Smart City Applications

Subjects: Others

Contributor: Jameela Al-Jaroodi

Smart city applications are designed to take advantage of the smart city ICT and collected data to provide value-added smart features. These applications use data analytics, intelligent techniques and other advanced technologies to make smart decisions that improve the smart city's operations and quality of life.

Keywords: smart cities ; ethics ; data privacy ; Internet of Things ; smart city applications

1. Introduction

The smart city, as it is known today, has had a handful of names throughout the history of its establishment. Before the shift to smart city, it was known as the digital city. This latest change reflects the ways information and communication technologies (ICT) are implemented for smart cities. They have become more than isolated service systems. In fact, they are evolving into a diverse ecosystem, which includes sensors, software, robots, networks, real time surveillance, and even humans. For example, Amsterdam is using ICT to slowly push citizens' behavior towards a more "sustainable lifestyle". They also plan to introduce smart ports to streamline shipping traffic. London is looking to develop new markets for its waste and its utilization as a resource. They also aim to use 3D visualization to bring safety and efficiency to agencies in construction and other public works. The main goal is to improve the living standards for smart cities residents [1]; however, there is a price to pay when it comes to ethics.

The extensive use of ICT and connected technologies like the Internet of Things (IoT) [2], Cloud and fog computing [3], and Cyber Physical Systems (CPS) [4] to name a few has led to data being generated and gathered at lightning speeds. This data comes from various sources and may carry increasingly sensitive and private information about smart city residents. To a certain extent, data gathering has become an integral part of our lives to a point where some see it as invasive. Assuming an ideal world where everything is done correctly, gathering and using this data poses no threat to anyone and the benefits far outweigh the risks. Unfortunately, in the real world, there are always issues and problems to be addressed when dealing with such data. Some may be intentional, while others are accidental. Issues with data privacy and ethical use of gathered information are always present. Yet, not many have attempted to address them or provide solutions to minimize the risks. Researchers and developers are always concerned with the technologies, approaches, architectures, and methods they introduce and their correctness and benefits. Business people are more interested in what will make them more profits, while policy makers want to make their lives easier and use the technologies to support their decision-making processes. All together they are aiming to better serve the residents who are mainly concerned about high quality of life and financial stability. The main players concerned about ethics and ethical use of the data are the residents. Yet, they are the ones who at the current state have the least control over who collects the data, how it is used, and what it is used for.

2. Review of Smart City Applications

As the concept of smart cities evolved, many applications emerged in support of this concept and various cities around the world put in motion plans to become "smart cities". The approaches taken and technologies used differ everywhere and the applications vary and expand across all aspects of city life. Research and development efforts are continuous and new models and solutions emerge every day. Yet, the wealth of outcomes from these efforts have not been strongly linked to the ethical implications associated with them.

In an effort to initiate this type of conversation as smart cities continue to evolve and grow, we try to provide a link between different applications for smart cities and the impact they make in terms of ethics and ethical conduct. The following are some examples of smart city applications and approaches and a brief view of how ethics come in the picture. The list is by no means comprehensive; however, the selected projects in the literature can be considered a representative sample of different areas where smart applications can contribute towards building a smart city. Some of the examples are actual projects that have been developed and used, while others are in their design or research phase.

However, collectively these projects offer a general view of what technology offers and as a result allow us to identify where and how ethical issues may arise.

2.1. Water Monitoring System, Korea

Vender cooperation proves to be a major key to the success of a smart city. The water monitoring system introduced in a Korean city showcases how the lack of cooperation in the private sector can hinder any meaningful progress. A water supply system in a South Korean "U-City" is designed to provide real time information on the health and operational characteristics of the main water supply infrastructure for the city. It includes many sensors and software systems from a number of different private companies that collect this information and feed it to a central location for monitoring and evaluation. Currently, when a sensor fails they must contact the company that owns and operates it and have them fix it, but to fix it they must shut down or interact with other systems that are maintained by other vendors leading to excessive time delays [5]. This example shows that all vendors, public and private, must create a clearly defined process to diagnose and repair any issues that may occur, otherwise projects incur time delays and wasted resources. Such needs are not always governed by laws and regulations that can be enforced. They are more about collaboration and agreement across vendors and if some vendors choose to favor certain outcomes, ethical issues could easily arise. There are always issues with getting the private sector more involved for two reasons: legislation that has impeded this progress and the lack of profit incentives. In addition, they present a list of general issues in the development of the Korean U-Cities that is largely technology-influenced, yet design, privacy and digital inequality are not fully addressed. The overhyped premise is leading to a lack of credibility and no way to monitor and evaluate the smart city projects.

