ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Privacy and Security for Internet of Things (IOT) Smart Cities with implementing Analytics on (Network Data) Using Big Data Technologies (HADOOP)

Dhafer Sabah Yaseen
Master of Science (Information System),
Nizam College (Autonomous), O.U,
BasheerBagh, Hyderabad.

T.RamdasNaik
Assistant Professor, Computer Science (PG)
Nizam College (Autonomous), O.U,
BasheerBagh, Hyderabad.

ABSTRACT:

Smart cities is a buzzword of the moment this paper has tried to establish that while the political and economic drivers of smart cities tend towards technology supremacism, smart cities, at least in Europe, will still suffer as a project if they fail to get privacy right; and that at the moment this failure is very likely, suffering as they do from the combination of three of the most difficult issues for modern privacy law to regulate: the IoT, Big Data and Cloud based infrastructure. DP is still fit for purpose and in principle does not need modified, though the detail may need some fine honing to deal with threats such as the increasing marginalisation of informed consent, big data, the IoT and the Cloud. The FTC's reaction is surprisingly similar: faced with the enumerated issues of IoT above, and even without the cultural foundation of an omnibus privacy law founded in human rights to depend on, they still assert "protecting privacy and enabling innovation are not mutually exclusive and must consider principles of accountability and Privacy by Design". "Code" solutions may be more useful and should certainly be investigated to supplement the law. Four particular suggestions for further research involvement are herein promoted:

(i) Investigation into the potential for a smart city PIA or DPIA;
(ii) Investigation into the technical and social potential of methods of giving "pre-consent" or "sticky consent" to deal with the constraints of the IoT;
(iii)Legislating for algorithmic transparency and researching ways of making algorithmic data comprehensible to consumers;
(iv)Moving at least partially away from consent or "notice and choice" as a main mechanism for validating data collection and processing; connectedly, prohibiting certain data processing activities even where there is consent.

INTRODUCTION:

In order to enable a fast uptake of the IoT, key issues like identification, privacy and security and semantic interoperability have to be tackled. The interplay with cloud technologies, big data and future networks like 5G have also to be taken into account. Open and integrated IoT environments will boost the competitiveness of European SMEs and make people's daily life easier. For instance, it will be easier for patients to receive continuous care and for companies to efficiently source components for their products. This will lead to better services, huge savings and a smarter use of resources. To achieve these promising results, I think it is vital to enhance users' trust in the Internet of Things. The data protection legislation and the cyber security strategy proposed by the European Commission clearly go in this direction. I am confident that the following chapters will cater for interesting reading on the state-of-the-art of research and innovation in IoT and will expose you to the progress towards the bright future of the Internet of Things with focusing for Big Data .

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

SMART CITIES

Smart Energy , Smart Building , Smart Health , Smart Industry and specially "Smart cities" (see Figure 1) are a buzzword of the moment. Although legal interest is growing, most academic responses , are still from the technological, urban studies, environmental and sociological rather than legal, sectors and have primarily laid emphasis on the social, urban, policing and environmental benefits of smart cities, rather than their challenges, in often a rather uncritical fashion . However a growing backlash from the privacy and surveillance sectors warns of the potential threat to personal privacy posed by smart cities. A key issue is the lack of opportunity in an ambient or smart city environment for the giving of meaningful consent to processing of personal data; other crucial issues include the degree to which smart cities collect private data from inevitable public interactions, the "privatization" of ownership of both infrastructure and data, the repurposing of "Big Data" drawn from IoT in smart cities and the storage of that data in the Cloud.

Figure 1 IoT - Smart

INTERNET OF THINGS (IoT)

Smart cities combine the three greatest current threats to personal privacy, with which regulation has so far failed to deal effectively; the Internet of Things(IoT) or "ubiquitous computing"; "Big Data" ; and the Cloud. While these three phenomena have been examined extensively in much privacy literature (particularly the last two), both in the US and EU, the combination is under-explored. Furthermore, US legal literature and solutions (if any) are not simply transferable to the EU because of the US's lack of an omnibus Data Protection (DP) law. I will discuss how and if EU DP law controls possible threats to personal privacy from smart cities and suggest further research on two possible solutions: one, a mandatory holistic privacy impact assessment (PIA) exercise for smart cities: two, code solutions for flagging the need for, and consequences of, giving consent to collection of data in ambient environments.

