Privacy and Security Concerns for the Internet of Things in the GDPR Era - A Survey

Laura VEGH

Abstract—**Over the past years the Internet of Things (IoT) has become a subject of utmost interest both in research and industry. Technology is now present in most areas of our lives. As a result, security and privacy have become increasingly important and the idea that they must be put first when designing new systems is accepted by more and more people. The high complexity of IoT systems makes it hard to find the perfect security solution and many wonder if this will not be what will eventually stop their evolution. This year saw the enforcement of one of the most discussed privacy regulations of the past decade – The European General Data Protection Regulation, in short, the GDPR. It is a law that aims to give back to the users the power over their personal data. Furthermore, countries worldwide are starting to understand the need for such regulations and are implementing new provisions. Many are concerned that with the known security issues of the IoT, these new laws will slow down the progress made in this area. This article presents a survey of the most important issues in security and privacy in IoT and looks at existing solutions that can be used in the current scenario.**

Index Terms—**Internet of Things, GDPR, security, privacy, data protection.**

I. Introduction

The Internet of Things can be comprised of sensors and various objects connected together and communicating without human intervention. On a lower scale, IoT can be any device, such as smart phones, computers, smart TVs connected to the internet. It is estimated that by the year 2020 there will be 20 billion such devices interconnected. All these devices collect data from the users and often exchange it with other devices in the name of better, customized services. Until recently this has never truly been an issue. Some privacy enthusiasts were concerned by the lack of privacy these devices can bring, others opposed the way in which their data was transferred often without their knowledge or consent. Research focuses on the best methods to ensure privacy and security to a system, but rarely targets the users' rights.

The new European Data Protection Regulation [8], in short, the GDPR, puts the users' rights first. While the huge fines for noncompliance are incentive for most companies, we as researchers need to think beyond the fines. We need to see the opportunity behind a regulation that puts security and privacy first and bring forward the best methods in these areas. In the present paper we present a survey focusing on methods aimed to ensure security and privacy of communications in the IoT. We also discuss these methods from the perspective of the GDPR in order to find those methods that can help compliance with this revolutionary regulation. We also aim to discover new research opportunities by identifying the blind spots left by the existing methods. The paper is structured as follows: in Section 2 we present a summary of the GDPR with emphasis on its requirements for privacy and security while also discussing the worries risen around the use of IoT in the GDPR era. In Section 3 we discuss privacy. Section 4 deals with security. In Section 5 we analyze what might be next in this area, while in Section 6 we discuss a special case in the Internet of Thing – military technology. Section 7 presents some of the most important regulations worldwide, analyzes their relationship to the GDPR and their possible impact for IoT. Finally, in Section 8 we draw the conclusions.

II. General Data Protection Regulation

A. Overview

The GDPR has been enforced on the 25th May 2018. It was approved in May 2016, leaving companies and researchers a two-year period to become compliant. It is considered an almost revolutionary regulation with its stricter provisions and its aim to give back users the power over their data. This means that companies will no longer be able to use any data without consent. This consent needs to be explicit and specific - the person needs to know exactly to what type of processing they are consenting. Also, consenting to have your email address and name saved in order to access certain services will not mean a company can reach out to that person for marketing purposes. That is a different type of consent and it needs to be asked separately.

From the user's point of view, the GDPR means more rights and more protection over their data. Security and privacy become a must in the GDPR. If a data breach occurs and personal data is stolen and if it is proven that the company had not taken all the appropriate security measures, the fines will be of 20 million dollars. Encryption of all data is highly encouraged, although not mandatory. This is another interesting aspect with the GDPR's provisions regarding security. It encourages the use of various methods, in accordance with the level of risk and costs. It is not necessary to use the newest methods out there. Encryption, pseudonymization and, when possible, anonymization are all types of methods that can be used. The list is not closed ended, leaving it up to each data controller to choose the right one. Privacy by design and by default is considered key here.

Users, or data subjects, as the GDPR calls them, also have the right to object to the processing and have the right to withdraw consent at any time. Unless bound by contractual

L. Vegh is with the Technical University of Cluj-Napoca, Romania, Department of Automation, Strada Memorandumului 28, Cluj-Napoca, 400114 (e-mail: laura.vegh@aut.utcluj.ro).