2.2. 100 Smart Cities, India

Since coming into power in 2014, the National Democratic Alliance started an initiative to have 100 smart cities across India with the goals to bring quality of life, high tech infrastructure, improved mass transit, pollution free areas, energy efficiency, and transparent governance. These cities are divided into nine satellite cities with a population of four million or more, 44 cities with a population of one to four million, 17 state and union territory capitals, 10 of tourist and religious importance, and 20 with a population of half a million to a million [6]. Resources have been redirected to accomplish this goal, leading to shortages of resources in other areas. As a result, the Indian community is currently facing a more obvious separation of classes than previously defined. The introduction of smart cities throughout the country is seemingly advancing the upper-class cities while overlooking the poorer cities. The country's previous mission of 1980, before the smart city initiative, was to make every Indian city achieve sustainable living conditions. Decades later, this mission has still not been accomplished. The means to advance substandard cities are now being abandoned and the cities themselves are becoming overlooked, while the efforts are being focused on enhancing the exclusive and already sustainable, upper-class cities to reap the societal advantages and living conditions of smart cities. This unbalanced advancement concerning the middle and upper classes is a direct ethical concern revolving around smart city implementation.

2.3. Performance Measurement System, Europe

Smart city initiatives in Europe have increased over time leading to different, usually independent, efforts from each city. As a result, it has become obvious that some form of measurement standards are needed to identify successful smart city projects. The CITYKeys research project aims to create a performance system to measure how Smart Cities are performing all across Europe and how new smart cities can use the system. It outlines six steps to formulate the system: specifying the needs of the city; compiling existing indicators; building new indicators to fill existing gaps, defining the framework; studying available data for calculations; and developing a prototype system for data collection and visualization. The researchers in the project determined that an average of 72% of the data needed was available from public and private sources for the calculations used to create the system [7]. The data is defined as any relevant information collected from smart technologies that would help enable all stakeholders to learn from each other and monitor their progress. During the course of the project they determined that the main issue with their collection of the data was that there was a clear lack of centralization and management. They also suggested that there should be better standard practices for sharing and publishing data emphasizing that it is important to have output indicators that measure the implementation of smart technologies and "impact indicators that measure progress towards overall targets". Using emissions reduction as an example, smart cities could monitor traffic flow then adjust the appropriate systems to minimize congestion and prevent unnecessary idling in confined areas. The major concern in this scenario is how data is shared or published. If this data include personal and private information about city residents, there are various concerns regarding ensuring ethical access and use of this data. Moreover, for a measurement system like this one to operate successfully, strong collaboration efforts and willingness to adapt and share data are needed across all organizations, which again raise the question, “how to trust each other?”

2.4. Crime Prediction

Crime prediction software is geared to use collected data within a smart city to identify potential risks in terms of criminal activities. A software is created to monitor and collect information on communications and interactions across certain locations, or among certain groups of people may offer some insight into possible unlawful activities. This software works by aggregating and anonymizing mobile phone metadata along with demographic and geographic data [8]. This data is then used to predict where the heaviest concentration of criminal activity will occur and law enforcement may then focus on the hotspots predicted by the software. Other than securing and protecting this data, we also run into other important issues. For one, this software will inherently work best in areas where more mobile phones are available, which are usually better areas economically, thus leading to better protection for these areas over other, possibly poorer areas. Another issue that may arise is that over time, the results obtained will get skewed by the higher arrest and preventions rates in the highly monitored areas. This may also raise ethical issues when considering possible discrimination based on some prominent factors in certain areas. Furthermore, issues may arise when accessing and sharing this data with other organizations.

