Masters Program in Geospatial Technologies

OBFUSCATION AND ANONYMIZATION METHODS FOR LOCATIONAL PRIVACY PROTECTION

A systematic literature review

Mitzi Araujo Vidal

Dissertation submitted in partial fulfilment of the requirements
for the Degree of *Master of Science in Geospatial Technologies*

NOVA IMS Information Management School

UNIVERSITAT JAUME·I

WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER

Obfuscation and Anonymization methods for locational privacy protection
A systematic literature review

Dissertation supervised by

Marco Painho, PhD

NOVA Information Management School,

Universidade Nova de Lisboa, Lisbon, Portugal

Co-supervised by

Christian Kray, PhD

Institute for Geoinformatics (IFGI),

Westfälische Wilhelms-Universität, Muenster, Germany

Joaquín Huerta, PhD

Institute of New Imaging Technologies,

Universitat Jaume I, Castellón, Spain

February 2019

Acknowledgements

I am grateful to the Erasmus Mundus program for the opportunity and funding to attend the course M.Sc in Geospatial Technologies. I also would like to express my sincere gratitude to the administrative personal in both of the Geoinformatics Institute and NOVA IMS to help us with the bureaucratic affairs.

I would like to thank my supervisors Professors Christian Kray, Marco Painho and Joaquín Huerta for their feedback.

I am also grateful to my classmates of MSc Geospatial Technologies for the enriched and supportive environment during this Master's course.

Finally, I would like to express my love and gratitude to my family and friends, their encouragement and support throughout this period.

Obfuscation and Anonymization methods for locational privacy protection
A systematic literature review

Abstract

The mobile technology development combined with the business model of a majority of application companies is posing a potential risk to individuals' privacy. Because the industry default practice is unrestricted data collection. Although, the data collection has virtuous usage in improve services and procedures; it also undermines user's privacy. For that reason is crucial to learn what is the privacy protection mechanism state-of-art.

Privacy protection can be pursued by passing new regulation and developing preserving mechanism. Understanding in what extent the current technology is capable to protect devices or systems is important to drive the advancements in the privacy preserving field, addressing the limits and challenges to deploy mechanism with a reasonable quality of Service-QoS level.

This research aims to display and discuss the current privacy preserving schemes, its capabilities, limitations and challenges.

Keywords

Locational Privacy

Obfuscation Techniques

Anonymization

Acronyms

PET Privacy Enhancing Techniques

LPPM location-privacy preserving mechanism

SLR Systematic Literature Review

GL Grey Literature

GDPR General Data Protection Regulation

PIPEDA Personal Information Protection and Electronic Documents Act

TA trusted authority

TTP trusted third party

CA certificate authority

QoS quality of service

CTPP collaborative trajectory privacy preserving

POIs points of interest

ACM Association for Computing Machinery

IEEE Institute of Electrical and Electronics Engineers

dblp Digital Bibliography Library Project

GPA Global Passive Adversary

LPA Local Passive Adversary

PIR Private Information Retrieval

GPS Global Positioning System

RFID Radio Frequency Identification

RS Reported server

DDoS Denial of Service

RA Registration Authority

HISP-NC Homogenous Injection for Sink Privacy with Node Compromise protection

TVM Temporal Vector Map

DPMM Dynamic Pseudonym based Multiple Mix-zones

FGCS Future Generation Computer Systems

INDEX OF TEXT

INDEX OF TABLES

INDEX OF FIGURES

Chapter 1

Introduction

The societies are facing a shift in the computational paradigm, from desktops to mobile phones, from common devices to internet of things, pushing the capabilities to a ubiquitous computing, or pervasive computing. The plethora of applications uses personalization, collects a tremendous amount of data and applies machine learning algorithms to them. The majority of this data is locational and private whose owners are not aware of their collection, transferring and analysing.

The improvement of the mobile technologies and the pervasiveness of the computing, along with increasingly more sophisticated and personalized services has become a concern to the user's privacy. This technology could be misused and applied to dataveillance. Location and trajectory are sensitive data which can disclose critical information, such as living and consumption habits, health conditions, social, sexual, religious behaviour, political views, work and home addresses (Gao et al. 2015). The localization and its historical recording, nowadays, is a means of profit for many companies. Hence many of them see the protection of the user's locational privacy as a potential danger to monetization and a challenge to their business model (Herrmann 2016).

The locational privacy is under attack not only by adversaries and criminals but also by the government and big corporations. Institutions which continuously try to gain more and more personal and intimate data from the individuals. Se-

curity breaches along with the company's business model are the current most common threats to the locational privacy. There are several privacy preserving techniques called privacy enhancing techniques PET for general personal data and locational data focused Locational Privacy Protection Mechanism LPPM that aim to provide anonymization, pseudonymization, unlinkability and unobservability (Pfitzmann et al. 2010) of the data subjects.

Two different and complementary approaches are responses to the challenges of privacy erosion: the regulatory-enable solutions and the technology-enable solutions (Bouguettaya et al. 2003)to privacy preserving mechanisms. In order to reduce the intrusions from both attackers and companies tools and solutions applied to preserve privacy have been developed which can be classified in distinct classes. The main classes of solutions according to Y. Sun et al. (2017) are Data Anonymization and Data Obfuscation while for Fang et al. (2017) are Data Anonymization, Data Perturbation (or Obfuscation) and Data Encryption. Bettini et al. (2015) add two other classes to latter author's definitions: Access Control and Privacy Preserving Data Mining.

1.1 Scope of the research

The research title ***Obfuscation and Anonymization methods*** *for* ***locational privacy*** *protection - A* ***systematic literature review*** has highlighted expressions which are key concepts to define the scope. The methods chosen and the reason for that choice, a clear definition of locational privacy and the methodological instructions and restrictions, respectively. The selected studies will account only technology-enable solutions (Bouguettaya et al. 2003) and consider the Bettini et al. (2015) classification for the Privacy preserving mechanism. Restrained to only two of the classes defined: Data Anonymization and Data Perturbation. Studies with techniques which only fell into the other categories, namely: Data Encryption, Access Control and Privacy Preserving Data Mining are out of scope. Conversely, studies with combined technologies will be selected only if any of the

techniques were classified in one of the two scope classes. If the study applies encryption in combination with data perturbation or data anonymization techniques; it will be included as a relevant study.

Instead of use the general concept of privacy which are intimately related to personal or personally identifiable information (PII) data, only the dimension related to data which has a spatial dimension will be used on this thesis. The Data transmitted in location-based applications are classified by Chunguang et al. (2015) there are of three kinds, namely: location privacy, query privacy, and identity privacy. Query privacy present two dimensions query content and query context. There are intensive work on the mobile application development on use of context to improve the user experience and performance. However, it is a double-edged sword as a potential source of background knowledge to malicious entities. Long et al. (2015) show the distinction between content-based and context-based queries. The former is well understood and documented, predominantly related to Identity Privacy and query privacy content whereby Data encryption technology is commonly applied. The latter threat presents a challenge, because locational privacy is a problem with a context-based nature, with an extensive flow of information coming from different sensors and devices, similarly to query context providing background and a priori knowledge to services.