Digital Object Identifier 10.32754/JMT.2018.2.01

purposes, a company, a data controller in GDPR terminology, cannot deny a data subject these rights.

Research has a different status. Organizations processing personal data for research purposes may avoid various restrictions. This is especially true for those researchers using sensitive data (biometric, genetic data). This type of data is heavily regulated within the GDPR, with research being one of the few areas in which its use is permitted. Also, research as a basis for processing can be used to counter the data subject's objection to the processing. Research however, does not have a full status as lawful basis for processing, so institutions will still need to be careful with consent and other legal issues.

Furthermore, an aspect that sets the GDPR apart is that it is not only for public or private companies that are inside the European Union. It is for every public or private company that uses personal data of EU citizens, regardless of the company's location. That means companies worldwide need to comply. And we are not just talking about big companies like Facebook or Microsoft, or about those who sell goods to EU citizens. As an example, if a student from a EU country decides to study in the USA for one semester, that university will need to be compliant with the GDPR at least when it comes to that student's data. We will not go into further detail about how this will work and the options in place for the US or other countries outside the EU as it is not the focus of our paper. However, this aspect is important to mention as it emphasis the difficulties surrounding IoT in the GDPR era.

B. Concerns surrounding IoT

Security for one thing is hard to ensure in IoT, which is why this is a focus in research. However, since the GDPR itself does not request a certain method to be used, this freedom is actually an advantage that can be used to find the best method for each data controller.

Fig. 1 presents the main requirements surrounding privacy by design and by default as per the GDPR. The first step is to perform what is called a privacy impact assessment. It is important both in research and in business, as it allows to analyze the potential consequences on data privacy of the processing activities. The next step is simple - make sure data is always protected, even before processing it. Records of processing activities are again important in all areas and industries, but even more so in the IoT. These records allow for better control over the data but also minimize any risks that come from data being communicated, shared from one device to another. The next three steps regard limitation - of collection, of processing and of access. First of all - only collect data strictly necessary. It goes without saying that this step reduces unnecessary data exposure risks, by only using what is strictly needed. In the same way, limiting data processing reduces the risk of data breaches, by eliminating unnecessary operations. Finally, controlling who has access to the data is a crucial step for preventing attacks and loss of data in any system.

It is important to understand that, as a law, the GDPR sets merely some guidelines for ensuring security. It does not say exactly what methods one must use. This has created a lot of confusion in many cases, as people were expecting a set of rules that tells them exactly what they must do to be complaint. Unfortunately, things are not as simple. It is up to each company, whether public or private, to do everything in their power to protect the data they have. Again, this should be seen more as an opportunity and not as a constraint.

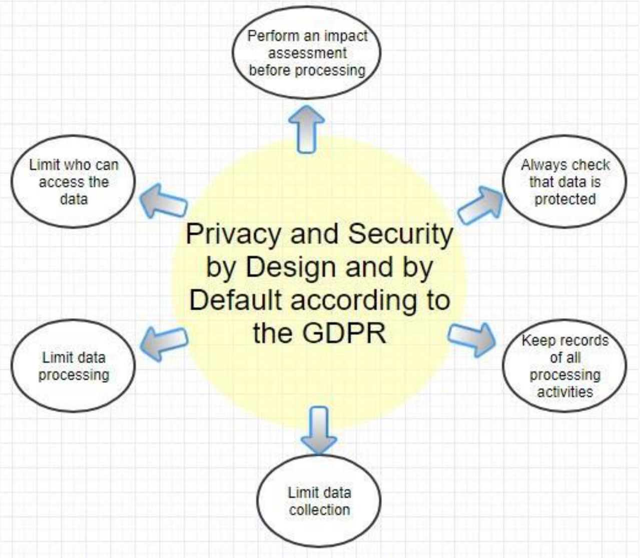
Perform an impact assessment before processing
Limit who can access the data
Always check that data is protected
Privacy and Security by Design and by Default according to the GDPR
Limit data processing
Keep records of all processing activities
Limit data collection

Figure 1. The main steps to achieve privacy by design as per the GDPR

While these steps may not be so hard to implement, two great concerns remain with regards to IoT: consent and location of data. With consent the question that arises is how to make sure it is explicit and specific for each device connected to the IoT? These systems often function in such a way that the communication between devices happens without human intervention. At the moment, it is assumed that a user entering their data for one device in the system, automatically agrees that data can be transferred to other devices, regardless of where they are in order to get a certain service. However, with the GDPR this will no longer be possible. Asking for consent on each device and at every step would be a possibility, but it would take away a lot of the principles of the Internet of Things.