2.5. Smart Grid

Much like the smart city itself the smart grid has an exciting array of beneficial effects on the quality of life of people using it. However, the smart grid also opens up ethical concerns on various levels. Smart grids would allow companies and consumers to better monitor and control energy use [9]. This means that a consumer’s privacy has the potential to be violated, specifically when the data collected can reveal the types of electrical devices a consumer uses as well as how often an individual device is used. In addition, this type of fine-grain data collection and analysis could also reveal other types of private information about the consumers, such as time they spend away from home, travel periods, and other habits. Considering that the smart grid is well protected, this may not be a huge issue; however, any security breaches and leaks of such data could lead to disastrous effects. Moreover, the smart grid owners may also be tempted to use this data for other benefits, like targeted advertisements or specialized marketing, which could in many cases violate consumers’ privacy. Smart grid integration into the IoT and other smart applications in a smart city also opens up the possibility of cyber-attacks that could deny individuals or whole cities power. Once again, the issue of social class arises in the fact that power can be throttled during peak usage times, and that consumers that are better off economically will possibly have the option to opt out of this peak usage throttling. In a worst-case scenario, a poorer family might lose heat during a cold day due to electrical usage being at a peak.

2.6. Occupancy Detection

Occupancy detection focuses on whether or not a space is occupied, instead of the number of occupants within a space. This binary form of occupancy monitoring tends to focus solely on private spaces, such as office buildings [10]. This form of occupancy monitoring could possess the ability to control systems within the building or the office space. Some example systems could include: lighting, heating air conditioning and ventilation (HVAC) systems, and electricity use as a whole. With the potential ability to autonomously control these systems based on occupancy detection, not only would bills be significantly reduced at a larger scale, but less pollutants would be released into the air. On one hand, there are advantages that could be used by the building owner to operate their business efficiently while also providing emergency personnel information regarding the building being occupied or not in case of an emergency. On the other, it could produce potential safety and ethical concerns if the information was intercepted or used to ensure a higher success rate of criminal activity. An example of this would be using this software to rob an office of confidential information or a business of their property. Another possible issue to consider is using his type of monitoring to greedily reduce buildings operational costs even when certain occupants are still in certain areas of the buildings. For example, setting the system to turn off HVAC systems in the offices even when the cleaning staff are there outside regular working hours.

2.7. Occupancy Counting

Unlike occupancy detection, occupancy counting focuses on the actual number of people in a building or a structure. Occupancy counting seems like a very helpful approach to solving occupancy issues that could lead to violations of fire safety laws within buildings, for example. There is one problem, however; that is counting all of the people in the building. The current solutions involve the use of mobile devices and cameras [10]. The main concern is that not all individuals carry mobile devices, which may default into the use of cameras being the primary source of occupancy detection. Although most buildings are already equipped with camera-monitoring systems, these systems would function differently. Some of these systems would track the number of people within the structure by extracting features of the individuals which could describe body parts and shapes of an individual [10]. This basically means that individuals are identified and labeled with personal information and locations at any point of time. This form of monitoring could ethically infringe upon rights concerning confidentiality or anonymity if this information is used to label a person by their name. If this form of occupancy counting is accepted, it is important to focus solely on the component originally being monitored, which is the number of people in the building or structure, instead of who is in the building. Accurate measures need to be in place to control the collection and labeling of the data to ensure the privacy of the occupants of the buildings. The ethical emphasis in this case is higher on making sure the personalized data is not misused or directed to purposes other than the original intent. In addition, sharing this information with other organizations should be highly regulated and adequate mechanisms for authorizations and permissions are needed to ensure the individuals' rights to privacy.

