Applying Privacy Patterns to the Internet of Things' (IoT) Architecture

Sebastian Pape ✉ 0000-0002-0893-7856 and Kai Rannenberg,

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt, Theodor-W.-Adorno-Platz 4, 60323 Frankfurt, Germany,
{sebastian.pape, kai.rannenberg}@m-chair.de, +49-69-798-{34668, 34701}

Abstract

The concept of cloud computing relies on central large datacentres with huge amounts of computational power. The rapidly growing Internet of Things with its vast amount of data showed that this architecture produces costly, inefficient and in some cases infeasible communication. Thus, fog computing, a new architecture with distributed computational power closer to the IoT devices was developed. So far, this decentralised fog-oriented architecture has only been used for performance and resource management improvements.
We show how it could also be used for improving the users' privacy. For that purpose, we map privacy patterns to the IoT / fog computing / cloud computing architecture. Privacy patterns are software design patterns with the focus to translate "privacy-by-design" into practical advice. As a proof of concept, for each of the used privacy patterns we give an example from a smart vehicles scenario to illustrate how they could improve the users' privacy.

Keywords

Privacy by Design; Cloud Computing; Fog Computing; Internet of Things; Privacy Patterns; Autonomous Cars; Smart Vehicles

1. Introduction

With an estimated number of 50 billion ubiquitous, interconnected devices by the year 2020 the Internet of Things (IoT) is growing rapidly [9]. Since its beginning, the IoT concept is relying on a strong computing infrastructure built on cloud computing services [4]. However, new concepts and technologies to manage the huge amount of devices gain importance. The backbone evolved into a more heterogeneous concept which is known as fog (or sometimes mist or edge) computing. A literature survey by Thien and Colomo-Palacios [37] showed that the main purposes or developments of the architecture addressed six different areas: resource management, energy efficiency, offloading, data processing, performance enhancement and networking. All of these are merely performance problems.

However, privacy concerns in the IoT are not only a research topic [14], but have arrived at customers which were spied by their devices [10, 13]. Adams [1] notes that due to the nature of IoT devices and the way they collect information, their use leads to a higher risk of having information collected and shared. Often the IoT devices and sensors come together with mobile apps. Papageorgiou et al. [26] discovered in the mobile health domain that most of the apps do not follow well-known practices and guidelines and jeopardizing the privacy of millions of users. Weinberg et al. add that in the IoT environment the user faces a trade-off between convenience and privacy [39]. Moreover, Adams [1] and Walker [38] found that the regulators cannot keep up with the advances in the market, e.g. because of the speed with which data is exchanged. Apparently, privacy notices or policies could reduce the risk of disclosing personal information, but customers are increasingly frustrated with them [20, 21]. Since this discovery, not much has changed, as a recent study on IoT privacy policies shows [25].

We argue that in particular with the *General Data Protection Regulation* (*GDPR*) which has just become effective, more emphasis should be put on designing privacy-friendly services (privacy by design). Therefore, we investigate how the different characteristics within the IoT / Cloud / Fog architecture could be used to improve the users' privacy.

The remainder of this work is organized as follows. Section 2 gives a brief introduction into fog computing and describes related work, in particular about privacy in IoT environments and privacy patterns. In Section 3 suitable privacy patterns are mapped to the IoT / Cloud / Fog architecture. Section 4 gives some examples using scenarios of smart vehicles for (partially) autonomous driving. Section 5 discusses the findings and concludes this work.

2. Background and Related Work

In this section, we first briefly sketch the differences between cloud and fog computing and how they work together with IoT devices. Next, we describe work on privacy for IoT systems including relevant work on fog and cloud computing when appropriate. Since our work strongly relies on it, we also address research on privacy patterns.

2.1 Fog Computing Conceptual Model

Our description of the conceptual model for fog computing follows the NIST special publication [12]. The idea of *cloud computing* was to have central large datacentres with huge amounts of computational power. However, it has been shown that with the exponential growth of IoT devices and the amount of data they produce this architecture produces costly, inefficient and in some cases infeasible communication [42]. This is in particular true for services with low latency requirements, e.g. real-time interactions. In order to achieve minimal latency and reduce costs, a new architecture with distributed computational power closer to the IoT devices was developed – *fog computing* (cf. Fig. 1). In this architecture, a substantial amount of data processing is done in decentralised, distributed nodes and thus complementing the centralized cloud computing model when serving IoT devices. According to the NIST report [12], no clear distinction between the names *fog computing*, *edge computing*, *mist computing* or *cloudlets* exist. However, following Bonomi et al. [3] edge computing is the