The cryptography approach is predominantly applied to identity and query content problems, including secure/private network transportation, however is less appropriate to address the context and locational types of information. The hostile environment of the Mobile Networks requires assumptions and designs which account to untrustworthy behaviour or compromised entities in a LBS scheme. Using just cryptography between an untrusted entity is not a rational system design. The untrusted or semi-trusted Server which provide the service will have access to both context and precise locational data, therefore the cryptography approach alone present limited resources in this case.

The reason for query context exclusion from scope resides on its characteristics. Dey (2001) defines context as "any information that can be used to char-

acterise the situation of an entity that is considered relevant to the interaction between a user and an application, including the user and applications themselves". To Rosenberger et al. 2018, context is built from gathering and combine different types of information and interpret them with a higher level of abstraction to understand the situation of the users and its relation with a given application.

The majority of the data preserving mechanisms focus on unlikability and anonymity, decoupling the identity from attributes, relationships, location positions and traces, and creating pseudonyms. In most of the cases the techniques just applied identity privacy, such anonymization whereby all the locational data and its context are just striped of the actual owner identification by pseudonyms.

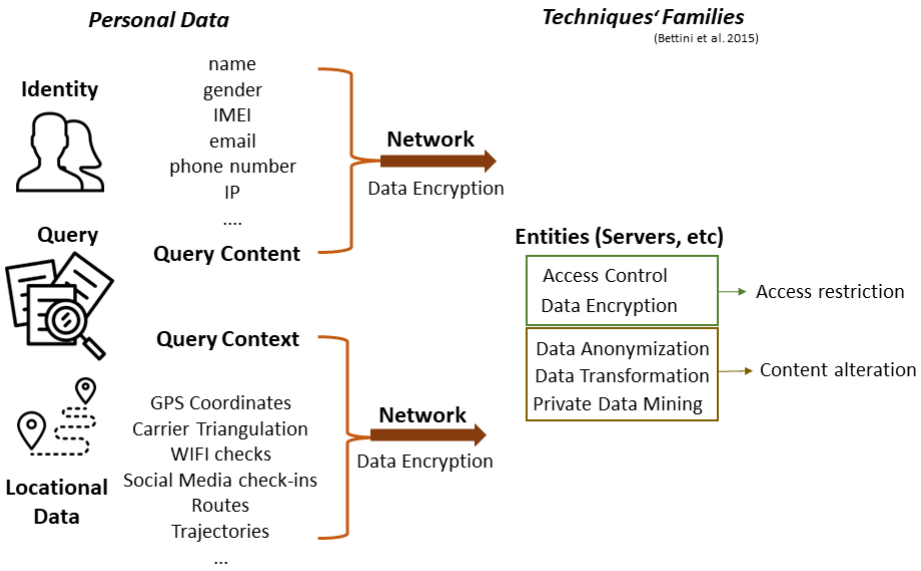

Figure 1.1: Locational Privacy in Mobile Networks

In most of the cases the techniques just applied identity privacy, such anonymization. All the locational data and its context are just striped of the actual owner identification by pseudonyms. The hostile environment of the Mobile Networks requires assumptions and design decisions because entity related to the LBS can

be either compromised or be untrustworthy. Using cryptography between an untrusted entity is not a rational system design. The untrusted or semi-trusted Server to provide the service will have access to both context and precise locational data, for this reason the cryptography approach alone present limited resources in this case.

The definition of privacy used on this thesis is a subset of what is understood by the concept of locational privacy. It is defined as "the ability to prevent other parties from learning one's current or past location" (Beresford et al. 2003).

The Vehicular Networks were removed from scope. Therefore, the studies related to vehicular networks in the pool of selected studies would implicate in more time to extract, synthesise and report the information since its nature and characteristics other than the ones from the Mobile Networks.

Another approach to classify the mobile user data problems was given by (Heurix et al. 2015) such as Identity Management, Network Traffic Anonymization and Anonymous Databases are themes out of the scope of this work. The thesis focus is on locational data and how the entities on the architecture treat and process them, the network security in not on scope, but the majority of the studies uses encryption for the data transportation. The post-treatment and private Data mining is not on scope of this research.

The privacy identity or query content privacy which has no locational data it is not scope of the thesis. For the same reason the techniques such as Data Access and private data mining are not in scope since they interrelated more to users' identity than to locational data. This work will focus exclusively on location privacy even though some query context has locational nature.

1.2 Aim and Objectives

The main objective is to provide a state-of-art of the obfuscation and anonymization technologies for preserving locational privacy. In order to achieve this aim four dimensions of the topic were distinguished and research questions were re-

spectively composed as following:

RQ1 - CONCERNS: What are the addressed concerns for applying obfuscation and anonymization techniques to protect location privacy?

RQ2 - SOLUTIONS: What are the proposed solutions in obfuscation and anonymization techniques to protect location privacy?

RQ3 - TRENDS: What are the existing research directions within obfuscation and anonymization techniques in location privacy?

RQ4 - RISK AND ARCHITECTURE: How architecture affects the solutions, service quality with the use obfuscation and anonymization techniques to protect location privacy?

1.3 What Locational Privacy actually mean?

The ubiquity of devices and steadily information acquisition place oneself's privacy in danger. The pervasiveness of sensors, the huge amount of environment, human motion and behaviour information recording is now part of daily lives. Due to the massive access to personal data, along with the possibility of tracking and profiling, individuals, institutions and governments are concerned in how to preserve privacy, but there is no consensus regarding its meaning (Birnhack 2011).

In order to protect privacy, the concept need to be clearly explained, since its definition is imprecise and have a variety of understanding in different study fields, such as: philosophy, sociology, law, political science, human rights and more recently within the information technologies.

According to Kounadi et al. (2014) location privacy can be compromised by new geospatial technologies, lenient laws regarding privacy and as by a scientist's and publisher's negligence. Three dimensions of data treatment: data acquisition, data publication and regulation. For this author privacy definition relies on the combination of the correctness and uncertainty concepts. Meaning that the level of location privacy could be a combined measure of position accuracy and its mensuration uncertainty.

The common understanding of privacy is in terms of control over personal information. Westin (1967) defined privacy as "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others." In (Tavani et al. 2001) is possible to find Charles Fried and Dag Elgesem statements, the former defines it as *not a simply absence of information about an individual in the minds of others, rather than the control over information about oneself*, the latter defines it as *a personal ability to consent to the dissemination of personal information.* In privacy theory, Tavani et al. (2001) argues the existence of three components: conceptualization, justification and management. Moor 1997 as cite in Tavani et al. 2001 states that

privacy best definition is access restriction rather than control of information.