IoT ARCHITECTURE

It clearly emerges that most Smart City services are based on a centralized architecture, where a dense and heterogeneous set of peripheral devices deployed over the urban area generate different types of data that are then delivered through suitable communication technologies to a control center, where data storage and processing are performed.

A primary characteristic of an urban IoT infrastructure, hence, is its capability of integrating different technologies with the existing communication infrastructures in order to support a progressive evolution of the IoT, with the interconnection of other devices and the realization of novel functionalities and services.

Another fundamental aspect is the necessity to make (part of) the data collected by the urban IoT easily accessible by authorities and citizens, to increase the responsiveness of authorities to city problems, and to promote the awareness and the participation of citizens in public matters. see description of the different components of an urban IoT system, as sketched in Figure 2.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

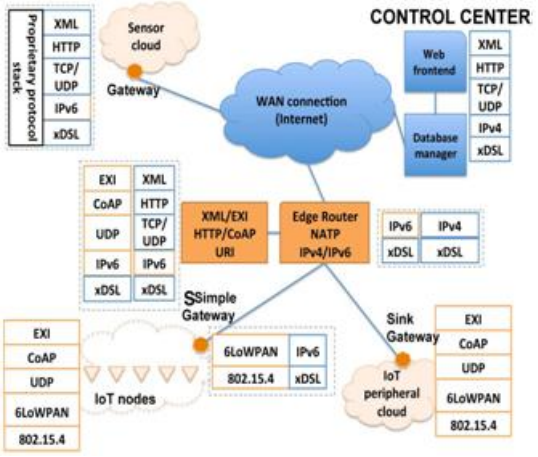

Figure 2 Conceptual representation of an urban IoT network based on the web service approach

We describing the web service approach for the design of IoT services, which requires the deployment of suitable protocol layers in the different elements of the network, as shown in the protocol stacks

IoT STRATEGIC RESEARCH AND INNOVATION DIRECTIONS

The development of enabling technologies such as nanoelectronics, communications, sensors, smart phones, embedded systems, cloud networking, network virtualization and software will be essential to provide to things the capability to be connected all the time everywhere. This will also support important future IoT product innovations affecting many different industrial sectors. Some of these technologies such as embedded or cyber-physical systems form the edges of the "Internet of Things" bridging the gap between cyber space and the physical world of real "things", and are crucial in enabling the "Internet of Things" to deliver on its vision and become part of bigger systems in a world of "systems of systems". An example of technology convergence is presented in Figure 3

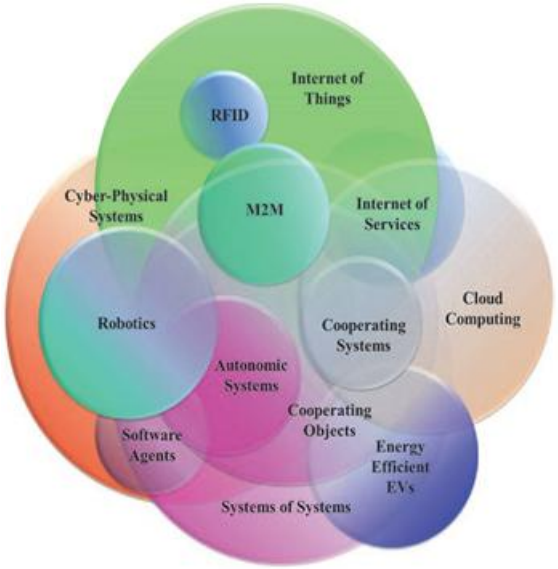

Figure 3 Technology Convergence

RESEARCH SECTIONS:

This research focus falls into five main sections.

First : I sketch the rise of smart cities globally, both in the West and East and the less developed South, and discuss the key technological, economic and political drivers which have made them an unstoppable part of the future urban living conditions of much of the global population. Rather than giving one formalistic definition of smart cities which will inevitably be a moving target and may not aid legal analysis, I try to sketch their key characteristics, focusing on two which are clearly problematic from a privacy frame: first, their dependence on technological infrastructures, big data, the IoT and the Cloud; and second , their financing and hence "ownership" in almost all cases by public-private partnerships (PPP).