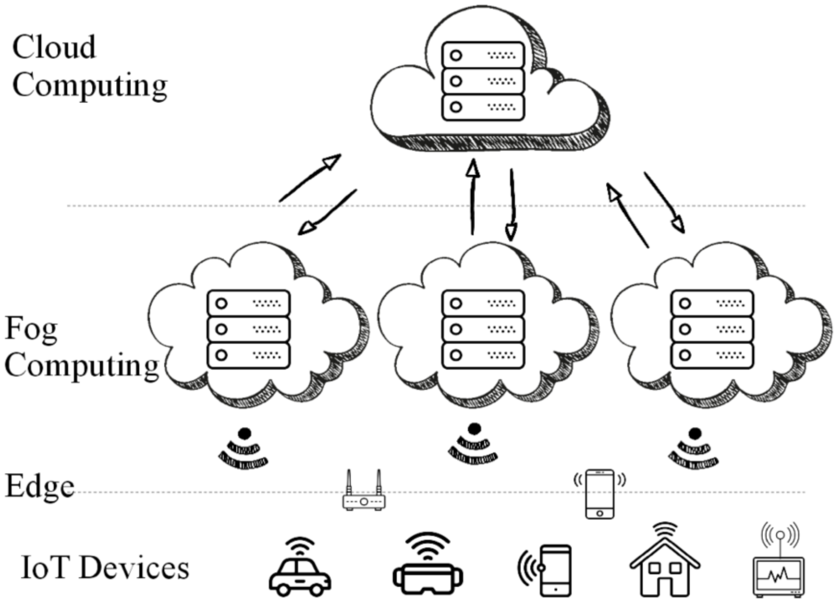

Fig 1: 3 layer service delivery model

underlying principle which allows data storage and computation at the edge of the network, and thus close to the end users.

Figure 1 shows the three layer service delivery model, where fog nodes reside between the IoT devices and the cloud service. Fog computing is not a replacement but an extension to the cloud computing architecture [2]. Naturally, the fog notes are context-aware, e.g. they know about their location. Fog nodes can be clustered vertically to allow isolation or horizontally to support federation. According to NIST [12] and Thien and Colomo-Palacios [37], fog computing has the following essential characteristics:

- *Contextual location awareness, and low latency*: Since the fog nodes are closer or often even co-located to the IoT devices, responses by these nodes can be delivered faster than by the centralised cloud computing system. Natively, the nodes know about their logical location in the context of the whole computational system.
- *Geographical distribution*: In contrast to the centralised cloud computing paradigm, fog nodes are widely distributed and geographically identifiable. This is necessary to provide services for example to vehicles. The fog computing nodes can be distributed along the track the vehicle is moving on.
- *Heterogeneity*: In contrast to cloud computing, where there is only one large node, fog computing nodes can consist of different forms and types of computing nodes.
- *Interoperability and federation*: In order to achieve seamless service distribution, the cooperation of different providers is needed.
- *Real-time interactions*: Natively, applications which involve real-time interactions make use of fog computing while traditional batch processing can still be performed in cloud computing services.
- *Scalability and agility of federated, fog-node clusters*: New clusters of fog computing nodes can easily be added or existing clusters can be extended.
- *Edge analytics*: Fog computing can support analysing data locally instead of sending it to the cloud for analysis.

2.2 Privacy in the IoT

Kumar and Patel [15] give a very high level overview of privacy concerns in the IoT. They build the four groups of privacy in the device, during communication, in storage and at processing. Analogous, Martinez-Balleste et al. [19] identify privacy threats in Smart Cities and group them into the five dimensions: identity privacy, query privacy, location privacy, footprint privacy, and owner privacy. In a next step they point to technologies that could address these threats.

Kowatsch and Maass [14] addressed privacy concerns and acceptance of IoT services from the perspective of information systems. They proposed and tested an instrument to evaluate IoT services by extending the privacy calculus model [7] and combining it with the Technology Acceptance Model [5]. Their goal was to gain insights about the users' willingness to share information to use IoT services to provide recommendations to policy makers and developers how to design privacy-aware IoT services.

Kozlov et al. [16] discuss security and privacy threats in the IoT architecture and also connect them to EU legislation. They do not mention the cloud or edge computing paradigms, but have a very similar architecture where they elaborate on privacy and security threats. One of their conclusions is that many threats are similar to those in already existing architectures. Complementarily, Lee et al. [17] focus on security issues in the fog computing supported IoT cloud and argue that its adoption introduces several unique security and privacy threats. Stojmenovic et al. [34, 35] studied issues such as security, demand response, privacy, fault tolerance in the context of fog computing. They in particular focus on man-in-the-middle attacks and sketch how to adapt a data aggregation scheme from Lu et al. [18] to address privacy issues. In their extensive work, which is focused on security threats, Ni et al. [22] also list some privacy threats along with discussing security and privacy requirements and state-of-the-art solutions in fog computing. Tayeb et al. [36] and Sadeghi et al. [30] focus on an industrial viewpoint and discuss security threats and challenges separately for all the layers. They point out that industrial systems are an attractive target since they generate, process and exchange vast amounts of security-critical and privacy-sensitive data. This way they show that security and privacy are often two sides of the same coin. Yi et al. [40] highlight privacy issues in data privacy, usage privacy, and location privacy on the new aspects of fog computing by surveying the literature.

