Plan:

Smart Cities, IoT and Security

* A smart city is an urban area that uses different types of electronic IoT sensors to collect data and then use insights gained from that data to manage assets, resources and services efficiently.
* Keep paper as tutorial in nature
* 3000-4500 words.
* Max 6 figures/tables.
* Max 15 references – min 5 academic papers

Introduction:

* Explain concept of smart cities
* Outline topics that will be discussed.
* Explain why my research is important – i.e. what importance smart cities have

Security/Performance of smart cities:

* A lot of info from <https://sci-hub.tw/10.1109/ISC2.2018.8656694>
* Base off of the Pillars of Cybersecurity for Smart City
* Since the IoT use cases are growing in the Smart Cities, their data is also increasing in an uncontrolled way, opens a huge gap for cyber attacks.
* Blockchain for reducing security gaps – cryptography – provides security, data integrity, and anonymity thanks to its feature to record each transaction in an immutable way.
* A city is a system with a unique history and specific context [6].To ensure good cohesion at the city level, it is necessary to ensure that all key actors in the city work together using resources in an optimized way, all to speed up the transition and at the same time for more effectiveness at the project level.
* The "intelligence" of a city is shown primarily by its capacity to gather its resources and to achieve the objectives emphasized and especially through the rate of satisfaction of the needs of its inhabitants, while ensuring an effective involvement of the inhabitants in the approach
* 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)*,.
* (Mora et al., 2018)
* Smart Cities are firmly based on IoT sensors and actuators to improve services by automation and reducing operational costs. However, IoT solutions and their interoperability in the Smart City can open the door for Cybersecurity issues able to collapse critical services.
* Failures can appear as part of the interaction of the different cyber-physical systems, their cycle of life and proper maintenance or presented intentionally exploiting security breaches in systems including social engineering [15]. As a consequence, as part of the resiliency strategy, the cities implement strict controls to survey the Smart Citizen activities to avoid the possibilities of Cyberinfrastructure failures due to hacking activities. In this case, we are falling into a dilemma of choosing to privilege privacy or security for the Smart City.
* Blockchain technologies promise to help in this dilemma by improving Cybersecurity as well as user’s privacy.

![A close up of a mans face

Description automatically generated]()

* Since the Citizens are the users of the system depending on its role (industry, government authority, academic, civil), they have different levels of access to the Smart City cyberinfrastructure. The process node relates to activities of citizens integrating the proper security policies to keep a sage IT infrastructure.
* In the centre, all the IoT Smart Devices works autonomously on behalf of his owners to improve their life as ID tags, healthcare wearables, sensors, actuators, or other devices. For each edge, the relation of privacy looks to protect the sensitive data of citizens used on the IoT and IT cloud environments. The safety edge guarantees many automated tasks from city cyberinfrastructure to run in a safe manner for the citizens. Reliability edge connects the IT infrastructure with the probability of failures and security threats. From the IoT smart devices, we need to manage ID and access control as well as trusted that the device is safe and acknowledged to connect to the IT infrastructure with responsible processes to enhance and keep security.
* In this standard, we can see that weak reliability of systems among processes due to the complexity of the city to interoperate different systems, lead to having an impact in citizens privacy and the increment of devices and processes to identify users in the cyberinfrastructure. Many cities, to keep security create an active link between citizens and IT infrastructure not balancing reliability, safety on the processes. That explains why the citizens are challenging how to protect their privacy rights against governments.
* There is an extensive collection of systems to verify the personal identity in the physical world, such as IDs, Social Security number, driver licenses, national passports documents and others. We can trust on those authentication systems. However, all of them make weak once we realized that in some way or another, falsification of them occurs. To overcome that, surveillance systems of Cyberinfrastructure must integrate several steps of credentials validation. Among them, cities are running image processing for facial recognition on all their street cameras tracking the citizens to improve the safety of processes in the city. Moreover, in some cases, citizens are tracked by the government authorities on their daily digital world interaction, not allow them to have control of their sensitive data threating their privacy.
* 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)*,.
* (Sfar, Chtourou and Challal, 2017)

![A picture containing text, map

Description automatically generated]()Graphical illustration of the IoT context

according to its main elements (nodes) and their

relationships (edges)

* 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*,.
* (Riahi et al., 2013)
* A. Person
* The first node plays a fundamental role in the IoT security framework. The human resources are responsible for security rules management, which includes:

• Defining security practices and rules.