Both Dwork (2006) and Solove (2006) addresses the concept in terms of its violations. The former has concerns about: (i)Defining what constitutes a preserve privacy failure (ii)Defining the objectives and the power of an adversary against privacy (iii) Identifying the possible background and a priori information the adversary can hold. While the latter proposed a privacy taxonomy with four basic groups of harmful activities: (1) information collection (Harms: Surveillance, Interrogation),(2)information processing (Harms: Aggregation, Identification, Insecurity, Secondary Use, Exclusion), (3)information dissemination (Harms: Breach of Confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation, Distortion), and (4)invasion (Harms: Intrusion, Decisional Interference).

In Ethics and Law, there are two definitions of Privacy: Normative Privacy and descriptive privacy. The former is delimited by law in effect and the latter the effective and actual restriction to any information (Tavani et al. 2001).

The taxonomy of Pfitzmann et al. (2010) is a pivotal contribution in how to generate understanding to a complex concept as privacy that can be evaluated and improved. It defines a vocabulary which expresses levels and dimensions to the conceptualization: Anonymity, Unlinkability, Undetectability, Unobservability and their variations:

- Anonymity of a subject is a level of indistinguishability within a set of subjects from an attacker perspective. Its level varies according to the a priori knowledge from an attacker. The higher the background knowledge the lower the anonymity.

- Unlinkability is an impossibility of fairly distinguish whether items of interest are related from an attacker's perspective.

- Undetectability is an impossibility of fairly distinguish whether items exist or not from an attacker's perspective.

- Unobservability from an item of interest means that all subjects involved cannot sufficiently distinguish whether it exists or not. In addition, anonymity of the subject involved with it.
- A pseudonym is an alias to the subject's real names.
- An identity is any subset of attributes of an individual person which uniquely identifies him within any set of persons.

1.4 How to preserve Locational Privacy?

Privacy and more particularly locational privacy need to be protected with both Regulatory and technological enabled solutions (Bouguettaya et al. 2003). These approaches are complimentary. Nonetheless, complex and diverse. For that reason, the objective of this work is to know the state-of-the art the technological solutions without disregarding the regulatory implications. Because the regulations should orient the early stages of the applications and system development.

Data Anonymization and Obfuscation classes of techniques are examples of how to preserve geoprivacy. Some families of techniques are worth to mention in Mobile Networks. Asuquo et al. (2018) lists some of them: (a)Mix-zones in Mobile Networks, (b) Obfuscation-based Approaches in Mobile Networks, (c) Location Cloaking in Mobile Networks, (d) Dummy-based techniques In Mobile Networks, (e) Caching Schemes in Mobile Networks, (f) Coordinate Transformation in Mobile Networks(g) Information Access Control in Mobile Networks.

1.5 How Systematic Literature Review (SLR) can contribute to locational privacy

Shokri et al. (2011) advocates that the location privacy research is in its infancy added to the fact that humans are naturally poorly performers of risk estimation, privacy level evaluation is a challenge. It presents some shortcoming, commonly

the adversary model of the systems are not appropriately addressed and formalized. The Attack capabilities Model and measurements of the adversary's success in his attacks, accuracy, certainty and correctness of estimations of the user's location and trajectory are missing. Adding to that, some current used metrics such entropy and k-anonymity for quantifying location privacy are inappropriate and there is no privacy benchmark for location information. (Shokri 2013)

For that reason, it is required a formal and standardized way of evaluate and understand the development and advances of the privacy preserving mechanism field of study. The systematic literature review is the method found to identify experiments, suggested models and schemes as primary studies using the practices of the Evidence-based software engineering. Using the Evidence-based paradigm will drive the findings/extraction and reporting will allow a consistent and robust knowledge of the given questions related to local privacy preservation with obfuscation and anonymization methods. The definition and the details regarding the review will be thoroughly explained in the following chapters.

Software development and IT systems has Design Science Research as one paradigm analysis which builds artefacts that follow the engineer cycle. Design Science Research is a research approach introduced to Information Systems to tackle properly the practical and dynamic nature of such artefact like algorithms, HCI Human-Computer Interfaces, schemes and languages Kanellis et al. (2008). This research approach is a rigorous process to build solving problems mechanism, evaluate what was projected and working, finally communicate the results. Its objective is to generate applicable useful knowledge for a problem of solving, the improvement of existing systems and the creation of new solutions or tools (Lacerda et al. 2013). Since software artefacts do not provide sufficient statistical basis for confirming or rejecting a hypothesis, the credibility level of the studies depends on the validity of the conclusions drawn Basili et al. 1999.

Carver et al. (2016) define the subjects types which can be evaluated in order to establish a baseline to measure advancements in security science, such as Algorithm/theory, Model, Language, Protocol, Process, Tool. Identifying the

novelty of subjects or if they are the basis of prior ones help the understanding the relevant and prospective subjects. The authors suggest the following questions related to the evaluation of the subjects: "Q1: What types of artefacts are being evaluated (e.g. algorithm, language, model, process, protocol, or tool)?
RQ2: How are the artefacts being evaluated (case study,experiment, survey, proof, discussion)?
RQ3: Are there trends in the type of artefact and the evaluation method used to evaluate it?"

These questions on the subjects evaluation approach from (Carver et al. 2016), add to the contributions of (Basili et al. 1999) and (Lacerda et al. 2013) from Design Science can be helpful to build the Review Protocol and the Data extraction and Data Synthesis.

1.6 Overview of Locational Data Protection Legislation

In the recent history some countries have been passing legislation in order to preserve privacy which clearly stablish it as a basic right or more specifically to protect and regulate how to treat personal data from the access, acquisition, storage and processing. Other countries are passing laws and policy to preserve the privacy rights of its citizens, and locational data is one object from this regulation. Some countries have explicitly laws protecting privacy and private information. Privacy is mention in the Universal Human rights, in Constitutional texts of some countries with just mentions or clearly protection such as USA, Portugal, Brazil, etc. In some countries privacy is not mentioned on their constitution but it is present in other legislations, like Canada, New Zealand, Germany, etc.

In 25th May 2018 entered into effect The General Data Protection Regulation of the European Union to protect personal data, the GDPR, which is one of the tools import to cope with the threats of one's privacy. It regulates the acquisition,

storage and transferring of personal data requiring from the user its consent as well as the users the knowledge of the data acquisition and its purposes as well as the possibility to manage it through the access, erasure and portability requisition. The regulation consists of 11 Chapters to lay down the rules to processing and traffic of the personal data of the individuals of the European Union("Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" 2016).

In Brazil, the law to regulate personal Data was approved in August 2018 and will enter into effect in 2020, it was inspired by GDPR.

1.7 Contributions

- Visualise the state-of-art of locational privacy preserving technologies present on the works from technological information community;
- Give an overview of at what extent the current technologies are capable to address the locational privacy threats issue, its limitation and challenges, identifying the trends in research in privacy preserving field;
- Analyse the trend on the schemes proposed in follow distributed architecture, avoiding to rely on Trusted Third Party and giving more control to the user and running more procedures on client side.

1.8 Thesis Outline

The rest of the thesis is organised as follows: the chapter 2 presents a review of the Systematic Literature Review methodology as a theoretical background the Methodology used is explained and how the Review was performed described. The chapter 3 presents the results and discussions related to the Data collected and synthesized. Finally, the chapter 4 bring some conclusions, limitations, future improvements and suggestions from the acquired knowledge.