However, only few of these works propose approaches on how to address privacy issues. Those who do, rarely make use of the specific architecture of fog computing to improve the users' privacy. Closest to our work is the work from Rahman et al. [27] who discuss and compare IoT programming frameworks in order to give some guidance to find the most suitable. For that purpose, Rahman et al. define a taxonomy to classify the architecture which makes essential architectural aspects explicit in order to compare the aspects' influence on functional properties. Among other features, privacy issues are also discussed. Naturally, the decision for a programming framework is on a different level than the application of privacy patterns in the IoT architecture. Thus, the guidance points in the same direction but towards different levels of abstraction compared with our work.

2.3 Privacy Patterns

Patterns are a useful method – often used in software design – to describe already known solutions and best practices for design problems [11]. Yoder and Baraclow were the first who developed patterns to address information security issues [41].Based on the Common Criteria [43] Schumacher identified two user-focused privacy patterns [31]. Privacy patterns can be considered to be a subset of design patterns with the focus to translate "privacy-by-design" into practical advice for software engineering [45].

The have been contributions to privacy patterns since the beginning of the two-thousands, although some of them do not include the term privacy pattern. Schümmer introduces six patterns and groups them into the two categories: blocking personal information from being transmitted from the user and filtering information sent from others to the user [32]. Romanosky et al. [29] identify three privacy patterns for web-based activity. Graf et al. [11] describe the development of User Interfaces Patterns for Privacy Enhancing Technologies (PET).

Doty and Gupta [8] note a lack of concrete guidance for implementing Privacy-by-Design. Therefore, they proposed privacy design patterns adapted from software engineering design patterns and established a site to allow a collaborative collection and development of privacy patterns [45]. The privacy patterns website aims to standardize the language for privacy-preserving technologies, to document common solutions to privacy problems and to help designers identify and address privacy concerns. In a similar manner, the Privacy Design Pattern Library Website [46] provides a pattern library for making privacy policies understandable. Both libraries [45, 46] provide a database where common patterns can be looked up and searched.

3. Mapping Privacy Patterns to Architecture Considerations

Ni et al. [22] list four aspects of information which is privacy relevant in the IoT.

- *Identity Information*: Any information that can link to a specific user, e.g. name, address, telephone number, credit card number or public-key certificate.
- *Data*: Various sensitive information, such as a user's preferences, occupation, health status and political inclination.
- *Usage Information*: Usage pattern with which a user utilizes the services offered, e.g. the readings of a smart meter.
- *Location Information*: With location information an attacker is able to identify a user's trajectory, identity, points of interest. It seems that location privacy is a kind of privacy that we have to sacrifice to use online services, such as navigation and location-based services.

In the following subsections, we first introduce a privacy pattern (if possible) based on the PrivacyPatterns Website [45] and then show how it can be applied to the IoT with the cloud / fog computing architecture behind. We only discuss privacy patterns where the characteristics of the specific IoT / cloud computing / fog computing architecture can be exploited.

3.1 Personal Data Store

The main idea of the "Personal Data Store" privacy pattern is that users keep control on their personal data and store it on a personal device. The pattern can only be applied for data produced by the user and not for data produced by a third party. The pattern aims to prevent the user to lose control over their data when submitting it to a server operated by a third party or storing it there.

For IoT devices this could mean that identity information or data is stored locally and (if possible) computations are also done locally (see Fig. 2). If the IoT device is too small and has too little computational power, a workaround would be to make use of the user's mobile phone. Many devices connect to the Internet via the user's phone or they use the user's phone with an app as interface to control the device. Often the data is stored in the cloud and accessed by the phone's app. If this cannot be changed, a possibility would be that the IoT device encrypts the data and the decryption key is on the mobile phone while the cloud respectively fog nodes do not have the decryption key. Nowadays, many mobile phones offer a decent level of computational power.

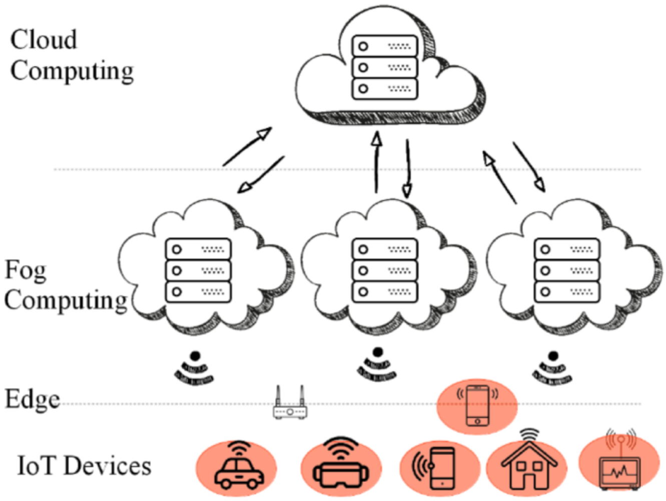

Fig. 2: Personal Data Store at IoT Devices or the Mobile Phone

3.2 Data Isolation at Different Entities

The main idea of the “Data Isolation at Different Entities” privacy pattern is that if data or usage information is distributed among several entities, all of the entities can only see a part of the data. This improves the users’ privacy since it gets harder to profile him/her.