• Auditing practices and rules efficiency.

• Applying practices and rules when into operational mode.

* Due to the complex environment of the IoT, this node is a vital component in security management and enhancement. To this purpose, the human component should be able to analyse the context of IoT, individuate its advantages and limitations, and exploit the technology evolution to bring adequate solutions.
* B. Process
* The second node refers to a means to accomplishing tasks in the IoT environment according to some security requirements. The process is required to be compliant with the security policies in order to keep the environment secure at different levels. Furthermore, due to the complexity of the model and the presence of different interactions originating from this node, security processes are difficult to implement.
* C. Intelligent Object
* This node is the heart of the new approach. It refers to an “object” augmented by the electronic features needed to let it communicate with other objects in the surrounding environment. These objects will become active participants in business, information and social processes [2].
* D. Technological ecosystem
* This node refers to technological choices made to ensure IoT security. According to [15], information security technology falls into several broad categories:

• Security Design and Configuration

• I&A: Identification and Authorization

• Enclave internal

• Enclave boundary

• Physical and environmental

* The choices related to each of these elements may include system architecture, communications protocols, implemented algorithms, access control methods, performance, etc. It is evident that a trade-off among security requirements, feasibility and technology evolution should be found in order to ensure the appropriate level of security without degrading the performance of the system.

Tensions: These tensions represent the dynamical character of the model.

* A. Identification and authentication
* “Identification and authentication” is the tension that ties the intelligent object with the person. In the IoT context, objects are spread globally. An efficient resolution scheme needs to be set to identify different entities. Privacy and other security issues must be taken into consideration as well as the specific function of the object, which can change over the time. Furthermore, an object can have one core identity and several temporary identities; an hospital can become a meeting place for a health conference or a shelter after a fire [3].
* B. Trust
* “Trust” is the tension that ties the intelligent object with the technological ecosystem. Basically, it represents the level of confidence that the environment can grant to the intelligent object.
* C. Privacy
* “Privacy” is the tension that ties the person with the technological ecosystem. Privacy is an important tension in the systemic model for IoT security because of the ubiquitous character of the environment.
* D. Responsibility
* “Responsibility” is the tension that ties the intelligent object with the process. In order to share resources and other added values, which are useful for different processes, privileges and access rights must be clearly defined according to privacy constraints. In addition, responsibilities and liabilities rules of each entity must be considered in order to avoid dangers when the object regulates a process.
* E. Autoimmunity
* “Autoimmunity” ties the intelligent object in self-loop. The objective of this tension is to propose an artificial immune system solution for IoT.
* F. Safety
* “Safety” is the tension that ties the person with the process. An environment permeated with intelligent objects is supposed to cope with many security challenges. One of these is ensuring safety when a sudden failure occurs for one or many system components. Then, safety must be considered as a mean to reduce the possibility of damage.
* G. Reliability
* “Reliability” is the tension that ties the process with the technological ecosystem. The reliability deals with data and communications management. The reliability aims at guaranteeing availability of information over time through efficient ways of managing data repositories. Reliability of communication links can be ensured through the redundancy provided by multiple paths.