Chapter 2

Systematic Literature Review

2.1 Theoretical Background

The systematic review has been widely used in medical research and just recently applied in the field of computer science and software development (Kitchenham 2007, Kitchenham 2004). The procedures were adapted from the heath studies to the computer studies. Condensing and transposing the rules and strategies used in the medical research to the software development context. There is a plethora of empirical studies and documents. In order to understand clearly the distinctions between the studies and documents produced in medical research which were adapted to computer science, there is a following list with some succinct definition (Kitchenham 2007) of: Meta-analysis, Primary study, Secondary study, Sensitivity analysis, Systematic literature review, Systematic review protocol, Systematic mapping study and Tertiary study.

- Primary study - An empirical proposition to answer a problem.
- Meta-analysis - Secondary study where the synthesis is made based in quantitative analysis.
- Secondary study - A study which review primary studies.

- Sensitivity analysis - Analysis to verify bias in Meta analysis and Systematic literature review.
- Systematic literature review (SLR)- A secondary study with a well-defined methodology and reproducible.
- Systematic review protocol - A plan for a systematic literature review.
- Systematic mapping study - General and wide vision of the primary studies, commonly providing a classification.
- Tertiary study - A study which review secondary studies about a same topic.

The systematic review or systematic literature review is a formalised way to combine a set of empirical studies using the concept of evidence-based method as orientation. Focusing on aggregating empirical evidence of a defined question or problem according to Brereton et al. (2007). The main objective is to build a protocol which describes the source selection, inclusion and exclusion criteria, search methods and keywords (Felizardo et al. 2009). The SLR consists in three main parts Planning, Execution and Report.

In Kitchenham 2004, Kitchenham 2007 the authors define the aim of the SLR as a research topic evaluation applying a formal, replicable and well defined methodology, and it has several benefits: reduces bias, allow general conclusions from broader contexts. Complemented by a meta-analysis the pool of studies can detect more than individual studies alone. In (L. Feng et al. 2017) the authors understand the importance of SLR, but its performance manually is quite challenging, with intensive work and prone to bias and omissions.

Biolchini et al. (2005) as cited in (Felizardo et al. 2009) states that the benefits of this type of research method rely on the fact that SLR has objectives clearly defined, a review protocol built which contains all items needed to perform the task, such as selection of sources, searching methods and keywords, inclusion and exclusion criteria and finally the quality assessment of primary studies. Hence,

the use of such a methodology in computer science and in software/application development can support the professionals to adopt a standard or techniques proven to be more effective: Consequently, improving the quality of their final products and services.

Garousi et al. 2017 suggests two new secondary studies which consider not only white Literature but also Grey Literature, the Multivocal Literature Review and Multivocal Literature Mapping. A Multivocal Literature Review (MLR) is a Systematic Literature Review (SLR) which includes materials called grey literature." Garousi et al. 2017

Mapping or Scoping Studies is another type of second study which do not focus in answer research questions but identify omissions in primary studies and which are the topic clusters that can be an object to SLR The process of search, the inclusion and exclusion criteria are explicitly defined in the protocol of SLR differently than the mappings. They are broader on scope of topics (Petersen et al. 2008) although, comprising by the same early steps of SLR, but they aim to classify the studies instead of performing data extraction and data synthesis. These are the essential difference between mapping studies and SLR. For Petersen et al. (2008) the following three stages of SLR are common to mapping studies: 1. identification of relevant primary studies; 2. selection of the appropriate primary studies following a set of inclusion/exclusion criteria; 3. Performing the quality assessment the selected studies (bias/validity).

Meta Analysis is a type of data synthesis techniques along with: narrative synthesis, quantitative synthesis, qualitative synthesis, thematic analysis. It is most appropriate to quantitative studies (Garousi et al. 2017). Beside, the quantitative approach, Meta-analysis can also be qualitative and reveal the biases, strengths, and weaknesses of existing studies Russo 2007.

The quality tool developed by Dybå et al. 2008 has been applied frequently to systematic reviews to measure the quality of empirical studies. It comprises 11 questions as follows:

"1.Is the paper based on research or is it a “lessons learned” report based on

expert opinion? 2.Is there a clear statement of the aims of the research? 3.Is there an adequate description of the context in which the research was carried out? 4.Was the research design appropriate to address the aims of the research? 5.Was the recruitment strategy appropriate to the aims of the research? 6.Was there a control group with which to compare treatments? 7.Was the data collected in a way that addressed the research issue? 8.Was the data analysis sufficiently rigorous? 9.Has the relationship between researcher and participants been considered to an adequate degree? 10.Is there a clear statement of the findings? 11.Is the study of value for research and practice?"

The same way that Dybå et al. 2008, Carver et al. 2016 suggested a quality assessment tool for primary studies, but instead of 11 questions 10 were proposed, as it can be seen below. "QC 1 Is there is a clear statement of the aim of the research?

QC 2 Is the study put into a context of other studies and research?

QC 3 Are system or algorithmic design decisions justified?

QC 4 Is the test data set reproducible?

QC 5 Is the study algorithm reproducible? QC 6 Is the experimental procedure thoroughly explained and reproducible?

QC 7 Is it clearly stated in the study which other algorithms the study's algorithm(s) have been compared with?

QC 8 Are the performance metrics used in the study explained and justified?

QC 9 Are the test results thoroughly analysed?

QC 10 Does the test evidence support the findings presented?"

On the Planning phase, the structure of the review will be shaped and task and subtasks assigned. All these components should be explained in detail.

To perform a review a guideline is needed, according to Pickard et al. 1998, Greenhalgh et al. 2005 there are three methods: Protocol driven, "Snowballing" and Personal knowledge. Protocol driven is a strategy to establish the detailed prescriptions for the review. It is driven by rules and criteria define beforehand

to serve as a guideline to perform the tasks and report it.

Snowballing is a cross-referencing method of studies. From the references from the fist batch of studies it is decided whether to pursue the references of the references. The Snowballing process includes studies in the selection. Greenhalgh et al. (2005) Snowballing consists in pursuing references of references and electronic citation tracking which will result on finding high quality sources on uncommonly locations.

Personal Knowledge approach starts with resources requests to the experts in the field; it is the search criteria. The background knowledge of the experts and its connection with others from the field allow access to relevant and not indexed material. However snowballing and personal knowledge can provide high relevant studies, report them need a more attentive and through description. Because it is not a systematic way of acquiring material, the studies could be subject to selection bias.

To the general structure of the Planning phase is to develop a protocol for the review. Conversely, Greenhalgh et al. 2005 advocates that for complex evidence studies review along with the protocol driven search a snowballing method should be also applied.

Moher et al. 2015 discusses how the protocol driven guideline is restrictedly used in SLR despite of its usefulness. He also defines protocol as a document that presents an explicit plan for SLR which constitutes a detailed rationale and methodology.