In the determined architecture, the fog nodes or clusters would be an excellent layer to enforce isolation. As already stated, if fog nodes are clustered vertically, each cluster can belong to a different organisation respectively provider. Note that this privacy pattern does not prevent collusion attacks. Several providers could exchange information to profile a single user or a group of users. Since the unauthorized exchange of data does not need to use the IoT infrastructure, and thus cannot be controlled, the easiest way to prevent it are legal arrangements. This pattern can be easily combined with the following patterns “Decoupling Content and Location Visibility”, “Added Noise Measurement Obfuscation” and “Data Aggregation”.

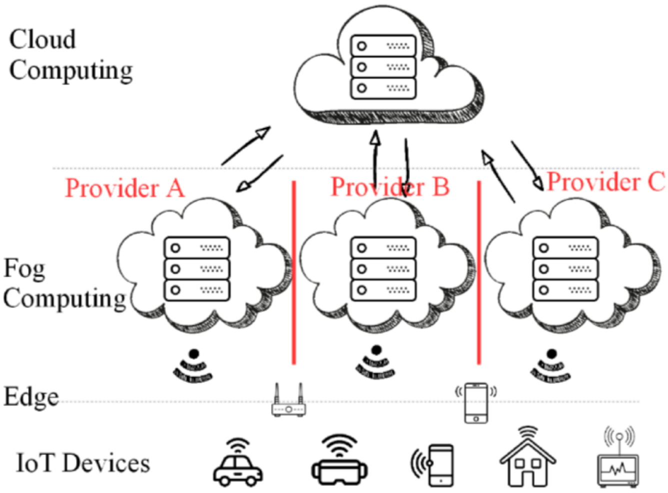

Fig. 3: Data Isolation at Different Entities

3.3 Decoupling Content and Location Information Visibility

Users often share content in socially oriented services. Since many consumer devices, e.g. mobile phones, have location data available, applications may attach location information when uploading data. However, in fog computing environments it is difficult to protect the users’ locations as users normally access the services provided by the nearest fog node. This node can then assume the user is nearby, and thus infer about the users’ location [22]. On the other hand, it would be possible that each fog node can specifically monitor if a user is transmitting location information and then either make the user aware or remove this information (see Fig. 4).

Additionally, if users access the same service at multiple fog nodes their movement can be disclosed. This can be countered by vertically clustering the fog nodes as already discussed in the previous subsection.

3.4 Added Noise Measurement Obfuscation

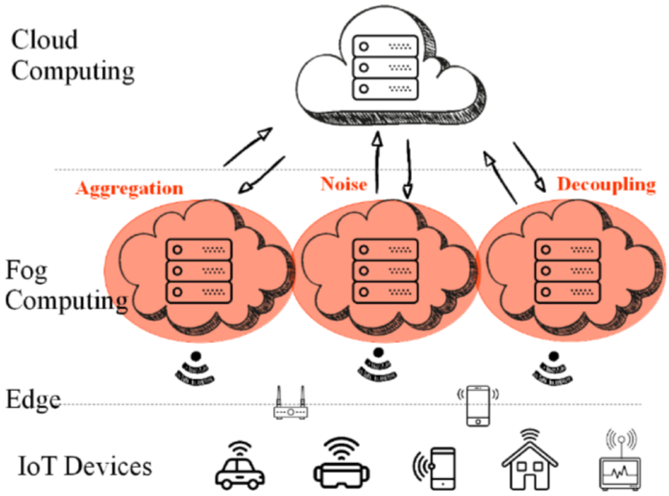

Fig. 4: Decoupling, Noise Adding and Aggregation of Data at the Fog Nodes

If users repeatedly use a resource over time, detailed measurement may reveal further information about the users such as personal habits. This privacy pattern suggest to add some noise to the measurements which cancel itself in the long term.

In this case the fog nodes could add the noise if run by a provider the user trusts, so that the cloud service provider only gets the noisy data (see Fig. 4). Users who do not trust the fog computing provider, could do the same on their mobile phone if the IoT device connects through it to the fog or the cloud computing service. However, the implementation depends a lot on what usage information it is and for what purpose it is collected. A provider probably wouldn't allow the users to add noise by themselves if the information is used for billing purposes. Additionally, a tradeoff between the usefulness of the data and the protection of the user's privacy is required. The more noise is added, the less useful the data is, but the better the user's privacy is protected.

3.5 Aggregation of Data

Analogous to the previous privacy pattern, where noise was added, another possibility to prevent the leakage of further information is the aggregation of data. For example the usage information of multiple users or the usage information of a single user aggregated over time.

Analogous to the adding of noise, the aggregation can either be done by a trustworthy provider or (in the case of aggregation over time) by the users (see Fig. 4). The same restrictions and considerations apply. However, depending on the purpose, the aggregation can be done with homomorphic encryption as described in the next subsection.