Knowing where data is and ensuring a secure, safe and legal data transfer can also be problematic. Transferring data from one device to another is necessary in many IoT systems. Unfortunately, this also means that a user might not always know where their data is going. Is the new device safe? Does the new device offer at least the same level of security and privacy as the one on which the user gave their consent? All these are questions that need to be answered once the GDPR is enforced.

Research is the areas of security and privacy especially in the area of communications in the IoT is essential. The market is in need of robust solutions, that are fast and easy to implement and also easy to understand for the everyday user.

III. Challenges for Privacy in IoT

The Internet of Things is usually viewed as having either three or five architectural layers. The three-layered approach contains the application, network and perception layer respectively. The five-layered approach contains business, application, processing, transport and perception layer respectively. But these are not the only types of architectures proposed. Another approach is the cloud and the fog-based architecture. One thing is certain: there is no one architecture approved for all IoT. It all depends on the size of the system, where it is used, its components and more. All this makes it even harder to ensure security and privacy.

Security and privacy by design and by default, as required also by the GDPR is a solution that should be implemented regardless of the system's architecture. But with the complexity of many of these architectures have, ensuring privacy in all layers seems to be difficult. However, the principle of "by design and by default" speaks most of all to large systems. This is due to the fact that it requires for security to be implemented from the early stages of the design. In many situations we see systems up and running without any privacy or security considerations. Only once the system is tested and properly functional starts the work towards security and privacy. This approach has many downsides and is strongly discouraged by the GDPR. It is considered that precisely by embedding these aspects from the start and through every layer and component the system will have a robust and reliable privacy and security framework.

Most threats and vulnerabilities in IoT revolve around the main domains of these systems: the architecture, the applications, the communication and of course, the data itself. In terms of architecture most threats revolve around authorization and authentication. Who has the right to access certain resources and how to give access rights so that misuse cannot happen? With security of communication the most common threats are man-in-the-middle attacks and eavesdropping, whereas when trying to ensure data security we'll see issues like trust and privacy arising. For example, one concern is ensuring two neighboring nodes will not have access to the same data unless access is specifically granted.

IV. Solutions for Privacy in IoT

Devices in an IoT system communicate large amounts of data in order to properly function and offer an overall good user experience. This communication can include users' personal data without them even being aware.

Paper [1] tackles the challenges around privacy in IoT, more specifically end-to-end privacy across the three layers of these systems. The solution proposed uses privacy preservation techniques with multiple Internet of Things cloud data stores.

Article [2] takes things further, by discussing the issue of user controllability on device privacy. Their solution, while not directly addressing the GDPR, aims to solve an issue with see over and over again within the regulation: giving control to the users, allowing them to decide exactly which data is shared on each device. Also, in the area of technologies that may lead to a loss of privacy is paper [3]. Here we see the issue of location-based services, which are used more and more in devices. The algorithm proposed by the authors' aims to lower the chances of the user's location being revealed to unwanted parties.

The authors of [7] discuss privacy in a cloud-based Internet of Things. Like paper [2], this paper does not directly address the GDPR. However, it addresses issues that need to be covered once the regulation will be enforced, such as privacy concerns with cloud-based IoT, protecting data before it is uploaded to the cloud, allowing the users to make decisions regarding their data. Their solution also provides transparency for all activities requiring data privacy and it also sustains the idea of implemented privacy as a core functionality - otherwise said, privacy by design.

Paper [9] provides a survey and analysis of the security requirements of IoT. The authors highlight the need for security by design and propose an embedded framework for security as a feature of co-design methodology.