Regarding protocol development the articles, Kitchenham 2004,Biolchini et al. 2005, (Uzun et al. 2018), Moher et al. 2015 can offer examples of protocol to be applied. Some are more thorough than the others in relation of each subtasks documentation such as (Uzun et al. 2018) and Biolchini et al. 2005.

On the execution phase, the SLR chosen guideline is applied, either protocol-driven, snowballing or personal knowledge or a combination of the three. The basics tasks are described, keywords chosen in the planning phase will identify eligible papers, subsequently the criteria for selection and exclusion will be ap-

plied, added by the time frame criteria, quality assessment to establish the first amount of studies to be taken into account for further investigation.

The tasks to be performed defined in Review Protocol are: Keywords Definition, Search and Selection, Quality Assessment, Data Extraction and Data synthesis.

The report phase consists in the written description of the steps and respective tasks in detail and reasonable justification. The guideline for its performance is given by the review protocol build in the planning phase of the research. On the report all conclusion drawn as well as the documented tasks will be interning in one document. This document should contain the bias and validity discussion. The report should contain all the steps taken with detailed procedures of each of its tasks. All unexpected issues should be reported as well as unexpected situations and results. Limitations, constrains, conflicts should be also be reported. Before proceeding to the reporting step the results obtained should be validated, it is a common approach to use checklist to evaluate the validity. Some useful questions applied were previously presented.

Issues

This methodology is subject to different types of biases: Selection bias, performance bias, attrition bias, detection bias and report bias Higgins et al. 2011. In consequence, the tasks and subtasks should follow well-defined guidelines, individual or ad hoc decisions should to be avoided. However, in case it is needed it should be properly justified.

SLR presents some issues such as Publication Bias, Protocol Form adaptations and implementation, Grey Literature shortcomings with no controlled vocabulary, flawed and not indexed search tools, variety levels of quality and striving to evaluate.

2.2 Methodology

Since the scope of this study is the technological enabled solutions, understanding the locational privacy preserving tools and schemes state-the-art is imperative. In order to perform this task, the method selected was the systematic Literature review, addressing the current obfuscation and anonymization techniques, its structures and architecture, weakness and threats.

The aim of this research will be delimited in four dimensions: Concerns, Solutions, Trends and Risk Assessment and Architecture defined as research questions to assess the efficiency of the obfuscation and anonymization strategies. The protocol of the Data extraction will be improved during the process of the reading the papers which will not be older than 5 years.

Even though there are relevant Phd Thesis been developed on the privacy preserving research, It was opted to keep only using the white literature instead of include what J. Adams et al. 2016 define as the first tier of Grey literature (GL) Figure 2.1. Grey Literature was not included in the research due to its challenging control and evaluation needs.

As verified at the Theoretical Background, Systematic Literature Review needs to be performed in three Steps: Planning, Execution and Report. The complete overview of the methodology applied to this SLR it is shown in Figure 2.2.

On the Planning step, the aims and Research Questions will be defined and a Review Protocol built. The Review Protocol is pivotal to perform an SLR, this document contains all the actions thoroughly explained. It defines how the search and Selection will be performed, how the Data will be collected, aggregate, synthesised and report. On the Executing step, all activities planned on the previous step, Search and Selection, Data Extraction, Data Synthesis will be executed.

On the Reporting step, it will be following the guidelines of master thesis document.

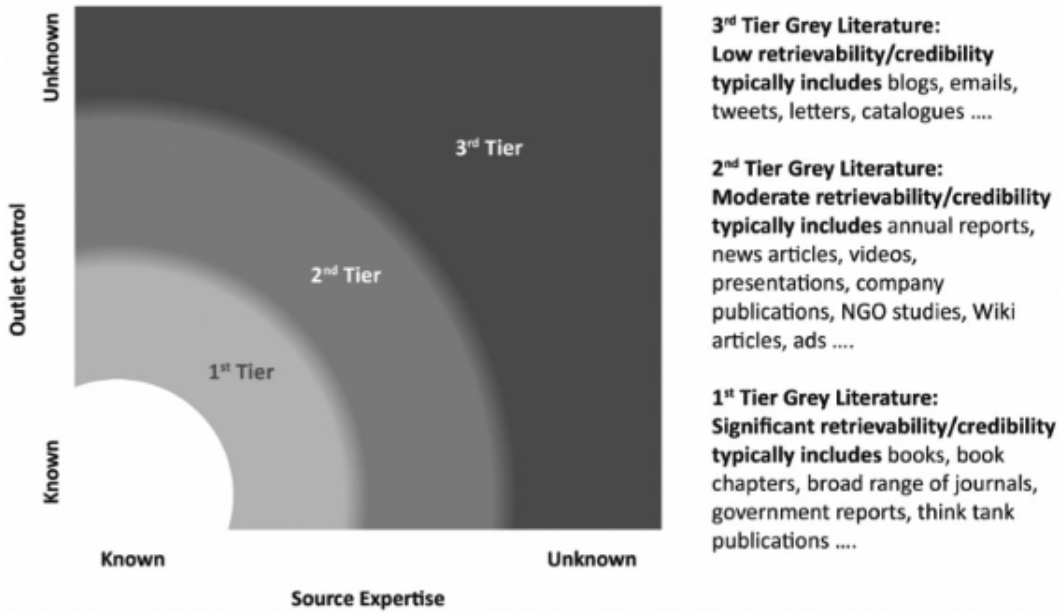

Figure 2.1: Shades of Grey Literature (From J. Adams et al. 2016)

Review's objectives

The Main objective is to provide a state-of-art of the obfuscation and anonymization technologies for preserving locational privacy.

RQ1 - CONCERNS: What are the addressed concerns for applying obfuscation and anonymization techniques to protect location privacy?

RQ2 - SOLUTIONS: What are the proposed solutions in obfuscation and anonymization techniques to protect location privacy?

RQ3 - TRENDS: What are the existing research directions within obfuscation and anonymization techniques in location privacy?

RQ4 - RISK AND ARCHITECTURE: How architecture affects the solutions, service quality with the use obfuscation and anonymization techniques to protect location privacy?

