cities: Case Studies. *Smart Cities Atlas*. Springer Link. November 2016, 82, pp. 47–140. https://doi.org/10.1007/978-3-319-47361-1_3

Santos, J., et al. (2017) City of things: Enabling resource provisioning in smart cities. *IEEE Communications Magazine*, pp. 1-8. https://biblio.ugent.be/publication/8572970/file/8572995.pdf

Sarker, M. N. I., Wu, M., & Hossin, M. A. (2018). Smart governance through bigdata: Digital transformation of public agencies. *2018 International Conference on Artificial Intelligence and Big Data*, ICAIBD 2018. https://doi.org/10.1109/ICAIBD.2018.8396168

Shah, T., & Patel, S.V. (2014). A Review of Requirement Engineering Issues and Challenges in Various Software Development Methods. *International Journal of Computer Applications.* 99(15), pp. 36–45. https://doi.org/10.5120/17451-8370

Shahat, A. M., Elragal, O. A., & Bergvall-Kåreborn, B. (2017). Big Data Analytics and Smart Cities: A Loose or Tight Couple? *International Conference on Connected Smart Cities 2017* (CSC 2017), Lisbon, 20-22 July 2017. https://www.researchgate.net/publication/317491579_Big_Data_Analytics_and_Smart_Cities_A_Loose_or_Tight_Couple

Siddiqui, Z., Tayan, O., & Khurram Khan, M. (2018). Security analysis of smartphone and cloud computing authentication frameworks and protocols. *IEEE Access*, pp. 1–16. https://doi.org/10.1109/ACCESS.2018.2845299

Sikora-Fernandez, D., & Stawasz, D. (2016). The Concept of Smart City in The Theory and Practice of Urban Development Management. *Romanian Journal of Regional Science*. 10(1), pp. 86–99. https://ideas.repec.org/a/rrs/journl/v10y2016i1p86-99.html

Simonofski, A., Asensio, E. S., De Smedt, J., & Snoeck, M. (2017). Citizen Participation in Smart Cities: Evaluation Framework Proposal. 2017 *IEEE 19th Conference on Business Informatics* (CBI), Thessaloniki, 2017, pp. 227-236. https://doi.org/10.1109/CBI.2017.21.

Sinaeepourfard, A., Krogstie, J., & Peterse, S. A. (2018). *A Big Data Management Architecture for Smart Cities based on Fog-to-Cloud Data Management Architecture*. Retrieved from CEUR-WS.org/Vol-2316/paper4.pdf

Sindhusha, P., & Bharathi, B. (2018). Privacy protection on data overflow system for smartphones. *6th International Conference on Computation of Power, Energy, Information and Communication*, ICCPEIC 2017, pp. 310–315. https://doi.org/10.1109/ICCPEIC.2017.8290383

Siris, V. A., Fotiou, N., Mertzianis, A., & Polyzos, G. C. (2019). Smart application aware IoT data collection. *Journal of Reliable Intelligent Environments*, 5(1), pp. 17–28. https://doi.org/10.1007/s40860-019-00077-y

Smolander, K., Rossi, M., & Pekkola, S. (2017). Infrastructures, Integration and Architecting during and after Digital Transformation. *Proceedings – 2017 IEEE/ACM Joint 5th International Workshop on Software Engineering for Systems-of-Systems and 11th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems*, JSOS 2017, 23–26. https://doi.org/10.1109/JSOS.2017.1

Soultatos, O., Spanoudakis, G., Fysarakis, K., Askoxylakis, I., Alexandris, G., Miaoudakis, A., & Nikolaos Petroulakis, E. (2018). Towards a Security, Privacy, Dependability, Interoperability Framework for the Internet of Things. *IEEE International Workshop on*

Computer Aided Modeling and Design of Communication Links and Networks, CAMAD. https://doi.org/10.1109/CAMAD.2018.8514937

Steuer, S., Benabbas, A., Kasrin, N., & Nicklas, D. (2016). Challenges and Design Goals for an Architecture of a Privacy-preserving Smart City Lab. *Datenbank-Spektrum*, 16(2), pp. 147–156. https://doi.org/10.1007/s13222-016-0223-8

Swarnkar, M., & Bhadoria, R. S. (2017). *Security Issues and Challenges in Big Data Analytics in Distributed Environment.* Springer International Publishing AG 2017, pp. 83–94. https://doi.org/10.1007/978-3-319-59834-5_5

Tanaka, S. A., de Barros, R. M., & de Souza Mendes, L. (2018). A Proposal to a Framework for Governance of ICT Aiming at Smart Cities with a Focus on Enterprise Architecture. 2018 *Association for Computing Machinery*. ACM, pp. 408–415. https://doi.org/10.1145/3229345.3229400

Tawalbeh, L. A., Tawalbeh, H., Song, H., & Jararweh, Y. (2017). Intrusion and attacks over mobile networks and cloud health systems. 2017 *IEEE Conference on Computer Communications Workshops,* INFOCOM WKSHPS 2017, 13–17. https://doi.org/10.1109/INFCOMW.2017.8116345