3.6 Aggregation Gateway

The use case for the "Aggregation Gateway" privacy pattern is when a service provider needs a continuous measurement and adding noise is not acceptable. This problem can be solved by using homomorphic encryption (e.g. Paillier [24]) and a trusted third party aggregating the measurements of multiple users.

Each measurement is encrypted by the IoT device or the user's mobile phone. The key is shared between the fog node and the IoT devices, e.g. by making use of Shamir's Secret Sharing Scheme [33]. The encrypted measurements from a group of users are transmitted to the cloud computing provider. Since the data passes through a fog computing node, which may have the decryption key, an additional encryption, e.g. transport layer security (TLS) [6] needs to be applied. Since the measurements have been encrypted with a homomorphic encryption system, the cloud is able to operate on the data and, e.g. can aggregate it, without being able to access the data in clear. The result of the computation, e.g. the aggregation, can then be sent to the fog node. With the previously shared secret, the fog node can decrypt the result and access it in clear without knowing about the individual values of the different users respectively devices (see Fig. 5). It is worth to mention that homomorphic encryption in general has additional computational costs, but the aggregation operation when applying this privacy pattern to the IoT architecture is located at the party with the most computational power. For a state-of-the-art scheme, we refer the reader to recent work from Okay and Ozdemir [23].

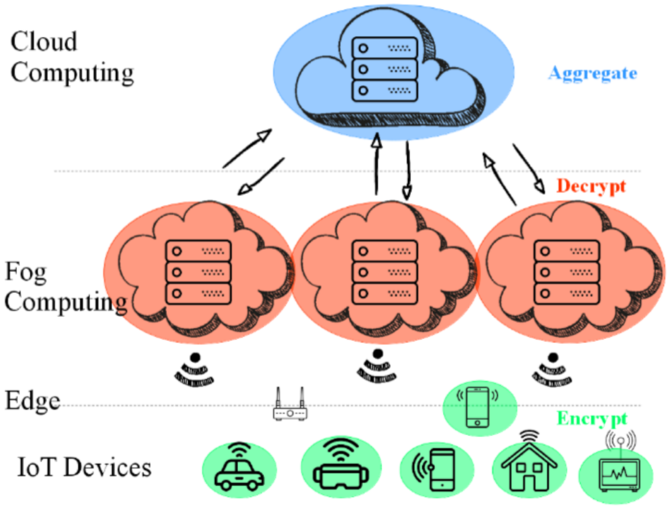

Fig. 5: Aggregation Gateway

3.7 Single Point of Contact

With distributed storage, a specialised privacy management becomes necessary, the "Single Point of Contact". The Single Point of Contact should be able to issue security tokens, authenticate local domain users as an Identity Service Provider, certify attributes as an Attribute Provider, and accept external claims as a Relying Party.

The cloud computing service can manage and coordinate the storage on different fog nodes by providing the services described above (see Fig. 6).

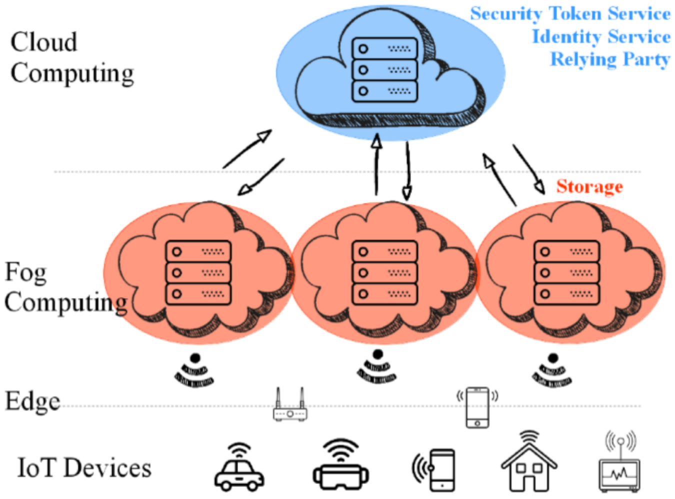

Fig. 6: Single Point of Contact

4. Evaluation of the Patterns by Applying the Privacy Patterns in the Smart Vehicles Scenario

In order to demonstrate the applicability of privacy patterns, we also show how they could be applied in a typical IoT / Fog Computing scenario. Thien and Colomo-Palacios [37] found five relevant scenarios in the literature survey about fog computing: healthcare, smart grid, smart vehicles, urgent computing (e.g. disaster support) and augmented reality. For all those scenarios, one can easily come up with a connection to IoT (sensors). In order to have one coherent scenario for all seven patterns, we chose smart vehicles to demonstrate how the privacy pattern can be applied in practise. For that purpose, we build on former work from Rannenberg [28] which investigates privacy issues in smart vehicles, especially in relation to autonomous driving. We briefly sketch the scenario in the next subsection before we can apply the privacy patterns.

