# Smart Cities, IoT and Security

Davy Nolan
*Trinity College Dublin*
*Student Number: 17330208*

***Abstract*—This paper is about the development of Smart Cities around the world, the IoT involved and the security and privacy issues attached to data harvesting. This paper is to be submitted as the final assignment for the Advanced Telecommunications CSU34031 module.**

## I. Introduction

A smart city is an urban area that utilises a variety of electronic IoT (Internet of things) sensors and actuators to collect data and then use insights gained from that data to manage assets and resources and also to improve services by automation and reducing operational costs. To ensure adequate cohesion in a city, all key actors must co-operate to use resources in an optimised way. The intelligence of a city is shown by its ability to gather its resources and to achieve its emphasised objectives through the rate of satisfaction of the needs of its inhabitants while also involving its inhabitants in the approach [4]. Throughout this paper, the security, performance and privacy of Smart Cities will be explored along with use cases in the world today. These use cases will be analysed to see if they are reaping the benefits of data-directed development or suffering from the exploitation of personal data. New technologies will then be analysed to see how the future trends of Smart Cities will be impacted.

## II. Security and Performance of Smart Cities

Since Smart Cities rely mostly on IoT sensors and actuators to gather the data they need, this usually leads to Cybersecurity issues which also leads to the collapse of critical services. As there are so many different cyber-physical systems interacting with one another in a Smart City, failures are expected to occur. This gives rise to the possibility of someone intentionally exploiting the security breaches. To try deter and avoid these hacking activities, cities must implement strict controls to monitor citizen's activities which prompts a decision of prioritising the privacy of the security for the Smart City [6]. Figure 1 illustrates the IoT context of a Smart City including its elements and the relationships between them. This model consists of four elements: the person, the technological ecosystem, the process and the intelligent object in the middle tying them all together.

### A. Elements

The **person** is the user of the system, which has different levels of access to the Smart City framework depending on their role. This element plays a vital role in the IoT framework, since it's the operators who are in charge of the security management. They define the practices and rules of security as well as testing how the practices and rules function [7]. The person element is in charge of how the IoT environment functions and ensure no breaches in the cybersecurity occur.

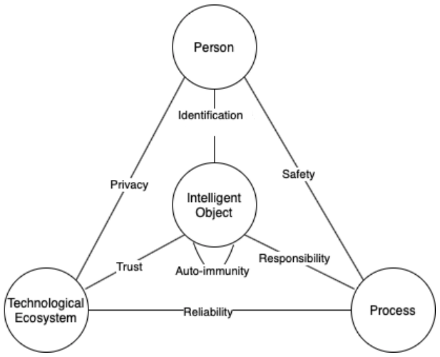

Fig. 1. Diagram of Cybersecurity in a Smart City [8]

The **process** element refers to the actions taken by the person in implementing security policies to ensure a safe IoT infrastructure [8]. The process of creating the security policies is easier said than done due to the various constraints attached to this element.

The **technological ecosystem** covers all of the technical decisions that were made to provide security. Some of these decisions can consist of the choice of system architecture and communications protocols including the algorithms that were implemented [8].

In the very centre of the system is the **intelligent object**. This element represents the smart devices involved in the network of IoT devices which provide data for the Smart City. This object communicates with other objects in the surrounding in environment, constantly sending and receiving information.

### B. Relationships

Each of the elements are connected together by relationships. The person and process elements are held together by the **safety** tension which represents that safety must be ensured in the case of a system failure occurring in one of the components. It is basically an insurance policy to reduce the possibility of damage [7]. The **identification and authorisation** relationship joins the person with the intelligent object. This symbolises the need for there to be some kind of verification of identity when it comes to a person accessing the intelligent object in this system. It must be taken into account that different intelligent objects carry different functions and different people carry different roles so identity verification is key. The person element is also connected to the technological system by the **privacy** tension which represents the need to protect sensitive data of the person from disclosure in the IoT environment [8].

The **responsibility** tension ties the process to the intelligent object, which outlines the responsibilities of each intelligent object that must considered to prevent dangers whenever the intelligent object carries out a process. Both of these elements are responsible for each other as they both must share resources and access rights for different processes [7]. The process and technological ecosystem are attached by the **reliability** relationship. This stands for the likelihood of the system elements failing.