Paper [15] discusses privacy in IoT and blockchain from a legal perspective, dealing precisely with the GDPR. The article tackles some of the risks associated with IoT such as the identification of personal information - the way in which devices and data are linked in an IoT highly increase the chances of personal data to be linked to an individual without their consent. In the same manner, the risk of profiling activities is increased. Profiling is a heavily regulated practice in the GDPR, restricted in many circumstances. The author considers that especially in smart houses, or smart cities the profiling is likely to happen, disguised as activities meant to offer the user better services. Geolocation is another risk not only in IoT, but with all smart devices that use GPS for various services. It is a practice not always understood by the average user and one that can disclose a lot of personal information. Loss of data during processing is another concern brought into attention by the author. This is especially important in the context of the GDPR as it can put the manufacturer in the position to be liable for a data breach.

The approach considered correct by the author of paper [15] is to emphasize that privacy is not security. Many tend to put the two in the same category and even the GDPR can have conflicting terminology in some of its articles. Attentively separating the two, giving both high importance when building an IoT can save this type of system, making it not only an amazing technology but also legally fit for use.

The authors of paper [16] underline a fact that is worrying not only from a GDPR perspective: companies within the IoT sector rely on personal data to deliver and monetize their services. The authors focus their paper around the value of privacy in the Internet of Things. They describe privacy in a quantitative manner, using a game theory concept - value of information. The article also presents a tool called PrivacyGate, a tool for Android devices meant to study privacy in IoT transactions.

Paper [17] considers the privacy implications in the integration of the Internet of Things and cloud computing. The premises are the use of cloud computing to store and process all the data transmitted between devices in an IoT system. This can lead to personal data of the users being collected by third parties without their consent. It is thus imperative to provide a solution for privacy. The architecture proposed by the authors proposes the protection of the data generated by IoT devices without the use of a secure transport layer protocol in order to minimize the resources used, while integrating privacy in the IoT and cloud communication.

Another interesting approach can be found in [18]. The authors start from the fact that excessive data collection in IoT can lead to data breaches. They propose a scheme that aims to minimize the amount of information exchanged by applying differential privacy. Furthermore, the authors use a

Stackelberg game to determine the amount of noise insertion in this type of privacy.

Paper [19] brings into attention the issue of Smart Homes, by proposing a framework meant to preserve privacy in these environments. Their solutions focus on both privacy and security, using symmetric encryption with a secret key generated by chaotic systems. The authors also use message authentication to ensure integrity and authenticity. Nonetheless, the solution also focuses on efficiency and memory cost, which is a crucial aspect for IoT systems. It is a solution that could very well satisfy the requirements of the GDPR of both privacy and security by design and by default.

An approach that deals with both privacy and access control can be seen in paper [20]. Here, the authors use classification of data to ensure access control and through it, privacy. Paper [21] looks at things from a different perspective by discussing trust in Social IoT.

Paper [22] starts from the premises of possible privacy violations stemming from the way in which data can be processed in IoT without consent. The article addresses directly one of the most pressing matters when working with IoT in the GDPR era. The authors propose a solution that addresses this risk, with the purposes of giving individuals control over their data.

In article [25] we see how IoT can be used for eHealth technologies. The authors discuss the challenges in the area of privacy and security, providing numerous recommendations to address risks, to help improve future implementations.

The authors of article [23] raise awareness on the economic and social implications of the value of information and cost of privacy in the Internet of Things, while in paper [24] we see a survey on IoT that comprises architecture, technologies, security and privacy. Other surveys discussing privacy and security issues in IoT can be found in papers [4-6] and [10].

V. What Is Next for IoT

The solutions presented in Section IV are only some of the most recent works in the area of privacy and security for the Internet of Things. Do they cover all the requirements of the GDPR? Some might, but not all. There has been a lot of panic around this new law among the IoT enthusiasts, researchers and business owners alike. Many have said that the GDPR might halt the advances made by technology, not only in IoT but also in other technologies like machine learning and blockchain.

To turn the GDPR into an opportunity, we need to look at those requirements that speak directly to the IoT. Privacy and security are not the same, but both are needed "by design and by default". The requirements of the regulation apply to all systems, IoT included and we will discuss them in the following paragraphs.