The Systematic Literature Review (SLR) performed on this research will protocol based. The Review Protocol structure will be the following:

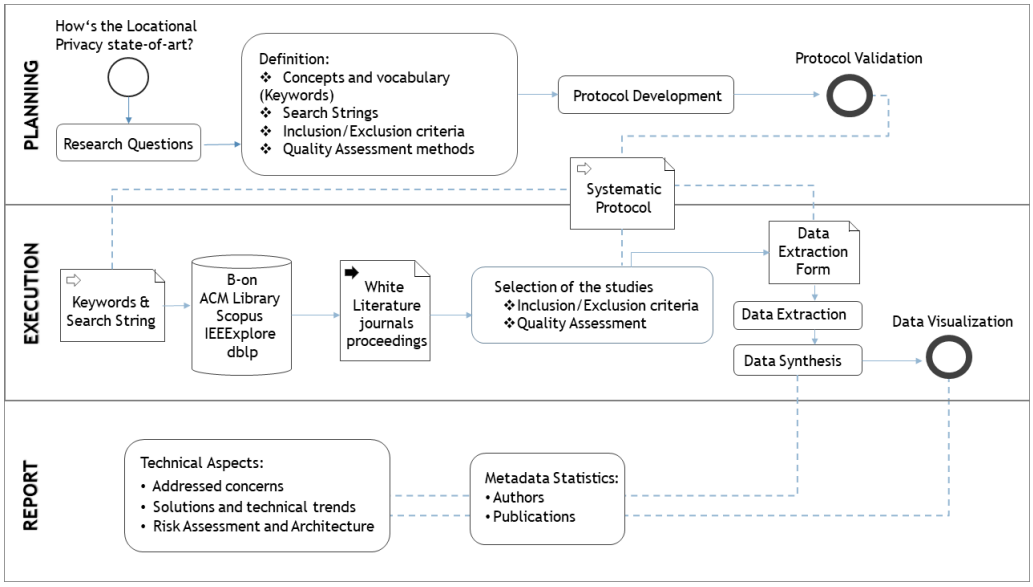

Figure 2.2: Review Methodology

1.Question formularization

Review's objectives

Keywords and synonyms

2.Source selection

Sources searched to identify primary studies.

Criteria used to assess the quality of primary studies and their application

3.Studies Selection

Inclusion/exclusion criteria and their application

4.Data Extraction

Data extracted procedure from the primary studies

5.Results summarization

Data synthesis

Differences between studies revised

Data combination and integration

Conclusions based on evidence

Source selection To perform a systematic search strategy, there is a need to define the vocabulary and key concepts in other to build the digital libraries search

strings. Several databases will be searched to guarantee a reasonable coverage on the topic.

The vocabulary assessment and keywords definition were orientated by the concepts list of (Wernke et al. 2014). From this list, test were performed and new words were added and excluded.

Listed by (Wernke et al. 2014)

position dummies	coordinate transformation
spatial cloaking	k-anonymity
spatial obfuscation	mix zones

and conjoint with the following:

PET - Privacy-enhancing technologies

geo-indistinguishability

The Keywords Definition took into account the usage of the spatial and location words to create the strings and test the searches. The following strings were tested against the digital databases.

“spatial cloaking” OR “location cloaking” *anonymity AND location or *anonymity AND spatial “spatial obfuscation” and “location obfuscation” “mix zones” and privacy

Privacy need to be added to mix zones because this expression is present in other knowledge fields beside privacy preserving. The words spatial and location were added to the string because just anonymity was generic, and the focus was locational data. For the same reason spatial and location were added to obfuscation and cloaking. There are other types of obfuscation, like authorship, code, etc.

The words and expression: coordinate transformation geomasking, Voronoi masking and point dummies were discarded because they were either too generic or exceedingly specific as Voronoi masking. The reason for the exclusion was a

great amount of irrelevant studies from the search results and the relevant ones were covered by the other keywords.

Once the aim and the research questions are defined the first step is to elaborate a plan to search relevant studies to answer to the questions. The keywords and synonym were tested in the engine search of different Digital Libraries. Since the engines work differently some search strings were written slightly different in each case that can be verified in Appendix B. The search used broad contexts, in order to bring different platforms and architectures. For that reason, the time span criteria, relevancy and quality assessments were applied to constrain the studies selected. The final number of the studies pass through the steps of selection, the search criteria and afterwards with the inclusion and exclusion criteria.

Only two classes will be on scope: Data Anonymization and Data Perturbation classes of techniques, the articles which present combined technologies will be selected only if they use any of the techniques classified in one of the two aforementioned classes.

The keywords related to Data Perturbation Techniques and Data Anonymization were used to search the relevant studies on the Digital libraries, namely: Scopus, IEEExplorer, B-on, ACM Digital Library and dblp. The Libraries Scopus, ACM Library, B-on, IEEExplorer the string were applied entirely in one step. Conversely, dlpb the search string was done by steps because we did not allow customization on the queries. For that reason there were duplicates results even within the papers found by the aforementioned Libraries. The selection of the online database followed the criteria of been a wide spectrum and a variety of articles and publication indexed. The selection was performed sequentially, as follows: the Scopus, B-on, ACM, IEEExplorer, dbpl. The description can be seen in the Appendix E.

Criteria to assess the quality of primary studies

The quality criteria chosen is a combination of the Peer-reviewed Journals with studies with a high number of citations. Pursuing the quality assessment

prescriptions from Dybå et al. 2008, Carver et al. 2016 and Kitchenham et al. 2011. Added to the two aforementioned factors generating the quality check-list as following.

Quality Assessment check-list

QA1 - Are the aims of the study clearly stated?

QA2 - Is the proposed solution clearly explained and validated by an empirical evaluation?

QA3 - Is the architecture clearly described?

QA4 - Is the threat model clearly described?

QA5 - Do the conclusions relate to the aim of the purpose of study?

QA6 - Does the report have implications in practice in a research area of privacy preserving mechanism?

The Extraction Form contains one entry QA which adds a number for the questions with a positive answer.

Studies Selection Inclusion/exclusion criteria:

Since the search was broad, more criteria other than then the keywords were necessary to narrow down the number of the studies, the relevance, reputation and quality criteria play a significant role in the selection of the studies in analysis. For this work the number citations, five years period of publications, from 2015 to 2018. Following are the inclusion and exclusion criteria in detail.

Inclusion criteria:

IC1-Papers Published between 01/01/2015 and 30/11/2018;

IC2-Number of citations

- Year of Publication 2015 >= 15
- Year of Publication 2016 >= 10
- Year of Publication 2017 >= 5

- Year of Publication 2018 (Jan-Jun) > 1
- Year of Publication 2018 (Jul-Nov) >= 1

Exclusion criteria:

EC1 - Articles which the full text is not available;

EC2 - Duplicate Articles from different platforms;

EC3 - Articles not written in English;

EC4 - Articles not related to locational privacy preserving mechanism;

EC5 - Articles not related to obfuscation or anonymization techniques;

EC6 - Articles not related to locational data;

EC7 - Articles from second studies

EC8 - Articles related with Vehicle Network

The Exclusion Criteria EC8 was established after the process of Data extraction due to the diverse concepts and artefacts not adaptable to the realm of the Mobile Networks.

2.3 Data Extraction and Data Synthesis

After the preliminary study selection, the data extraction phase initiates. The crucial task of this phase is to collect data from the studies through reading and filling up the Extract Data Form present on Appendix C built and validated on the planing step. Not all entries are applicable to all artifacts. The broad conception of the extraction form enables the maximisation of information collection thus the data analysis and synthesis will be enriched. Most of the articles did not present all details of the experiments, the threat model, platform and settings. It was not possible to extract all information to fill all entries on the extraction form.

The extracting process started with reading and screening of the studies. The focus at the beginning was on the abstract, introduction and conclusion. The reading task was executed as following: abstract screening, text sections screening, full text screening, data form entry filling screening. If after the process of reading all full texts of the studies some entries in the Data Extraction Form were left empty by omission it will be corrected during Data form entry filling screening phase.