4.1 The Smart Vehicles Scenario

Smart vehicles describes the automation of vehicles to support the driver and often involves the use of artificial intelligence. The support of the driver ranges from warnings through driving assistance, automation of some tasks to fully autonomous driving. For a systematic evaluation, the standard J3016 from SAE provides six levels with a detailed description of each automation level [44]. Rannenberg [28] notes that an autonomous car relies much more on interaction with the outside world than a human-driven car. This raises privacy concerns and motivates Rannenberg to analyse data flows and corresponding privacy impact. For that purpose, Rannenberg defines four use cases. The first two of them are sufficient to apply the privacy patterns discussed in Section 3.

Use Case 1: Interstate Pilot Using Driver for Extended Availability

The driving robot takes over the driving task, but only on interstates or interstate-like expressways. During autonomous journeys, drivers become passengers who can take their hands off the steering wheel and feet off the pedals and pursue other activities. The driving robot coordinates a safe handover to the driver and may even stop the car at a safe place if needed. We assume for our application of the privacy patterns that there is a fog computing infrastructure along the interstate.

Use Case 2: Autonomous Valet Parking

The driving robot parks the vehicle at a nearby or remote location after the users have exited and cargo has been unloaded. The driving robot drives the vehicle from the parking location to a desired destination. The driving robot re-parks the vehicle. The driver saves the time of finding a parking spot as well as of walking to/from a remote parking spot. In addition, access to the vehicle is eased (spatially and temporally). Additional parking space is used more efficiently and search for parking is arranged more efficiently. We assume for our application of the privacy patterns that there is a fog node at each parking location.

4.2 Application of the Privacy Patterns

For each of the privacy patterns discussed in Section 3, we show how they would be applied to the scenario discussed above for a more privacy friendly design of services.

Personal Data Store

The idea of the personal data store was that information is not stored in a central database but under the control of the user. Rannenberg already argues that for "data stored in a car are under the sole control of the car's owner or driver, [...] determining responsibility for these data may be relatively easy" [28, p.503]. This holds for several of the scenarios for smart vehicles and is in line with the privacy pattern of "Personal Data Storage".

In Use Case 2, traffic control centres or other entities involved in the choice of parking spaces should not ask the drivers or passengers for all kinds of priorities for a parking space or route, but instead give some options, so that the user or a local system assisting the user, can choose. This reduces the risk of a centralized processing of users' attitudes with regards to prices and locational preferences [28, p. 513].

Data Isolation at Different Entities

The idea of data isolation at different entities was to avoid building full profiles on the user and restrict each entity to only a part of the data. In Use Case 1, with different fog clusters along the interstate, the route of the vehicle, respectively user cannot be tracked that easily – if the fog clusters belong to different entities. In Use Case 2, the driver might have different preferences and habits at different locations. By isolating this data, building profiles is made more difficult.

Decoupling Content and Location Information Visibility

The idea of decoupling content and location information visibility was to avoid that one entity learns characteristics about the user along with his or her location. In Use Case 1, the manufacturer of the car might be interested in some usage statistics of the car. However, there is no need that the manufacturer learns the location information. In Use Case 2, the location cannot be hidden, thus the aim would be a minimisation of all other data collected at the fog responsible for coordinating the parking.

Added-noise Measurement Obfuscation

The idea added-noise measurement obfuscation was to hide certain characteristics by blurring the data. In Use Case 1, traffic and congestion analysis does not need to identify individual cars or even drivers. For that purpose it can be helpful to add noise to the data in order to hide certain characteristics of the car, e.g. maximum acceleration, which might lead to an identification of the car and thus reduce set of possible cars and respectively drivers and owners. In Use Case 2, the exact location of the car might be blurred when sending requests for free parking spaces.

Aggregation of Data

The idea of data aggregation is to not allow a certain entity to see single data. Analogous to the previous application in Use Case 1, in order to hinder the identifiability of individual cars, for traffic and congestion analysis it may be sufficient to work with aggregated values.

Aggregation Gateway

An aggregation gateway ensures the aggregation of data to not allow certain entities to still do their task but withou getting individuals' data. An application of this privacy pattern would be the emission of the cars in Use Case 1. If we assume that each car can report about its emission, their emission values could be aggregated by a central authority. If all cars within an area form a group, the aggregation could give some indication about the air quality in that area.

Single Point of Contact

The Single Point of Contact orchestrates distributed service providers. In Use Case 1, a central authority would need to organise the different fog clusters along the interstate. The central authority could issue security tokens, authenticate local domain users and provide payment services for the users make use of paid services.

5. Conclusion and Future Work

We applied seven privacy patterns to the IoT / Cloud Computing / Fog Computing architecture. By applying them to use cases from the smart vehicle scenario, we could demonstrate that they are applicable to real world scenarios. If used in the described manner, all of the privacy patterns can be used to improve the users' privacy. However, it is noteworthy to mention that not all of the patterns can be applied in every case. In particular, if certain properties of fog computing are desired, e.g. a low latency, this might prevent additional overhead caused by encryption or layers or redirection.