2.8. Occupancy Tracking

Occupancy tracking is the combination of the two aforementioned occupancy monitoring systems. This system not only monitors both the binary and numerical occupancy in a building, but also locates and tracks people within these buildings [10]. Binary occupancy is used to determine whether or not a building is occupied whereas numerical occupancy is used to determine the actual number of occupants within a specific location. The same ethical concerns that affect occupancy detection and occupancy counting also affect occupancy tracking; however, this form of occupancy monitoring contains even more ethical constraints as it offers more high-grain details about the individuals in these buildings. Individuals' whereabouts would always be known to the system. Instead of being identified solely as an individual at a location, an individual's identity will be determined and tied to their specific location. Such monitoring may be acceptable in public facilities to ensure safety and security. However, it could become a big concern when used in more private locations such as workplaces or residences. This type of access could easily lead to infringements on the basic individual's right to privacy.

2.9. Event Recognition

Occupancy event recognition focuses on the behavior and activities of the people detected within the monitored location [10]. This form of occupancy monitoring tracks these behaviors and activities to produce more intelligent HVAC system controllers, for example, as well as determining potential behaviors associated with criminal activities, as another example. Event recognition could be used in buildings that may have large crowds such as: sporting arenas, banquet rooms, theatres, and schools. Aside from obvious privacy issues resulting from this form of occupancy monitoring, these technologies could actually repress basic human nature and interactions due to the simple knowledge of being watched. This repression could infringe upon the principle of respect for the individual. It is an elementary concept that when being watched, your behavior is likely to change to avoid being labeled as suspicious, or so as not to mistakenly do something that may trigger an alert within the system. This form of monitoring could also embarrass an individual or group of people if their actions were misinterpreted. These issues relate to the common awkwardness of leaving a store without buying anything. Although you may not be stealing something, you still feel like everybody is watching you. Your behavior changes, putting on a false persona of who you really are just to remain unsuspected and unnoticed. Such systems may not identify individuals personally, but they accumulate enough data that could easily be used to do so later. Unfortunately, this type of data can be easily misused for seemingly harmless activities, like targeted advertising, or to cause intentional harm, like creating dangerous situations for some individuals or falsely incriminating someone.

2.10. GPS Tracking

Geographical Positioning Systems (GPS) tracking is becoming more common in various areas in smart cities and it offers location-monitoring capabilities outdoors. In this case the concern is who and how the location data provided by GPS devices is used. Several smart city applications rely on location information to operate effectively [11]. For example, providing smart traffic light controls based on GPS information collected about the vehicles in a given area. Another example is identifying the location of distressed residents and providing emergency support when needed. Location data can be used to find out numerous things about the person or persons being tracked and most of the information that could be revealed by such tracking is legally protected in the United States. GPS tracking in particular is of ethical concern, because it takes up little in the way of resources when compared to other methods of location tracking. In addition, it provides fine-grain and personalized tracking data [11]. This data, in addition to its immediate use, can also be stored and combed through later allowing breaches of privacy to occur long after the data was initially collected. The Supreme Court has already had rulings that forbid the use of GPS tracking by law enforcement unless they have reasonable cause to do so. However, the definition of reasonable cause is ambiguous enough to lead to various infringements on this ruling.

2.11. Autonomous Transportation

An important component of a smart city is its complement of autonomous vehicles. Autonomous transportation provides a cheap and safe alternative to get around the smart cities of the future. The current research in this area is progressing quickly and the industry is already working its way toward achieving fully autonomous vehicles. Some companies that are currently experimenting with autonomous vehicles are: Google, Uber, and most vehicles manufacturers in the automotive industry. The associated press points out that 94% of accidents are caused by human error [12]. This makes self-driving cars a desirable alternative for public transportation. However, some incidents with this technology are posing questions as to how safe it really is. For example, a woman crossing the street in Tempe, Arizona was struck by a self-driving Uber car [13]. The CEO of Uber, in the past, has pointed out that the self-driving cars feature an algorithm that learns as it drives [14]. This means that as they are implemented, the self-driving cars are the most dangerous they will ever be until the algorithm manages to learn. This incident also brings up an interesting question about who is liable in an accident involving a self-driving car. Is the company who owns the car culpable? Is it the back-up driver in the vehicle, or is it the programmer who built the self-driving software? These questions are currently unanswered. Another issue to consider is the minimum harm directive, where the self-driving vehicle should make a decision to cause the smallest possible damage if none can be avoided. This is also a learned behavior that the intelligent software uses, however, as the software learns, it can also easily pick up biased responses that may negatively affect its future decisions.