The technological system is connected to the intelligent object by the **trust** tension and can be described as the probability by which an individual expects that another individual performs a given action on which its welfare depends [8]. Basically, it symbolises the level of confidence that the technological system can grant to the intelligent object.

The **auto-immunity** tension ties the intelligent object into a self-loop as the IoT requires its own immune system in the case of physical attacks when there is limited physical defence.

## III. Privacy Concerns of Smart Cities

One of the most concerning aspects of implementing a Smart City is the use of private and personal data. When a Smart City is being constructed, it is inevitable that the IoT will be processing a wide variety of data. This includes data such as traffic, location and environmental data etc. Under the Data Protection Act, much of this data is prohibited to be used and shared without the consent of the owner. In order for the IoT to provide the enhanced services which a Smart City has to offer, it must be accepted that citizens' data will be used. Despite the fact that these individuals will be the ones benefitting from these services, this will have a big impact on their privacy.

As the Big Data that is being stored in Smart Cities continues to grow, the idea of profiling must be considered. This is where user profiles are made for the users/consumers of multiple public and private with the goal of collecting as much information as possible. Data-mining strategies are utilised to analyse common behaviour patterns in order to offer advanced solutions and resource optimisation as per factual derivations [10]. For example if we take the transport sector into account, each user (commuter) would each have their own transport card with NFC (near field communication) capabilities which would carry their profile information. Each time that commuter uses some form of public transport in the city, this data will be harvested and used to recognise habits and common behaviour patterns of that user. It must be understood that profiling can only be carried out with the user's personal consent.

Citizens have a right to be concerned about the use of their personal data. It is the fear of the unknown which worries the public; "the scariest thing is that we don't know what the scariest thing is" [12]. There is a risk involved in the collection of this data with the possibility of hackers accessing this information intentionally or unintentionally where sensitive information may be vulnerable. There is also a risk of companies harvesting this data and selling people's personal information for marketing purposes showing that data truly has monetary value [12].

The concept of a user persona (user experience) was introduced by Alan Cooper, a noted pioneer software developer, in 1983. This idea can be described as a fictional character that is created to represent a user type that may use a site, brand or product in a similar way. Since this concept does not involve an identified or identifiable person but models of users who are related through common behaviour patterns, common characteristics and needs, there is no reference made to the actual person behind the profile which in turn protects each user's personal information and privacy. Since this method is not interested in the processing of personal data from an identifiable person, solutions can be implemented in the interest of the community rather than having to seek consent from each user of the system before gathering data. This allows for citizens to keep their information private whilst also harnessing the benefits of the enhanced services [10].

## IV. Real World Applications

There are many examples of Smart Cities being implemented in present time such as in Singapore, Tokyo and Barcelona and many more being planned for the near future; one of the noted developments being the Sidewalk Toronto Quayside development planned for 2024 [9].

### *A. Toronto Quayside Development*

The Quayside urban innovation plan is the plan for Toronto to implement a Smart City "with a new approach to development that integrates new innovations into the physical environment, with the ultimate goal of improving people's lives". The developers of at Sidewalk Labs believe that digital innovation is necessary for producing an environment of new services and solutions to urban challenges by citizens, companies and local entrepreneurs. They also recognise that this digital innovation inevitably introduces a number of issues such as ensuring there in a transparent process in place for protecting the personal privacy of the public [9].

Sidewalk Labs has put forward a number of propositions to tackle these challenges introduced. Firstly, they suggest the establishment of an "open digital infrastructure that provides a shared foundation for using urban data to improve quality of life" [9]. Within the proposed "IDEA district" this infrastructure will be held in place by affordable internet connectivity. Secondly, they want to tackle the data privacy concern by introducing clear standards that make the data publicly "accessible, secure and resilient". They believe that since most of present day's data is dispersed among many different owners and stored in inaccessible and unsorted manners, that new clear standards would make it much easier for researchers and the community to access the data. It would also improve third parties' construction of adequate services which the city can avail of.

Lastly, Sidewalk Labs wishes to implement a reliable process which goes by previously established privacy laws and regulations that would apply to all companies ant third parties developing in the district. They plan to implement this process alongside a RDU (responsible data use) assessment which is a meticulous review which is carried out whenever a request to use urban data is made. This process is incorporated with a set of RDU guidelines created with globally recognised privacy by design principles [9]. There will be a steward of urban data put in place which is a government oriented urban data trust that overlooks the process and grants approval. This will ensure that some data which does not pose any privacy risks can be made accessible to the public by default. This will allow companies, community members and other third parties to use this data to develop new services.