Second: I lay out the well known vulnerability of smart cities, Security and Privacy for Smart cities, along with other venues for embedded IoT systems, to security threats and how this is approached by the law. This section covers well trodden ground and is therefore relatively short. It should be noted that considerations of "privacy" (wrongly so named and limited) in smart cities often stop here.also I turn to broader issues of conceptual privacy law frameworks,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

and lay out what may be perceived as a basic underlying theoretical problem, ie, that smart cities are, in essence, public places while traditionally privacy laws such as European Convention on Human Rights (ECHR) and US privacy torts have applied to private "bubbles" or zones focused on the body, the home and private communications. Drawing on ECHR case law as well as attitudinal research, I argue reasonable expectations of privacy even in public spaces, as in smart cities, are now both recognised by European law and needed by urban dwellers.

Thirdly : In this section, I turn to some solutions drawn not from law, but from "code" in the Discussion of Privacy by Design (PbD). Three particular avenues for further promising investigation are identified:
(i) exploring the development of a holistic privacy impact assessment (PIA) for smart city data flows; (see figure 4).

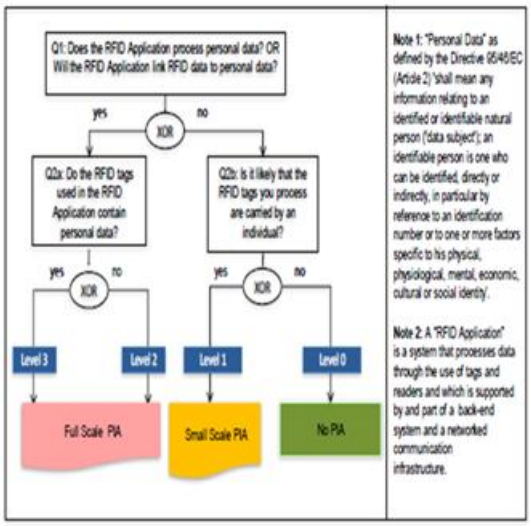

Figure 4 Decision Tree on whether and at what level of detail to conduct a PIA

(ii) finding new means for obtaining some kind of standing or "sticky" consent to data processing decoupled in time from when the data is actually pervasively collected via the IoT;
(iii) implementing a legal right to algorithmic transparency and finding ways of making this knowledge useful to ordinary users.

Fourthly : in the most crucial section, I address in some detail the three key threats to privacy and DP already identified – the IoT, Big Data and the Cloud - and outline how each problem manifests itself to endanger the privacy of smart city residents and users. In each subsection I then try briefly to analyse how, and how well, EU DP law currently deals with regulating, preventing or solving these threats.This section concludes pessimistically. Despite the many recent rhetorical assertions, politically required by the lobbying wars of the draft General DP Regulation (GDPR) and the Silicon Valley ideological thrust towards "permission less innovation", that DP law remains fit for purpose in principle, and merely needs tweaked in its detail to address technological challenge, in fact, a number of key challenges so far appear relatively insuperable by legal regulation alone.

Notable amongst these is the issue of how to obtain meaningful prior consent in Internet of Things systems, especially where data is collected in public, as eg in smart road or smart transport systems. A second key issue identified is how ordinary users can have any feeling of control over the processing of their data when "big data" through the notion of purpose limitation and data minimization, and the algorithms used to create inferences from it are opaque and capricious to them. Finally The dependence of smart cities on Cloud infrastructure which may be located anywhere in the world also makes them highly dubious from an EU DP point of view.

Fifth: In this section the important part of this project through some implementation for Big data using Hadoop and Hadoop Ecosystem and how to store the data in clustering mode and how process it and after that how analytic the data to get the information and reports .

RESEARCH PURPOSE:

In this thesis the view that to preserve privacy in smart cities we may need to move away from the liberal notion of "notice and choice" or, in European terms, "consent" and informed specific control over

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

processing, entirely, and look instead to an "environmental" model of toxic processes which should be banned or restricted notwithstanding user permission or substitute grounds for processing. This view, which is only tentatively introduced here, will be justified further in future work.In the project we can find the exact what time more users using the network and what time more downloads and uploads happening as example for using the Big Data technologies . Based on that, they can concentrate tower capacity enhancements. If the tower is underutilized then they can reduce the tower capacity. They can concentrate the area where they can invest more to get the more users. Find out the areas of partner leading and try to improve the owner tower installations.

RESULT REPORTS

As final step of the research we collect the results of analytics data and using reporting software to process that information as reports.