2.12. Intravehicular Communication

Intravehicular communication focuses on data that is being shared between motor vehicles in a given area, such as multiple vehicles around a specific intersection or near a specific highway exit. This technology mainly works to minimize traffic incidents and improve traffic efficiency [15]. For this type of application to contribute positively, the exchanged data is required to be accurate, relevant, and meaningful during the communication. One major issue is who is able to monitor or receive this exchange of information as well as what information the vehicles are able to communicate to one another. Current vehicular communication applications, such as Waze and Google maps, already present users with data integrity issues. A potential attacker could drive a route to collect data packets. They can then replay the data packets and change the time stamps to falsify data to the server. This simple attack can be intensified by performing many transmissions with different cookies and platform keys that represent multiple yet unique vehicles [16]. By using this information, an attacker could potentially force other drivers into traffic jams and keep certain roads cleared. In addition, when multiple vehicles are exchanging information, issues of trust arise since these connections are ad hoc and have no way to authenticate each vehicle. With that in mind, it becomes important to consider what ethical or legal problems may occur and how they will be addressed.

2.13. Drone Applications

Drones can provide many applications for smart cities and make a positive impact on society [17]. For example, drones can be used for environmental monitoring, traffic management, pollution monitoring, civil security control, crowd monitoring, infrastructure inspections, tourism support, health emergency services, and merchandise delivery [18]. Drone applications, among several others, can deliver cost-effective services to help achieve the objectives of smart cities [19]. Employing drones for these applications can improve operations and reduce the costs of offering these services. It can also improve safety and security and help save human lives. Drone applications such as security and crowd monitoring, health emergency services, and large-scale disaster management can notably contribute in creating smart cities safer for residents and visitors. Furthermore, some drone applications can stimulate business and offer a good image for a city thus serving to attract new businesses like merchandise delivery, tourism support, and air taxis [17]. Although using drones can provide many benefits to smart cities, there are many safety, security, privacy, and ethical issues involved on these applications [20][21][22]. Drones in smart cities may be used for diverse applications and under the control of multiple public or private organizations. Consequently, there are potentials that these drones are misused for purposes other than their originally planned functions. Examples include utilizing the drones to spy on residents or organizations, or using data collected by the drones to influence certain persons or organizations when making decisions. This can represent a difficulty for utilizing drone applications in smart cities [20].

References

1. Dirks, S.; Gurdgiev, C.; Keeling, M. Smarter Cities for Smarter Growth: How Cities Can. Optimize Their Systems for the Talent-Based Economy; IBM Inst. Business Value: Somers, NY, USA, 2010.

2. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.
3. Mohamed, N.; Al-Jaroodi, J.; Jawhar, I.; Lazarova-Molnar, S.; Mahmoud, S. SmartCityWare: A Service-Oriented Middleware for Cloud and Fog Enabled Smart City Services. IEEE Access 2017, 5, 17576–17588.
4. Al-Jaroodi, J.; Mohamed, N.; Jawhar, I.; Lazarova-Molnar, S. Software engineering issues for cyber-physical systems. In Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP), St. Louis, MO, USA, 18–20 May 2016; pp. 1–6.
5. Kim, J.S. Making smart cities work in the face of conflicts: Lessons from practitioners of South Korea’s U-City projects. Town Plan. Rev. 2015, 86, 561–585.
6. Souvanic, R. The Smart City Paradigm in India: Issues and Challenges of Sustainability and Inclusiveness. Soc. Sci. 2016, 5, 29–48.
7. Huovila, A.; Airaksinen, M.; Pinto-Seppà, I.; Piira, K.; Bosch, P.R.; Penttinen, T.; Neumann, H.M.; Kontinakis, N. CITYkeys Smart City Performance Measurement System. Int. J. Hous. Sci. Its Appl. 2017, 41, 113–125.
8. Bogomolov, A.; Lepri, B.; Staiano, J.; Oliver, N.; Pianesi, F.; Pentland, A. Once upon a crime: Towards crime prediction from demographics and mobile data. In Proceedings of the 16th International Conference on Multimodal Interaction, Istanbul, Turkey, 12–16 November 2014; pp. 427–434.
9. Kostyk, T.; Herkert, J. Computing Ethics: Societal Implications of the Emerging Smart Grid. Commun. ACM 2012, 55, 34–36.
10. Akkaya, K.; Guvenc, I.; Aygun, R.; Pala, N.; Kadri, A. IoT-based occupancy monitoring techniques for energy-efficient smart buildings. In Proceedings of the IEEE Wireless Communications and Networking Conference Workshops (WCNCW), New Orleans, LA, USA, 9–12 March 2015; pp. 58–63.
11. Elmaghraby, A.S.; Losavio, M.M. Cyber security challenges in Smart Cities: Safety, security and privacy. J. Adv. Res. 2014, 5, 491–497.
12. Krisher, T. Can Self-Driving Cars Withstand First Fatality? U.S. News & World Report. 20 March 2018. Available online: https://www.usnews.com/news/business/articles/2018-03-20/arizona-death-brings-calls-for-more-autonomous-vehicle-rules (accessed on 9 September 2018).
13. Kissler, M.; Levin, A.; Beene, R. Uber Victim Stepped Suddenly in Front of Self-Driving Car. Available online: www.bloomberg.com/news/articles/2018-03-20/video-shows-woman-stepped-suddenly-in-front-of-self-driving-uber (accessed on 9 September 2018).
14. Newcomer, E. Uber CEO’s Commitment to Self-Driving Cars Tested by Fatality. Bloomberg.com. 20 March 2018. Available online: https://www.bloomberg.com/news/articles/2018-03-20/uber-ceo-s-commitment-to-self-driving-cars-is-tested-by-fatality (accessed on 9 September 2018).
15. Cheng, X.; Yao, Q.; Wen, M.; Wang, C.X.; Song, L.Y.; Jiao, B.L. Wideband Channel Modeling and Intercarrier Interference Cancellation for Vehicle-to-Vehicle Communication Systems. IEEE J. Sel. Areas Commun. 2013, 31, 434–448.
16. Jeske, T. Floating Car Data from Smartphones: What Google and Waze Know about You and How Hackers Can Control Traffic. Black Hat. March 2013. Available online: https://media.blackhat.com/eu-13/briefings/Jeske/bh-eu-13-floating-car-data-jeske-slides.pdf (accessed on 9 September 2018).
17. Mohamed, N.; Al-Jaroodi, J.; Jawhar, I.; Idries, A.; Mohammed, F. Unmanned Aerial Vehicles Applications in Future Smart Cities. echnol. Forecast. Soc. Chang. 2018, in press.
18. Mohammed, F.; Idries, A.; Mohamed, N.; Al-Jaroodi, J.; Jawhar, I. UAVs for smart cities: Opportunities and challenges. In Proceedings of the International Conference on Unmanned Aircraft Systems (ICUAS), Orlando, FL, USA, 27–30 May 2014; pp. 267–273.
19. Mohammed, F.; Idries, A.; Mohamed, N.; Al-Jaroodi, J.; Jawhar, I. Opportunities and challenges of using UAVs for dubai smart city. In Proceedings of the 6th International Conference on New Technologies, Mobility and Security (NTMS), Dubai, UAE, 30 March–2 April 2014; pp. 1–4.
20. Finn, R.L.; Wright, D. Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. Comput. Law Secur. Rev. 2012, 28, 184–194.
21. Rodday, N.M.; Schmidt, R.D.O.; Pras, A. Exploring security vulnerabilities of unmanned aerial vehicles. In Proceedings of the 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS), Istanbul, Turkey, 25–29 April 2016; pp. 993–994.

22. Vattapparamban, E.; Güvenç, I.; Yurekli, A.I.; Akkaya, K.; Uluağaç, S. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In Proceedings of the 2016 International Conference of Wireless Communications and Mobile computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016.