Minimizing data, using only what is strictly necessary becomes more and more difficult as the size and the complexity of a system increases. In the context of big data and inter-communication in the Internet of Things, minimizing data feels like a daunting task but also very useful, as it can prevent many of the privacy and security risks associated with processing more data than needed.

Pseudonymization, a term that can be found in the GDPR refers to securing data, rendering it useless, unless the user has direct access rights. Encryption is probably the most used method for pseudonymization, but other methods such as steganography can be just as useful. Any encryption method can be used as long as data is well protected. Of course, one can argue that the newest methods might provide better, more robust protection. However, it has been proven that this is not necessarily true, as the way in which methods are applied, the context and the system itself are also factors that need to be taken into consideration when choosing a security method. Anonymization is another term discussed in the context of the GDPR and not only. Many consider that true anonymization can be hard to achieve, and it is also impractical as it would make rectification or modification in personal data hard if not impossible.

Access control has been previously explained when discussing privacy and security by design, so we won't go into more detail. Transparency, another important aspect in the GDPR is crucial in complex systems like IoT. The user needs to know at all times what happens to his personal data, why and how it is processed. We saw in Section IV that some research has been made in the direction of increasing transparency in IoT. However, considering what an important requirement this is, there is still room for improvement.

In a way, consent goes hand in hand with transparency. If you need consent for all data processing activities and it needs to be informed, transparency of processing activities comes naturally. Consent is probably something in which service providers and business representatives will be more interested in than researchers. However, providing better and more comprehensive solutions for transparency in IoT remains a challenge for researchers as well.

Monitoring refers to a wide variety of activities. Constantly monitoring data, especially in IoT where there are a lot of communications in between devices may not be easy, but it would greatly reduce the risk of attacks or data breaches.

Finally, the real purpose of the GDPR is switching control of personal data from service providers and developers to the user. While the regulation puts an emphasis on the rights on the individual, this has implications on a technical level as well. As proven throughout this survey, there aren't many solutions that take into consideration who has the power of the data once a someone starts using devices in an IoT system.

VI. IoT Special Cases – Military Technology

The applications of the Internet of Things go well beyond smart devices, smart homes and more. In recent years, more and more people start seeing the benefits in using intelligent adaptive systems to improve modern warfare and the defense and public safety sectors in general.

Paper [27] presents a review on ways in which the Internet of Things is used in defense and public safety. The review focuses, among other things, on how IoT can be used to reduce costs while increasing efficiency, but also to ensure better survivability to people such as first responders. The authors also discuss the shortcomings these systems still have and aim to find possible solutions.

Similarly, paper [29] focuses on the Internet of Things for defense. Here the author analyzes the changes that the commercialization of the IoT paradigm can bring for the defense sector and also highlight the fact that IoT started precisely in defense and with its current use in the private, commercial sectors, new technologies have been added, that can help improve the defense sector.

Furthermore, the Chief Information Officer of the United States Department of Defense released in December 2016 some policy recommendations for the Internet of Things [28]. The document highlights the weaknesses of such systems and the vulnerabilities they introduce, while suggesting solutions to address these issues in order to benefit from all the advantages of IoT.

So, are these military IoT systems affected by the GDPR and other similar regulations in the same manner commercial ones are? Yes and no. For one, the GDPR is focused a lot on individual rights, which is something to consider regardless of where a certain technology is applied. However, there are certain limitations involving public sectors, especially when it comes to defense, public safety and governments. However, due to the sensitive nature of defense applications, having the best security and access controls measures in place is crucial. As a result, applying GDPR principles like "security and privacy by design and by default", ensuring record control, and a limitation of usage to only what is strictly necessary can bring only improvements.

VII. Privacy Regulations Worldwide

The European General Data Protection Regulation has risen the alarm that a change needs to happen worldwide, and that the privacy of each individual in the online world must be of top priority. Its seeming severity stems from the fact that it applies to anyone, regardless of their location, if they process data of EU citizens. However, in terms of strictness of provisions, the GDPR is not a premiere worldwide.