- The daily user count and bytes transmitted on a particular time slot is a part of report results (see figure 5).

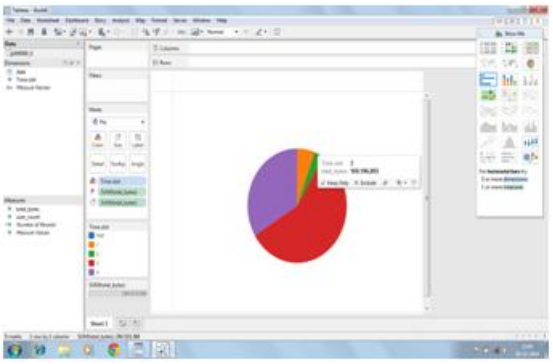

Figure5. Daily user count and bytes transmitted

- Area wise business(usage) share in the total business another part of report results (see figure 5).

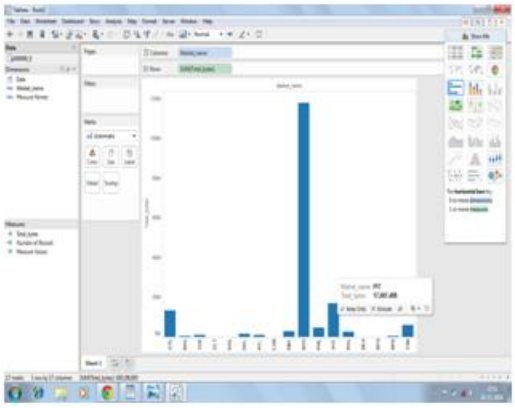

Figure 6 Area wise business (usage)

EXISTING SYSTEM:

IoT Smart Cities are dealing the huge amounts of data from sensors and cards usage records every day. There is a great challenge not only to store and manage such a large amount of data, but also to analyze and extract meaningful information from it, and getting the benefit out of that analysis. There are several approaches to collecting, storing, processing, and analysing big data .Present these analysis activities are happening using data warehousing technologies. But it is more expensive and time consuming.

PROPOSED SYSTEM:

Aim of thesis focusing on the risk of IOT Smart Cities in Security and privacy because there was broad agreement among participants that increased connectivity between devices and the Internet may create a number of security and privacy risks.The security risks in IoT devices may present a variety of potential security risks that could be exploited to harm consumers by:

(1) enabling unauthorized access and misuse of personal information;
(2) facilitating attacks on other systems;
(3) creating safety risks.

In addition to risks to security, participants identified privacy risks flowing from the Internet of Things. Some of these risks involve the direct collection of sensitive personal information, such as precise geo-location, financial account numbers, or health

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

information – risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to infer it. And for aim of the implementation project is finding the business insights of current user records data. And get the benefits for business growth.

The parameters to be considered for analysis are Daily user count and bytes transmitted on a particular time slot. Area wise business(usage) share in the total business. Since every network owner will be depending on partners to get the service where they does not have the service tower. To help better in this area, we are using the Hadoop and Hadoop Eco-systems.

CONCLUSION:

In this paper, we have investigated on the future of smart cities is important. They may offer solutions to some of our worst problems – conserving energy and creating a sustainable environment, maintaining public safety, engendering community, rescuing millennials from depression and loneliness, reducing road deaths. In cities with areas of mixed and multiple deprivation like the writer's own home town, Glasgow, their appeal is obvious and not to be rejected, even if a degree of cynicism on how much benefit will accrue to vendors and municipal leaders rather than the residents is reasonable.

But even within this context, privacy and security are important : if not simply as a fundamental right, then instrumentally, as a prerequisite to keeping the trust and engagement of smart city dwellers. By now, as a society, we have a number of salutary stories of what happens when technology is perceived as dangerous and out of control, rationally or irrationally: eg the backlash against GM crops and their products; the fear of "killer robots"; on public disquiet, all come to mind.

Even in the EU with its history of strong rights-based laws, DP solutions applicable to smart cities are so far generic and tenuous, and look to be getting further away not nearer, even after three years of negotiations on the GDPR.DP is still fit for purpose and in principle does not need modified, though the detail may need some fine honing to deal with threats such as the increasing marginalisation of informed consent, big data, the IoT and the Cloud. The FTC's reaction is surprisingly similar: faced with the enumerated issues of IoT above, and even without the cultural foundation of an omnibus privacy law founded in human rights to depend on, they still assert "protecting privacy and enabling innovation are not mutually exclusive and must consider principles of accountability and Privacy by Design".