The Quayside Smart City development project is a key example of how important it is to citizens for their data privacy to be protected whilst also reaping the benefits of newly enhanced services.

### *B. Kashgar, China*

Another real world example of a Smart City is the city of Kashgar in China, however the negative effects of data harvesting can be seen here. This developed city in China has surveillance cameras with image recognition capabilities installed on nearly every street. At the click of a mouse, the police can access any live video from any surveillance camera or even take a closer look at anyone passing through one of the thousands of checkpoints in the city. In the article [2], the interviewer was shown by the technician that the system could gather private information on a woman just from footage of her face. The woman had been stopped at a checkpoint on a motorway and using this footage the system cycled through a huge collection of data and then displayed the details of her education, her family and even showed her recent visits to a hotel and a café. This suggests that the citizens of Kashgar's private information is not being protected all in the hopes of reducing crime, protests and violence. Although citizens can reap the benefits of a seemingly safer environment, they must fear the unknown with their private data being potentially breached.

## V. Future Trends

With the constant development of new technologies as the decades go on, cities will only become more intelligent and work more seamlessly.

### *A. 5G Internet and Wi-Fi 6*

This year has brought us into a new decade and also introduced us to the concept of 5G internet. Smart Cities will be able to avail of the benefits of 5G, being able to offer smarter vehicles, processing, manufacturing and other IoT services which rely on this technology [5].

Since the next wave of innovation will be even more data intensive, to meet that demand, Wi-Fi 6 and 5G both prove to be enormously advantageous when it comes to bandwidth, speed and latency [3]. 5G introduces a massively improved platform to deliver scalable and reliable connectivity to the world. This technology is engineered to be high data-rate and low-latency. These two aspects ensure the fast transfer of data between multiple points which will allow for many new applications to be deployed that were not possible before. Both of these technologies have their own unique strengths in smart urban environments as they are both designed to work together.

The massive amounts of data generated by the sensors and actuators placed around a Smart City must be communicated, analysed a sent to the infrastructure to affect changes in the city, creating a huge demand on internet access [1]. Therefore, IoT will be able to carry out its role more seamlessly with 5G and Wi-Fi 6 connectivity and parties will be able to reconfigure their infrastructures to work even more efficiently. 5G also offers massive machine type communication (MMTC) and critical machine type communication (CMTC). MMTC is designed to work with a large amount of IoT devices, which allows for a lot of sensors and actuators to send a receive information simultaneously. Use cases of this technology include smart building and air quality monitoring. It is designed to be latency-tolerant as well as being efficient for sending and receiving small blocks of data on low bandwidth pipes [1]. Citizens will also benefit from this with greatly enhanced interactions with one another, with services and with the ecosystem around them.

### *B. Blockchain Technology*

Another future trend that can be noticed is the utilisation of blockchain as a means of protecting data privacy in Smart Cities. Blockchain can be explained as a distributed ledger network which makes use of key cryptography to sign transactions that are stored on a distributed ledger, where the ledger contains encrypted linked blocks of transactions [11]. These encrypted linked blocks of transactions are what are known as a blockchain.

The use of blockchain allows for the removal of the third party during data transactions. This can lead to faster and less costly transactions with higher privacy. For example, if one user wants to pay another user by card without blockchain, it seems like this is a direct transaction from one user to another. However there is a third party involved in the form of the bank. When this transaction is made, the bank must ensure that sender has sufficient funds in their account before sending the money. Once this has been proven, the bank then sends the other user the required amount of money which are kept in the bank's database. With blockchain, the sender's funds are already distributed among the relevant parties in an encrypted block that is within the ledger. Once the transaction occurs, an exchange of keys happens between the involved parties and block with the required information is decrypted. This makes the role of the bank obsolete [11].

Blockchain could also give solutions to the data privacy issue with personal data. Blockchain technology will only allow the access of personal data upon the owner's approval. The block which contains the required information will only become decrypted once the lawful owner and the third party agree to exchange decryption keys [11]. This can protect people's privacy when it comes to companies selling personal data for monetary profit.