DLA Piper [32] published a comprehensive map of the data protection laws of the world, which can be viewed in Fig. 2. From red - as the most comprehensive privacy laws, to green - as very light provisions, we can see there are a lot of regulations around data protection worldwide.

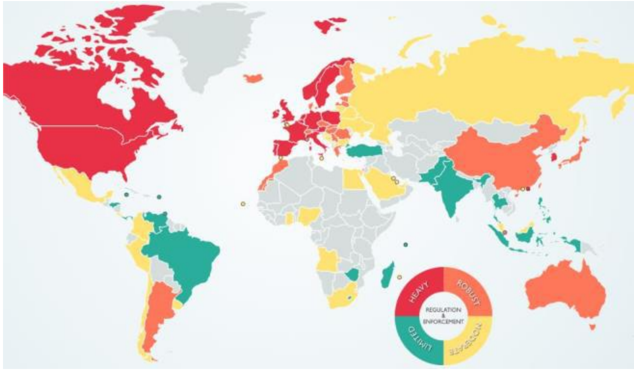

Figure 2. Privacy Regulations Worldwide [32]

The Payment Services Directive (PSD2) and the Children's Online Privacy Act (COPPA) are two of the most known such laws. COPPA is a United States federal law that requires consent for processing any personal data of children aged 13 or less. PSD2 on the other hand is a legislation aimed at banks, limiting them from taking money from someone's account without consent for example.

A regulation similar to the GDPR not only in provisions, but also in the international outreach is the Personal Data Protection Act in Singapore. The main difference between the PDPA and the GDPR is that the Singaporean law does not apply to the public sector. Another difference that impacts both the citizens of Singapore and the private companies is with regards to consent. With the GDPR, consent should never be implied. If a user gives consent for certain data processing operations, the company should not use the data for anything else, without reacquiring consent. As previously explained, this is one of the concerns surrounding the use of IoT, where one data processing operation may lead to another, and another, and so on, making it very difficult to request the user's consent for each such step. In contrast, the PDPA implies that once someone gives their consent to a company for a certain type of data processing, that company can process the given data in any way they want. Sure, Singaporean IoT enthusiasts may feel relieved to hear this. But is it really in the best interest of the users?

Canada has a total of 28 statutes regarding confidentiality and privacy. The best known is PIPEDA - Personal Information Protection and Electronic Documents Act, aimed at the private sector.

The United States have around 20 statues and laws governing data privacy. However, EU representatives still believe American regulations are not even close to the GDPR, and the EU-US Privacy Shield has more critics than fans. The Shield is in fact a self-certification program, and many of its critics argue that there is no actual evidence that a certified company is indeed GDPR compliant.

Recently, California passed the new Consumer Privacy Act, a law that might finally bring the changes to the US legislation the EU has been hoping for. The CPPA was subject to intense negotiations, but some of the events that took place this year, like the Cambridge Analytica incident, convinced the majority to vote in favor of the new law. Through it, a series of new rights are established for California's citizens, like the right to be informed or the right to have their data deleted upon request. Another significant change with regards to any other US privacy law is the broadening of the definition of personal data. Similar to the GDPR, CPPA includes biometric data, browsing history, geolocation, and more, in this definition. For researchers and especially those working in the field of Internet of Things, challenges arising from the CPPA will be similar to those arising from the GDPR. All in all, a globalization of data privacy laws is more than welcome, as it will have everyone working towards a common goal. With globalization happening in so many other ways, and the internet connecting virtually any and every country on the globe, it is only natural to expect to have the same laws governing personal data.

On the opposite side are the countries with more moderate privacy regulations. For example, China, a country that does have considerable privacy laws, as can be observed in Fig. 2, does not have one law dedicated specifically to this matter. Instead, privacy provisions can be found in several other regulations. The newest is the law of cybersecurity, enforced in June 2017, which is also called "The General Data Protection Law".

Finally, Russia, a country with only a moderate level of privacy laws, has some provisions regarding data protection in its Constitution. For example, any form of consent is considered valid as long as the data processor can prove they have it. Sensitive and biometric data are special cases where consent should be specific.