The reading process focused on the article's sections: system design, experiment and evaluations, the information extraction of the proposed solution, system architecture, the risk assessment and threat model, techniques, the results and discussion, applicabilities, capabilities, limitations, constrains challenges level and comparison with others solutions. Development environment, architecture, common threats and countermeasures encountered, concerns addressed and solutions as well as information journals metadata were also extracted.

On the entry *Why not* from the Data Extraction Form is a place to report the post excluded studies which exclusion was performed after the data extraction started during the reading process. The entry *sections* was helpful for study screening, showing quickly where to extract the Address Concern, Aims, solutions and the general overview of the study.

Differences between studies revised

The selected artefacts present different implementation and characteristics. In the Figure 2.3 it is possible to observe that the 37 of 54 studies comprises mostly by schemes and algorithms.

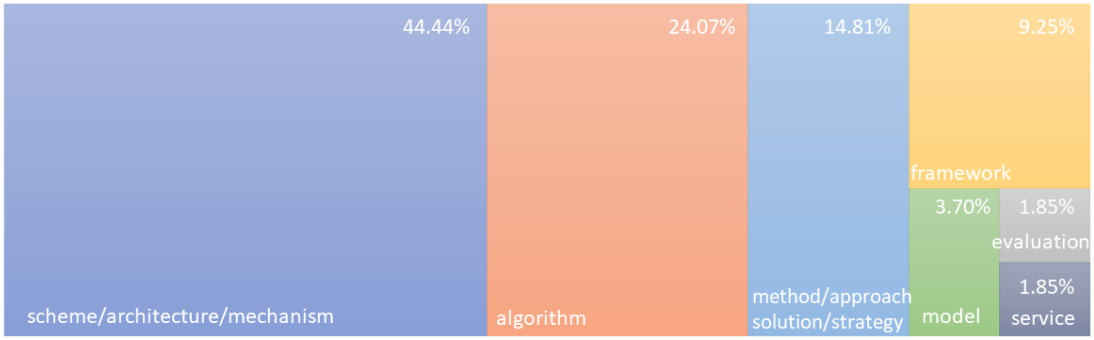

Figure 2.3: Types of Artefacts

Data combination and integration

The data integration will follow the similar structure of the research questions. There will be four main sections: metadata and technical aspects separated by the dimension. The research question (RQ1) will have the title addressed concerns, the second title will be solutions and trends answering to questions two and three (RQ2 and RQ3), the third title risk assessment and architecture answering questions (RQ2 and RQ4).

To manage risk, organisations need the means to assess them. In software development, the threat Model provides the description of the risk in security Networks. Describing the targeted assets and procedures of the system, the capabilities of the adversary and the policies to tackle them. On the Data extraction form, this information can be extracted. The entries used were type of artefact *artefact*, the threat model of the schemes and algorithms *threat_model*, the topology *topology*, the presence of a trusted third party *TTP*.

Chapter 3

Results

The selection results can be seen in Figure 3.1 which shows the number of the *Included*, *not included* studies, and number of each study for a type of the exclusion criteria. On the Appendix D it is possible to see a more detailed table with the Selection Status results with the studies disaggregated for Digital library used.

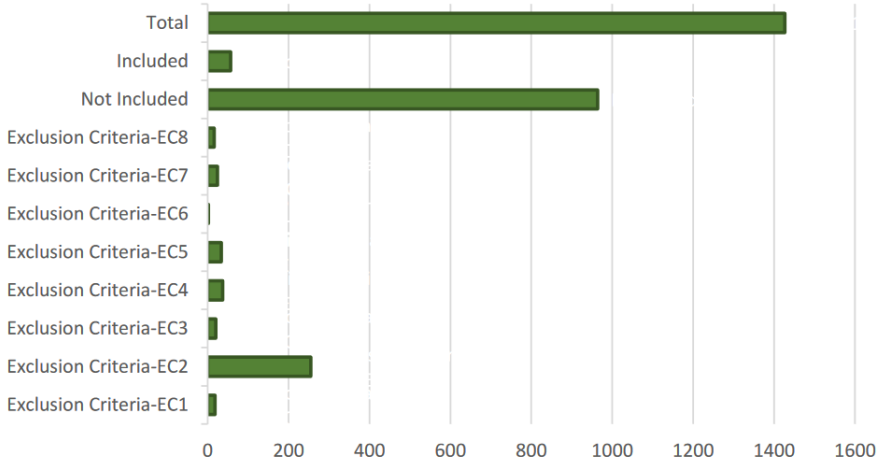

Figure 3.1: Results of Selection and Exclusion Criteria

From the 1427 articles after applying the inclusion and exclusion criteria 54 studies were selected.

From the total select studies, 43 from 54 present or should present system design and threat model. Because they are schemes, system architectures, service or algorithm with implementation described Figure 2.3. To total set of studies

not all the questions are applicable because they were just a simply improvement of a specific routine or algorithm but not a proposed scheme or mechanism.

A quality assessment was performed using the checklist defined in the planning phase of the review. From the studies which all the six questions of the quality checklist should applied were aggregated in the following Table 3.1.

QA codes	**QA Description**	**no.Studies**
1,2,3,4,5,6	Complete quality check-list	13
1,2,5,6	No adversary model nor System Design described	11
1,2,4,5,6	No system Design described	8
1,2,3,5,6	No adversary model described	2
1,5,6	No solution clearly explained and empirically validated, no adversary model nor system design described	2
2,3,4,6	No clear aim stated and consequently not achieved	2
2,6	solution clearly explained and relevant research Topic	2
1,3,4,5,6	No solution clearly explained and empirically validated	1
1,3,4,6	No solution clearly explained or conclusions related with the aim	1
1,3,5,6	No solution clearly explained and empirically validated nor adversary model described	1

Table 3.1: Quality check-list Synthesis

Eleven studies had neither a clear and detailed adversary model nor System Design described, adding to them the studies with either no clear and detailed adversary model or System Design described, two and eight respectively. It is around half of the studies has no clear description of the system design or privacy risk assessment/adversary model as it can be seen in fig:qa under the category of Risk and Architecture deficit.