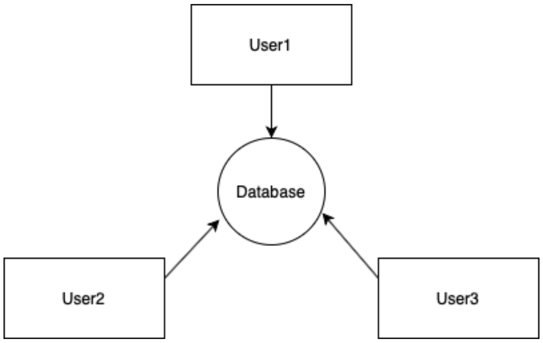

Fig. 2. Traditional Database [11]

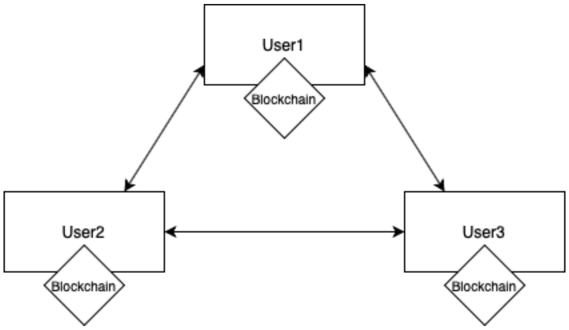

Fig. 3. Blockchain transactions [11]

## VI. Conclusion

Smart cities may appear as a subject of the future but in fact the future is now, with Smart Cities being developed and implemented all around the world at this present day. The benefits society will reap from the enhanced services and optimisation of resources acquired from the big data collected by IoT are endless including aspects such as more effective decision-making, improved citizen and government engagement, safer communities, upgraded transport services, enhanced infrastructure and even reduced environmental footprint. Smart Cities can harvest data for the good and the bad which can be seen in many cases across the globe today. The ever so increasing reliability on data puts everyone's personal information at risk and creates a need for security and protection of this data. The future of Smart urban development is looking bright with the introduction of new technology such as 5G and blockchain which will enhance IoT performance and improve citizens' data security.

## References

[1] Beheshti, B., 2020. What 5G Means For Smart Cities. [online] Smart Cities World. Available at: https://www.smartcitiesworld.net/opinions/opinions/what-5g-means-for-smart-cities

[2] Buckley, C. and Mozur, P., 2020. How China Uses High-Tech Surveillance To Subdue Minorities. [online] Nytimes.com. Available at: https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

[3] Delaney, K., 2020. Next-Gen Wireless: The Platform For Tomorrow's Smart Cities. [online] Newsroom.cisco.com. Available at: https://newsroom.cisco.com/feature-content?type=webcontentarticleId=2018982

[4] Founan, A. and Hayar, A., 2018. Evaluation of the concept of the smart city through local regulation and the importance of local initiative. 2018 IEEE International Smart Cities Conference (ISC2),.

[5] Linchpin SEO. 2020. Trends That Will Transform And Shape Smart Cities In 2020 — Linchpin SEO. [online] Available at: https://linchpinseo.com/trends-that-will-transform-smart-cities/

[6] Mora, O., Rivera, R., Larios, V., Beltran-Ramirez, J., Maciel, R. and Ochoa, A., 2018. A Use Case in Cybersecurity based in Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures. 2018 IEEE International Smart Cities Conference (ISC2),.

[7] Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z. and Bouabdallah, A., 2013. A Systemic Approach for IoT Security. 2013 IEEE International Conference on Distributed Computing in Sensor Systems,.

[8] Sfar, A., Chtourou, Z. and Challal, Y., 2017. A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges. 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C),.

[9] Sidewalk Toronto. 2020. Quayside - Sidewalk Toronto. [online] Available at: https://www.sidewalktoronto.ca/plans/quayside/

[10] Tarín, D., 2020. Privacy And Big Data In Smart Cities. [online] Thesmartcityjournal.com. Available at: https://www.thesmartcityjournal.com/en/technology/341-privacy-and-big-data-in-smart-cities

[11] Theodorou, S. and Sklavos, N., 2019. Blockchain-Based Security and Privacy in Smart Cities. Smart Cities Cybersecurity and Privacy, pp.21-37.

[12] Verkruisen, A., 2020. Privacy In Smart Cities - Smart City Hub. [online] Smart City Hub. Available at: https://smartcityhub.com/collaborative-city/privacy-smart-cities/amp/