The conclusion remains the same: the world is in need of uniform privacy regulations in order to advance with its research in a manner that benefits both researchers and end users alike.

VIII. Conclusions

Until now, it was rare to consider when developing new technologies any legal aspects surrounding the proposed solution. The EU General Data Protection Regulation and the rapid advances in technology bring forth the need to address the rights and the privacy of the individual as a fundamental issue. Some solutions already exist that put privacy first. However, even those solutions leave room for improvement, as they do not address all the legal requirements of the GDPR. Many see this new regulation as a possible impediment in the advances of technologies like IoT or machine learning. However, we can also see many positive changes in regulations worldwide. Countries that had little to no privacy regulations, are now starting to see the importance of such laws. Everything seems to underline the importance of having unified privacy regulations. These would not only help the citizens of countries worldwide, but it would also help research advance in a much more uniform and steady manner.

We believe that the GDPR is more of an opportunity to improve security and privacy, to raise awareness on the importance of these aspects and to develop new methods that are robust, efficient and easy to use both for scientists and for the everyday user.

References

[1] Prem Prakash Jayaraman, Xuechao Yang, Ali Yavari, Dimitrios Georgakopoulos, and Xun Yi, “Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation,” *Future Generation Computer Systems*, vol. 76, pp. 540-549, Nov. 2017. doi:10.1016/j.future.2017.03.001

[2] Waqar Asif, Muttukrishnan Rajarajan, and Marios Lestas, “Increasing user controllability on device specific privacy in the Internet of Things,” *Computer Communications*, vol. 116, pp. 200-211, Jan. 2018. doi:10.1016/j.comcom.2017.11.009

[3] Gang Sun, V. Chang, Muthu Ramachandran, Zhili Sun, Gangmin Li, Hongfang Yu, and D. Liao, “Efficient location privacy algorithm for Internet of Things (IoT) services and applications,” *Journal of Network and Computer Applications*, vol. 89, pp. 3-13, Jul. 2017. doi:10.1016/j.jnca.2016.10.011

[4] Rolf H. Weber, “Internet of things: Privacy issues revisited,” *Computer Law & Security Review*, vol. 31, no. 5, pp. 618-627, Oct. 2015. doi:10.1016/j.clsr.2015.07.002

[5] Arbia Riahi Sfar, E. Natalizio, Yacine Challal, and Zied Chtourou, “A roadmap for security challenges in the Internet of Things,” *Digital Communications and Networks*, vol. 4, no. 2, pp. 118-137, Apr. 2018. doi:10.1016/j.dcan.2017.04.003

[6] F. A. Alaba, M. Othman, I. A. Targio Hashem, and F. Alotaibi, “Internet of Things security: A survey,” *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, Jun. 2017. doi:10.1016/j.jnca.2017.04.002

[7] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, “A comprehensive approach to privacy in the cloud-based Internet of Things,” *Future Generation Computer Systems*, vol. 56, pp. 701-718, Mar. 2016. doi:10.1016/j.future.2015.09.016

[8] EU General Data Protection Regulation text, Available online at: http://www.privacy-regulation.eu/en/index.htm

[9] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, “Proposed embedded security framework for Internet of Things (IoT),” in *Proc. 2nd Int. Conf. on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE*, Chennai, India, 2011, pp. 1-5. doi:10.1109/WIRELESSVITAE.2011.5940923

[10] E. Borgia, “The Internet of Things vision: Key features, applications and open issues,” *Computer Communication*, vol. 54, pp. 1-31, Dec. 2014. doi:10.1016/j.comcom.2014.09.008

[11] A. Majeed, “Internet of Things (IoT): A verification framework,” in *IEEE 7th Annual Computing and Communication Workshop and Conf.*, Las Vegas, NV, USA, Jan. 2017, pp. 1-3. doi:10.1109/CCWC.2017.7868461

[12] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, “SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways,” *Procedia Computer Science*, vol. 52, pp. 452-459, doi:10.1016/j.procs.2015.05.013

[13] P. Persson and O. Angelsmark, “Calvin - Merging Cloud and IoT,” *Procedia Computer Science*, vol. 52, pp. 210-217, 2015. doi: 10.1016/j.procs.2015.05.059