Tay, K., Supangkat, S. H., Cornelius, G. & Arman, A. A. (2018). The SMART Initiative and the Garuda Smart City Framework for the Development of Smart Cities. *2018 International Conference on ICT for Smart Society* (ICISS), Semarang, 2018, pp. 1-10. https://doi.org/10.1109/ICTSS.2018.8549961

Teoh, C. S., & Mahmood, A. K. (2017). National cyber security strategies for digital economy. *Journal of Theoretical and Applied Information Technology*. https://doi.org/10.1109/ICRIIS.2017.8002519

Terzi, D. S., Terzi, R., & Sagiroglu, S. (2016). A survey on security and privacy issues in big data. 2015 *10th International Conference for Internet Technology and Secured Transactions*, ICITST 2015, 202–207. https://doi.org/10.1109/ICITST.2015.7412089

Tragos, E., Fragkiadakis, A., Angelakis, V., & Pöhls, H. C. (2016). Designing Secure IoT Architectures for Smart City Applications. In *Designing, Developing, and Facilitating Smart Cities* (pp. 63–87). https://doi.org/10.1007/978-3-319-44924-1_5

Venticinque, S., & Amato, A. (2018). A methodology for deployment of IoT application in fog. *Journal of Ambient Intelligence and Humanized Computing*, 10, pp. 1–22. https://doi.org/10.1007/s12652-018-0785-4

Wagner, I., & Eckhoff, D. (2018). Technical Privacy Metrics: A Systematic Survey. *ACM Computing Surveys,* 51(3), 1–38. https://doi.org/10.1145/3168389

Wang, P., Ali, A., & Kelly, W. (2015). Data Security and Threat Modeling for Smart City Infrastructure. *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications* (SSIC). https://doi.org/10.1109/SSIC.2015.7245322

Wang, P., Yang, L. T., Xavier, S. F., & Li, J. (2018). An Edge Cloud-Assisted CPSS Framework for Smart Cities. *IEEE Cloud Computing*, pp. 37–46. https://doi.org/10.1109/MCC.2018.053711665

West, D. M. (2004). *E-Government and the Transformation of Service Delivery and Citizen Attitudes.* Wiley Online Library, 64(1), pp. 15–27. https://doi.org/10.1111/j.1540-6210.2004.00343.x

Xie, Y., Wang, W., Wang, F., & Chang, R. (2018). VTET: A Virtual Industrial Control System Testbed for Cyber Security Research. 2018 *3rd International Conference on Security of Smart Cities, Industrial Control System and Communications*, SSIC 2018 – Proceedings. https://doi.org/10.1109/SSIC.2018.8556732

Yadav, P., & Vishwakarma, S. (2018). Application of Internet of Things and Big Data towards a Smart City. *2018 3rd International Conference on Internet of Things: Smart Innovation and Usages* (IoT-SIU), pp. 1–5. https://doi.org/10.1109/IoT-SIU.2018.8519920

Yamakami, T. (2017). An organizational coordination model for IoT: A case study of requirement engineering of city-government in Tokyo in city platform as a service. *International Conference on Information and Communication Technology Convergence: ICT Convergence Technologies Leading the Fourth Industrial Revolution*, ICTC 2017. https://doi.org/10.1109/ICTC.2017.8190982

Yan, Z., Yu, X., & Ding, W. (2017). Context-aware verifiable cloud computing. *IEEE Access*, 5, 2211–2227. https://doi.org/10.1109/ACCESS.2017.2666839

Yigitcanlar, T., Kamruzzaman, M., Buys, L., Ioppolo, G., Marques, J., Moreira Da Costa, E., & Yun, J. (2018). Understanding 'smart cities': Intertwining development drivers with desired outcomes in a multidimensional framework. *Cities*. https://doi.org/10.1016/j.cities.2018.04.003

Ylmaz, E. N., Ciylan, B., Gönen, S., Sindiren, E., & Karacayilmaz, G. (2018). Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect. Proceedings – *2018 6th International Istanbul Smart Grids and Cities Congress and Fair*, ICSG 2018, pp. 81–85. https://doi.org/10.1109/SGCF.2018.8408947

Zhang, G., Wang, J., Huang, W., Su, H., Lv, Z., Yao, Q., & Ye, S. (2015). Big Data Collection and Analysis Framework Research for Public Digital Culture Sharing Service. Proceedings - 2015 *IEEE International Conference on Multimedia Big Data*, BigMM 2015, 196–199. https://doi.org/10.1109/BigMM.2015.37

Zhang, K., & Zahng, Q. (2018). Preserve Location Privacy for Cyber-Physical Systems with Addresses Hashing at Data Link Layer. 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, United Kingdom, 2018, pp. 1028-1032. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00170

doi: https://doi.org/10.3127/ajis.v24i0.2531