Real World Applications (i.e. case studies):

* IoT based access control: distributed system over a specific area, with the purpose of selectively restricting access to physical and virtual spaces.
  + DAC – discretionary access control models where the creator of an object is assigned all the rights of the object and can transmit all or part of their rights to other users.
  + MAC – mandatory access control model regulates access based on the classification of subject and objects in the systems.
* **Sidewalk Toronto. 2020. Quayside - Sidewalk Toronto. [online] Available at: <https://www.sidewalktoronto.ca/plans/quayside/> [Accessed 20 May 2020].**
* Digital innovation is essential for catalysing an ecosystem of new services and solutions to urban challenges by individuals, Canadian companies, local Toronto entrepreneurs, and other third parties from around the world. But digital innovation raises a number of challenges that cities are just starting to address, such as making sure there is a transparent process for protecting privacy and the public good.
* These challenges are especially complicated for “urban data,” which Sidewalk Labs defines as information gathered in the city’s physical environment, including the public realm, publicly accessible spaces, and even some private buildings. There have been important initial strides to advance the conversation around data governance principles, but no place has yet adopted a comprehensive approach to address these challenges and create the conditions for digital innovation to flourish responsibly.
* First, Sidewalk Labs proposes to establish open digital infrastructure that provides a shared foundation for using urban data to improve quality of life. This core infrastructure would be anchored by ubiquitous, affordable internet connectivity within the IDEA District, consistent with Waterfront Toronto’s aspirations for closing the digital divide. It would also include physical mounts that can significantly reduce the cost of launching new digital innovations and help ensure that cities do not get locked into using proprietary solutions.
* Second, Sidewalk Labs proposes to outline clear standards that make data publicly accessible, secure, and resilient. Today’s urban data tends to be scattered across many owners, outdated, or stored in messy file formats, making it difficult for the community to use as a foundation for new ideas. Clear standards would make (properly protected) urban data accessible to researchers and the community in real time, and make it easy for third parties to build new services or competitive alternatives to existing ones.
* Third, Sidewalk Labs proposes a trusted process for responsible data use that builds on existing privacy laws and would apply to all parties (including Sidewalk Labs). This process would be anchored by a Responsible Data Use (RDU) Assessment — an in-depth review that is triggered by any proposal to collect or use urban data — and guided by a set of RDU Guidelines that incorporates globally recognized Privacy by Design principles. The process, including approvals, would be overseen by an independent, government-sanctioned Urban Data Trust created to be a steward of urban data and the public interest without stifling innovation. Furthermore, it would ensure that urban data that does not pose privacy risks (such as air-quality data) would be made publicly accessible by default, enabling companies, community members, and other third parties to use it as a foundation to build new tools.
* 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> [Accessed 20 May 2020].
* KASHGAR, China — A God’s-eye view of Kashgar, an ancient city in western China, flashed onto a wall-size screen, with colorful icons marking police stations, checkpoints and the locations of recent security incidents. At the click of a mouse, a technician explained, the police can pull up live video from any surveillance camera or take a closer look at anyone passing through one of the thousands of checkpoints in the city.
* To demonstrate, she showed how the system could retrieve the photo, home address and official identification number of a woman who had been stopped at a checkpoint on a major highway. The system sifted through billions of records, then displayed details of her education, family ties, links to an earlier case and recent visits to a hotel and an internet cafe.
* The system taps into networks of neighborhood informants; tracks individuals and analyzes their behavior; tries to anticipate potential crime, protest or violence; and then recommends which security forces to deploy, the company said.
* On the screen during the demonstration was a slogan: “If someone exists, there will be traces, and if there are connections, there will be information.”

Privacy concerns:

* 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> [Accessed 20 May 2020].
* (Tarín, 2020)
* So, let’s get to the point; or rather, the data. The development of Smart Cities inevitably entails the processing of all kinds of information; Geo-location, traffic, energy consumption, environmental etc, much of which falls within the scope of the Data Protection Act and, consequently, its collection and use for this purpose are prohibited without the informed consent of those individuals concerned. The interconnection of all this information in order to create available products and services for people to make cities more efficient and sustainable will have a clear impact on the privacy of these people, even though they will be the main beneficiaries of these services.
* Due to the exponential growth in Big Data that is gradually being stored within Smart Cities, this deserves special attention while pausing to reflect on the concept of profiling. That is, creating profiles of the users or consumers of various public or private services in order to obtain large amounts of information via data-mining techniques, to analyse common behaviour patterns so as to offer advanced solutions and resource optimisation according to statistical inferences. For example, through intelligent transport titles with NFC (Near Field Communication) technology, profiles about a person’s travel, habits and customs can be made based on certain urban public transport usage. As well as this, even fields such as how many people can live in a house, what timetables they have or their lifestyles can be profiled through domestic energy consumption information.
* Included in this area it should be noted that the concept of “person”, as developed by the software expert Alan Cooper, through the creation of an intermediate level of Personal Data, this does not concern an “identified or identifiable person”, but rather archetypes or models of people who meet a number of common characteristics and specific needs, This way they provide an easily analysable profile, without making reference to any real person ‘behind’ the processed information and so protecting the link to the subject's identity. Once officially recognised, methodologies such as this would avoid deficiencies in the collection of consent regarding the information you ‘have to borrow at interest’ when dealing with your data or in the use of costly security measures. It would not really be processing Personal Data from identifiable people and therefore solutions could be implemented in the interest of the community.
* In the same way as detractors of innovation force us to suspect that the large-scale data processing produced by the interconnection of different data gathering sensors can lead to a serious invasion of our privacy, we cannot ignore reality and give in to the fear of the unknown. Unstoppably, Open Data initiatives are progressing rapidly in many administrations and at all territorial levels across Spain, sponsored under the 37/2007Act on the reuse of public sector information. We therefore have an obligation to work towards consensual solutions which respect the privacy of individual people, and which can harness data analysis to improve infrastructure management, quality of life and coexistence among people.

Future trends:

* **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/> [Accessed 20 May 2020].**
* Year 2020 is not just a new year but the signal of a new decade. The concept of 5G is slated to dominate this year with the biggest names in telecomm like Verizon, Nokia, Ericsson, AT&T, and more making sure that their 5G offerings stay on point. In the same token, Android’s handset makers will hit the ground hard and running with their 5G offerings in 2020. Because of faster speeds and more reliable connection, smart cities will reap its benefits by being able to offer smarter vehicles, smart processing and manufacturing, and more because they rely on this technology, too. Phones will not just be improved, but just about anything that impacts a human being’s daily life shall be affected positively by the onset of 5G.
* **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=webcontent&articleId=2018982> [Accessed 20 May 2020].**
* Model smart cities like Barcelona, Vancouver, and Singapore (to name but three) have already demonstrated the profound impact of digitization on urban communities. But the next wave of innovation will be even more data intensive.
* To meet that demand, WiFi 6 and 5G each offer tremendous advantages in bandwidth, speed, and latency. And each have their unique strengths in complex urban environments. As Cisco CEO Chuck Robbins has said, “WiFi 6 and 5G are made to work together."
* “The creation of wealth, the ability to manage cities, the ability to make any place a great place, are going to be increasingly enhanced,” said Louis Zacharilla, an author and co-founder of the Intelligent Community Forum. “Because of 5G, because of IoT, we’re going to be able to reconfigure our infrastructures so that we can do the kinds of things that we want to do as part of our daily living.”
* For citizens, that means greatly enhanced interactions with one another, with government services, and with the environment around them, especially in the kinds of public spaces in which WiFi 6 excels.
* “WiFi 6 enables you to not just focus on your phone and staring down,” said Peterson, “but to interact with the environment around you. The Internet of Things is a big part of what’s going to be enabled by WiFi 6.”
* Zacharilla expects 5G and WiFi 6 to drive advances in citizen participation and awareness, education, health care, security, and sustainability. Critically, these benefits will extend to the growing number of megacities in the developing world, as urban migration continues to surge and resources and infrastructures are strained to the limit.
* **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> [Accessed 20 May 2020].**
* The creation of smoother and safer living through a gradual digital transformation is already beginning in some world cities, but it does not end there. Streets, buildings, public and personal devices need to be interconnected.
* Sensors must be placed everywhere to collect data. The massive amount of data generated by these sensors then needs to be communicated, analysed and fed back to the infrastructure to affect changes in the operation of smart cities.
* As an example, Barcelona’s sensor-embedded parking spots already connect with an app that directs drivers to available spaces. Projects are also underway in cities including Stockholm, Amsterdam, Copenhagen and Columbus, Ohio to realise the smart city vision as well.
* 5G brings about a massively improved platform to deliver scalable and reliable connectivity to the world. The technology is designed to be high data-rate and low-latency. These two characteristics allow for fast real-time transfer of data between two or more points. This will allow for many new applications to be deployed that were not possible before 5G.
* 5G is an enabling technology for IoT, and as smart cities essentially rely on IoT to function, 5G and smart cities are inextricably linked. As such, 5G will play a critical role in allowing information gathered through sensors to be transmitted in real time to central monitoring locations.
* Specifically, 5G offers massive machine type communication (MMTC) and critical machine type communication (CMTC). MMTC is intended for a large number of IoT devices, effectively a large number of sensors and actuators sending a lot of data back and forth. Example applications include smart buildings, logistics and fleet management, as well as air and water quality monitoring. It is designed to be latency-tolerant, efficient for small data blocks to be transmitted or received, and to be sent on low bandwidth pipes.
* **Theodorou, S. and Sklavos, N., 2019. Blockchain-Based Security and Privacy in Smart Cities. Smart Cities Cybersecurity and Privacy, pp.21-37.**
* **(Theodorou and Sklavos, 2019)\**
* Blockchain is defined as a “distributed ledger network using public-key cryptography to cryptographically sign transactions that are stored on a distributed ledger, with the ledger consisting of cryptographically linked blocks of transactions. The cryptographically linked blocks of transactions form what is known as a blockchain” [16]. To put it simply, blockchain can be seen as a spreadsheet that can be accessed by any computer in the network, and it tracks all the actions of these computers [17].
* To understand what blockchain has to offer, it would be useful to see a simple card payment transaction and com- pare the scenario with the traditional way of payment. Let us think of a scenario in which user A wants to pay user B by card. Even though it seems like this is a direct interaction of A with B, in fact user A authorizes her bank to investigate by searching its database to determine whether A had sufficient funds to pay B. If this is true, the bank pays B with funds that are kept in the bank’s database in order to close the transaction. The bank pays user B directly, therefore A pays user B indirectly. With blockchain technology, the funds of A are already distributed to all relevant parties in the form of an encrypted block that resides in the ledger. Upon the exchange of keys between the involved parties, the block that holds the information about A’s funds is decrypted. Therefore, the role of the third party (in this case, the bank) becomes obsolete. There is a strong belief that the elimination of the third party in the process of the closing of a transaction will have, as an effect, the faster and less costly transaction with higher privacy.
* Additionally, blockchain could provide solutions to the privacy of personal data. It is well known that end users’ personal data are resold between companies. Many users are opposed to these practices, as they have concerns regarding the circumstances of distributing, and especially storing their data. The use of blockchain will permit the access of personal data only upon the owner’s approval. The block that holds the information will only be decrypted as long the lawful owner and the third party agree to exchange decryption keys

A picture containing clock

Description automatically generated

Telecoms paper resources

IEEE: A Use Case in Cybersecurity based in Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures <https://sci-hub.tw/10.1109/ISC2.2018.8656694>

IEEE: Evaluation of the concept of the smart city through local regulation and the importance of local initiative <https://sci-hub.tw/10.1109/ISC2.2018.8656933>

IEEE: Application of Internet of Things and Big Data towards a Smart City <https://sci-hub.tw/10.1109/IoT-SIU.2018.8519920>

A Standard-based Open Source IoT Platform: FIWARE <https://arxiv.org/pdf/2005.02788.pdf>

Case studies: <https://urbantide.com/fullstory2/blog/2014/11/5/5-smart-cities-case-studies>