Additionally, with the lack of sufficient security protection causing IoT devices to be vulnerable to be hacked, broken or stolen [40], a general question arises. Is the data more secure if it is stored at the IoT nodes or at a central database of the cloud? To address this question one must make assumptions about possible and the most dangerous attackers in each case and in particular about the trustworthiness of the cloud and fog service providers. A general guideline is that the cloud and fog computing nodes will be more secure than the IoT nodes, so it will be less likely that they will be successfully attacked. On the other hand, the fog and cloud computing nodes are run by a third party with its own interests. Therefore, the question arises how trustworthy this party is.

In the same manner, it is not always clear, if users are able to control their data more easily if it is stored closer to them, but distributed (fog nodes) or if it is stored further away, but therefore centralised (cloud node).

We appreciate further research on the security and privacy relating to the storage of the data, the application of further privacy patterns to the IoT / Cloud Computing / Fog Computing architecture and thinking of further examples, in particular if there is a trade-off between performance and privacy.

References

- [1] Mackenzie Adams: Big Data and Individual Privacy in the Age of the Internet of Things. Technology Innovation Management Review 7, no. 4, 2017, p. 12-24.

- [2] Kay Bierzynski, Antonio Escobar, Matthias Eberl: Cloud, fog and edge: Cooperation for the future? FMEC 2017: 62-67

- [3] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli: Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing, p. 13-16. ACM, 2012.

- [4] Alessio Botta, Walter de Donato, Valerio Persico, Antonio Pescapé: Integration of Cloud computing and Internet of Things: A survey, Future Generation Computer Systems, Volume 56, 2016, p. 684-700, ISSN 0167-739X, available from: https://doi.org/10.1016/j.future.2015.09.021.

- [5] Fred D. Davis: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13 (3), 1989, p. 319-339.

- [6] Dierks, Tim: The transport layer security (TLS) protocol version 1.2, RFC 5246, 2008.

- [7] Tamara Dinev and Paul Hart: An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 17 (1), 2006, p. 61-80.

- [8] Nick Doty, M. Gupta. "Privacy design patterns and anti-patterns." In Trustbusters Workshop at the Symposium on Usable Privacy and Security. 2013.

- [9] Dave Evans: The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Online White Paper, April 2011, available from: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

- [10] Bree Fowler: Gifts That Snoop? The Internet of Things Is Wrapped in Privacy Concerns, Consumer Reports, December 2017, available from: https://www.consumerreports.org/internet-of-things/gifts-that-snoop-internet-of-things-privacy-concerns/

- [11] Cornelia Graf, Peter Wolkerstorfer, Arjan Geven, and Manfred Tscheligi. "A pattern collection for privacy enhancing technology." In The 2nd Int. Conf. on Pervasive Patterns and Applications (PATTERNS 2010), pp. 21-26. 2010.

- [12] Michaela Iorga, Nedim Goren, Larry Feldman, Robert Barton, Michael Martin, Charif Mahmoudi: Fog Computing Conceptual Model, NIST Special Publication 500-325, March 2018, DOI: 10.6028/NIST.SP.500-325 available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf

- [13] Kashmir Hill, Surya Mattu: The House That Spied on Me, Gizmodo, February 2018, available from: https://gizmodo.com/the-house-that-spied-on-me-1822429852

- [14] Tobias Kowatsch, Tobias Wolfgang Maass: Privacy Concerns and Acceptance of IoT Services. In The Internet of Things 2012 : New Horizons. Halifax, UK : IERC - Internet of Things European Research Cluster, 2012, S. 176-187.

- [15] J. Sathish Kumar and Dhiren R. Patel: A survey on internet of things: Security and privacy issues. International Journal of Computer Applications 90.11, 2014

- [16] Denis Kozlov, Jari Veijalainen and Yasir Ali: 2012. Security and privacy threats in IoT architectures. In Proceedings of the 7th International Conference on Body Area Networks (BodyNets '12). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 256-262.

- [17] Kanghyo Lee, Donghyun Kim, Dongsoo Ha, Ubaidullah Rajput, and Heekuck Oh. "On security and privacy issues of fog computing supported Internet of Things environment." In Network of the Future (NOF), 2015 6th International Conference on the, pp. 1-3. IEEE, 2015.

- [18] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications,” Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 9, pp. 1621–1631, Sept 2012.

- [19] Antoni Martinez-Balleste, Pablo A. Perez-Martinez and Agusti Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," in IEEE Communications Magazine, vol. 51, no. 6, pp. 136-141, June 2013.

- [20] George R. Milne, Mary J. Culnan: Strategies for reducing online privacy risks: Why consumers read (or don’t read) online privacy notices. Journal of Interactive Marketing. 2004 Jan 1;18(3):15-29.

- [21] Geroge R. Milne, Mary J. Culnan, Henry Greene: A longitudinal assessment of online privacy notice readability. Journal of Public Policy & Marketing. 2006 Sep 1;25(2):238-49.