But other voices from industry, security and policy grumble loudly beside them ; the UK as a business-friendly outlier in the privacy culture of Europe has been one of the principle voices pressing for a more "risk-based" application of DP law which has potentially found its way into various parts of the General Data Protection Regulation (GDPR) ; and enforcement, rather than the principles themselves, remains the key failure point of DP law, even more so when taking account the effective landgrab by the EU over data processing by non EU companies working in EU. Just as declaring "safe harbor" void will not in practice stop data flowing to Google, Facebook, Amazon et al, merely make it it a bit more difficult, so privacy in smart cities can also not be safeguarded by ever more exhortations to respect the law, particularly as that law becomes ever more complex and subtle to interpret.

In this researchers opinion, solutions in natural surveillance architectures such as smart cities must be built into the code of these cities – not just their software and hardware but their material design. This is the principle of "privacy by design", and in the final section, I examine this both in abstract, and with some concrete examples of solutions proposed by data scientists and human: computer interaction (HCI) specialists.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCES:

[1] Mukherjee, A.; Datta, J.; Jorapur, R.; Singhvi, R.; Haloi, S.; Akram, W. (2012) "Shared Disk Big Data Analytics with Apache Hadoop"

[2] Garlasu, D.; Sandulescu, V. ; Halcu, I. ; Neculoiu, G. ;(17-19 Jan. 2013),"A Big Data implementation based on Grid Computing".

[3] Kestelyn , J. "Introducing Parquet: Efficient Columnar Storage for Apache Hadoop." at http://blog.cloudera.com/blog/2013/03/introducing-parquet-columnar-storage-for-apache-hadoop/.

[4] D. Agrawal, S. Das, and A. E. Abbadi. Big data and cloud computing: PVLDB, 3(2):1647–1648, 2010.

[5] Aditya B. Patel, Manashvi Birla, Ushma Nair (6-8 Dec. 2012) "Addressing Big Data Problem Using Hadoop and Map Reduce"

[6] Sarwant Singh, "Smart Cities – A $1.5 Trillion Market Opportunity". Forbes / Business (June 20, 2014), at http://www.forbes.com/sites/sarwantsingh/2014/06/19/smart-cities-a-1-5-trillion-market-opportunity/ .

[7] Sarah Spiekerman "The RFID PIA – Developed by Industry, Agreed by Regulators" in David Wright and Paul de Hert eds Privacy Impact Assessment : Engaging Stakeholders in protecting Privacy (Springer, 2011), discussed further infra

[8] 36th International Conference of Data Protection and Privacy Commissioners, 14 October 2014 at http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf ; FTC, supra n 65.

[9] Anne Cavoukian and Drummond Reed Big Privacy: Bridging Big data and the Personal data Ecosystem Through Privacy by Design, 2013, at https://www.ipc.on.ca/images/Resources/pbd-big_privacy.pdf .

[10] G Danezis et al Privacy and Data Protection by Design – from Policy to Engineering (ENISA: Heraklion 2014) p iv.

[11] ICO, Conducting privacy impact assessments code of practice, Version: 1.0 (February 2014), p. 5, at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of- ractice.pdf

[12] Supra n 84. The final document produced is available at A29 WP, Privacy and Data Protection Impact Assessment Framework for RFID Applications (January 12, 2011), available at http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf .

[13] Smart Grid Task Force 2012-14, Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems (March 18, 2014), p. 5, at https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf .

[14] Thierer "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (21) Richmond Jnl of Law and Technology 1 at http://jolt.richmond.edu/v21i2/article6.pdf

[15] Cynically "W3C's failed "DNT" Do Not Track crusade tumbles to ad-blockers' Vietnam", The Register ,29 Jul 2015 at http://www.theregister.co.uk/2015/07/29/dnt_dead_in_the_water/ .

[16] Sammer, E. 2012. Hadoop Operations. Sebastopol, CA: O'Reilly Media.

[17] "HDFS High Availability Using the Quorum Journal Manager." Apache Software Foundation. Available at http://hadoop.apache.org/docs/current/hadoop-yarn/hadoop-yarn-site/HDFSHighAvailabilityWithQJM.html. Accessed on June 5, 2013.