[14] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, “Two-phase authentication protocol for wireless sensor networks in distributed IoT applications,” in *IEEE Wireless Communications and Networking Conf., (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 2728-2733. doi:10.1109/WCNC.2014.6952860

[15] N. Fabiano, “Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard,” in *2017 IEEE Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Exeter, United Kingdom, Jun. 2017, pp. 727-734. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.112

[16] A. Mayle, N. H. Bidoki, S. Masnadi, L. Boeloeni, and D. Turgut, “Investigating the Value of Privacy within the Internet of Things,” GLOBECOM 2017 – in *2017 IEEE Global Communications Conf.*, Singapore, Dec. 2017, pp. 1-6. doi:10.1109/GLOCOM.2017.8253958

[17] L. A. B. Pacheco, E. Alchieri, and P. A. S. Barreto, “Enhancing and evaluating an architecture for privacy in the integration of Internet of Things and cloud computing,” in *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, 2017, pp. 1-8. doi:10.1109/NCA.2017.8171355

[18] K. Jung and S. Park, “Grayscale access control: Applying differential privacy to access control for Internet of Thing environment,” in *2017 Int. Conf. on Information and Communication Technology Convergence (ICTC)*, Jeju, South Korea, Oct. 2017, pp. 849-854. doi:10.1109/ICTC.2017.8190797

[19] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, “A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes,” in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844-1852, 2017. doi:10.1109/JIOT.2017.2707489

[20] N. Kaliya and M. Hussain, “Framework for privacy preservation in iot through classification and access control mechanisms,” in *Proc. 2017 2nd International Conference for Convergence in Technology (I2CT)*, Mumbai, India, 2017, pp. 430-434. doi:10.1109/I2CT.2017.8226166

[21] N. B. Truong, T.-W. Um, B. Zhou, and G. M. Lee, “From Personal Experience to Global Reputation for Trust Evaluation in the Social Internet of Things,” in *GLOBECOM 2017 - 2017 IEEE Global Communications Conf.*, Singapore, Singapore, 2017, pp. 1-7. doi:10.1109/GLOCOM.2017.8254523

[22] A. Ayadi and S. Sassi, “Privacy in the Age of Internet of Things: Challenges and Prospects,” *2016 Global Summit on Computer and Information Technology (GSCIT)*, Sousse, Tunisia, 2016, pp. 48-53. doi:10.1109/GSCIT.2016.22

[23] D. Turgut and L. Boloni, “Value of Information and Cost of Privacy in the Internet of Things,” *IEEE Communications Magazine*, vol. 55, no. 9, pp. 62-66, 2017. doi:10.1109/MCOM.2017.1600625

[24] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, Oct. 2017. doi:10.1109/JIOT.2017.2683200

[25] M. Omoogun, P. Seeam, V. Ramsurrun, X. Bellekens, and A. Seeam, “When eHealth meets the internet of things: Pervasive security and privacy challenges,” in *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)*, London, UK, Jun. 2017, pp. 1-7. doi:10.1109/CyberSecPODS.2017.8074857

[26] M. Wolf and D. Serpanos, “Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems,” in *Proc. of the IEEE*, vol. 106, no. 1, pp. 9-20, Jan. 2018. doi: 10.1109/JPROC.2017.2781198

[27] P. Fraga-Lamas, T. M. Fernandez-Carames, M. Suarez-Albela, L. Castedo, and M. Gonzalez-Lopez, “A Review on Internet of Things for Defense and Public Safety,” *Sensors*, vol. 16, 2016. doi:10.3390/s16101644

[28] United States. Department of Defense. Office of the Chief Information Officer, “DoD Policy Recommendations for the Internet of Things,” 2016. https://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet%20of%20Things%20-%20White%20Paper.pdf?ver=2017-01-26-152811-440

[29] “The Internet of Things for Defense”

[30] “What you need to know about California’s new privacy law”, Available at: https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law

[31] GLOBAL DATA PRIVACY SNAPSHOT 2018 (dla piper)

[32] DLA Piper Privacy Regulations Worldwide Map: https://www.dlapiperdataprotection.com/index.html