- [22] Jianbing Ni, Kuan Zhang, Xiaodong Lin, and Xuemin Shen: Securing fog computing for internet of things applications: Challenges and solutions. IEEE Communications Surveys & Tutorials (2017).

- [23] F. Y. Okay and S. Ozdemir, "A secure data aggregation protocol for fog computing based smart grids", 2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018), Doha, 2018, pp. 1-6.

- [24] Pascal Paillier: Public-key cryptosystems based on composite degree residuosity classes. In International Conference on the Theory and Applications of Cryptographic Techniques, pp. 223-238. Springer, Berlin, Heidelberg, 1999.

- [25] Niklas Paul, Welderufael Tesfay, Dennis-Kenji Kipker, Mattea Stelter and Sebastian Pape: Assessing Privacy Policies of Internet of Things Services. In ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018, Poznan, Poland, 18-20 September, 2018, 2018

- [26] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas and C. Patsakis, "Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice," in IEEE Access, vol. 6, pp. 9390-9403, 2018.

- [27] Leila Fatmasari Rahman, Tanir Ozcelebi, and Johan J. Lukkien. "Choosing your IoT programming framework: Architectural aspects." In Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on, pp. 293-300. IEEE, 2016.

- [28] Kai Rannenberg: Opportunities and Risks Associated with Collecting and Making Usable Additional Data. Autonomous Driving. Springer, Berlin, Heidelberg, 2016. 497-517.

- [29] Sahsa Romanosky, Alessandro Acquisti, Jason Hong, Lorrie Faith Cranor, and Batya Friedman. "Privacy patterns for online interactions." In Proceedings of the 2006 conference on Pattern languages of programs, p. 12. ACM, 2006.

- [30] A.-R. Sadeghi, C. Wachsmann, M. Waidner, "Security and privacy challenges in industrial Internet of Things," Design Automation Conf. (DAC), 2015 52nd ACM/EDAC/IEEE, pp. 1-12, June 2015.

- [31] Markus Schumacher, “Security Patterns and Security Standards - With Selected Security Patterns for Anonymity and Privacy”, European Conference on Pattern Languages of Programs (EuroPLoP), 2002.

- [32] Till Schümmer, “The Public Privacy – Patterns for Filtering Personal Information in Collaborative Systems”, CHI 2004.

- [33] Adi Shamir: How to share a secret. Communications of the ACM 22, no. 11 (1979): 612-613.

- [34] Ivan Stojmenovic, Sheng Wen: The Fog Computing Paradigm: Scenarios and Security Issues. FedCSIS 2014: 1-8

- [35] Ivan Stojmenovic, Sheng Wen, Xinyi Huang, Hao Luan: An overview of Fog computing and its security issues. Concurrency and Computation: Practice and Experience 28(10): 2991-3005 (2016)

- [36] Shahab Tayeb, Shahram Latifi, and Yoohwan Kim. "A survey on IoT communication and computation frameworks: An industrial perspective." In Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual, pp. 1-6. IEEE, 2017.

- [37] An Tran Thien, Ricardo Colomo-Palacios: A Systematic Literature Review of Fog Computing (2016). Paper presented at NOKOBIT 2016, Bergen, 28-30 Nov. NOKOBIT, vol. 24, no. 1, Bibsys Open Journal Systems, ISSN 1894-7719

- [38] Kristen L. Walker: Surrendering information through the looking glass: Transparency, trust, and protection. Journal of Public Policy & Marketing 35, no. 1, 2016, p. 144-158.

- [39] Bruce D. Weinberg, George R. Milne, Yana G. Andonova, Fatima M. Hajjat: Internet of Things: Convenience vs. privacy and secrecy. Business Horizons 58, no. 6, 2015, p. 615-624.

- [40] Shanhe Yi, Zhengrui Qin, Qun Li: Security and Privacy Issues of Fog Computing: A Survey. In Wireless Algorithms, Systems, and Applications 2015 (pp. 685–695), 2015. Springer International Publishing. Available from http://link.springer.com/chapter/10.1007/978-3-319-21837-3_67
- [41] Joseph Yoder, Jeffrey Baraclow, “Architectural Patterns for Enabling Application Security”, Pattern Languages of Programs, 1997.
- [42] A. Yousefpour, G. Ishigaki and J. P. Jue, "Fog Computing: Towards Minimizing Delay in the Internet of Things," 2017 IEEE International Conference on Edge Computing (EDGE), Honolulu, HI, 2017, pp. 17-24.
- [43] International Standards Organisation, ”Common Criteria for Information Technology Security Evaluation” http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2, 1999.
- [44] SAE, Taxonomy and Definitions for Terms Related to On-Road-Motor Vehicle Automated Deriving Systems, J3016, SAE International Standard (2014)
- [45] Privacy Patterns Website: https://privacypatterns.org/,
- [46] Privacy Design Pattern Library Website: http://www.legaltechdesign.com/communication-design/legal-design-pattern-libraries/privacy-design-pattern-library/

All websites have been last accessed on June 12th, 2018.