SLR instructions understands quality assessment as one of the exclusion criteria. But instead of removing the studies, it was decided to have them analysed in

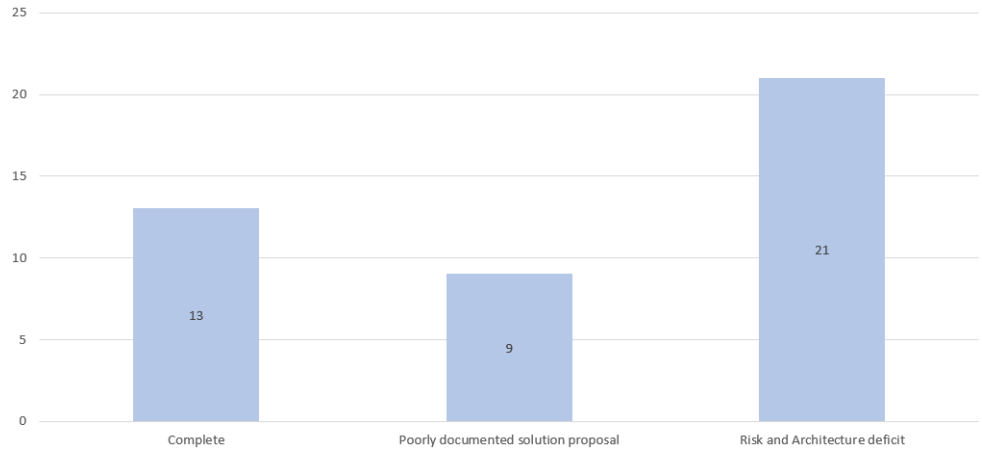

Figure 3.2: Quality check-list Categories

order to identify the most common relevant parameters and conditions overlooked in this type of research.

The studies which were listed as not having a clearly defined aim are generally the ones which the authors explained a general problem but not explicitly state that the aim of the proposed scheme or other artefact has a define design goal to be achieved.

3.1 Articles Metadata

In this section, the Metadata of the Studies will be discussed. The variables (entries) in the Data Extract Form considered are the ones related to the Publication media Information, such as Publication Date, publisher' name, written language, authors' names, Institutions and Digital Libraries. Nothing related to the study content itself. Because of the search criteria some information is already given and comon to all the studies, such as the language of the studies which is English and the period of publication that is from 01-01-15 to 30-11-18.

The major part of the author Institutions 43% are from the Republic of China, followed by USA with 27% as it can be seen in Figure 3.3. This massive number of studies is following a dominance trend of the technological sector in China,

growing with high rates in new technologies development, in the number of new start-ups finding no comparison in other countries, leaving even USA far behind. The amount of investment, a budget of some of these companies are massive. This phenomenon is so striking that the journalist Moritz 2018 in his article of the Financial Times from June 2018 states that *"China is winning the global tech race"*.

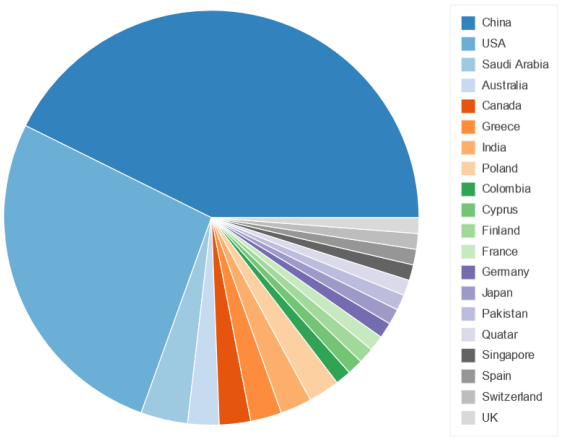

Figure 3.3: Author's Institutions Country

The most relevant publications found are: The Future Generation Computer Systems (FGCS) and Journal of Network and Computer Applications from the Elsevier Publisher, IEEE Access, IEEE IoT Journal (IoT-J) and IEEE Transactions on Knowledge and Data Engineering from IEEE Journals and Magazines were the top five of the Publications, FGCS with 6 and the others with 3 articles. The top ten publication with the respective studies can be seen in the Appendix F and the on the Figure 3.4. The number of journals with only one article selected is 24, which names are following: ACM Conference on Security and Privacy in Wireless and Mobile Networks, Applied Soft Computing, Computer Communications, Computer Networks, Computers and Security,IEEE INFOCOM, IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, IEEE International Conferences on Big Data and Cloud Computing, IEEE Wireless Communications, International Conference on Data

Engineering, International Journal of Distributed Sensor Networks, International Journal of Geographical Information Science, Investigación en Innovación en las Ingeneirías, Journal of Transport Geography, Knowledge-Based Systems, Multimedia Tools and Applications, Personal and Ubiquitous Computing, Sensors, Soft Computing - A Fusion of Foundations, Methodologies and Applications, Telecommunication Systems, Transportation Research Part C: Emerging Technologies, Tsinghua Science and Technology, Wireless Communications and Mobile Computing, Wireless Networks.

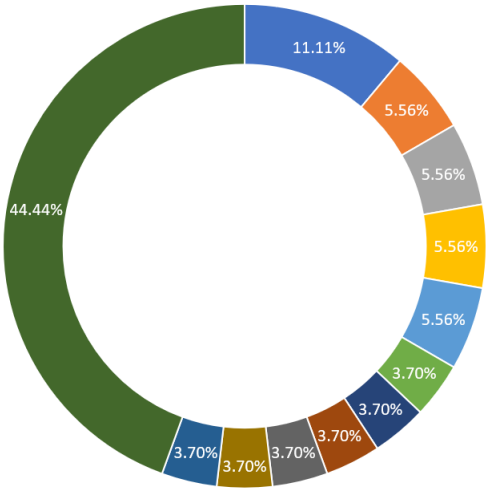

Figure 3.4: Publications from the selected articles

FGCS has its focus on distributed systems, collaborative environments, high performance and high performance computing, Big Data and Internet of Things presenting with an Eigenfactor of 0.008 and an Impact Factor of 4.639.

The Journal of Network and Computer Applications has its focus on computer networks and applications (design, standards,etc) studies. It presents an Impact Factor of 3.991 and an Eigenfactor of 0.008.

IEEE Access has its focus on the topics comprised by IEEE, emphasizing applications-oriented and interdisciplinary articles. It has an Impact factor of 3.557 and an Eigenfactor of 0.0186.

IEEE Transactions on Knowledge and Data Engineering has its focus on knowledge and data engineering aspects of computer science, artificial intelli-

gence, electrical engineering, computer engineering. It has an Impact Factor of 2.775 and Eigenfactor of 0.018.

IEEE Internet of Things Journal (IoT-J) has its focus on the latest advances on the various aspects of IoT. It has an Impact Factor of 5.863 and Eigenfactor of 0.00663.

Except from FGCS with 11% of the articles, there is no concentration on a specific journal. Since 44% of all studies are percentage of journal with only one single article. In addition, the journals with more numbers of studies presents high impact factors and a diverse scope of publication.

3.2 CONCERNS Addressed

The CONCERNS dimension was one of the four unfolded in research questions in order to display the state-of-art of locational privacy. Therefore, identify the current concerns and what extent they have been addressed is crucial. They can be related to defence to current threats, identification of new ones, limitation on privacy preserving technology, improvement of existent techniques and mechanism, or suggestion of new methods. This dimension will be extracted from the following Data Form entries: *addressed_concern* and *obs_addconcern*, the Addressed Issues collected from the studies can be seen on Appendix A. The aggregated concerns categories are the following:

- Identification of new threats
- Mechanism proposal against a current threat
- Solve a limitation on privacy preserving mechanism/scheme
- Improvement of existent techniques or scheme
- Suggestion of a new method
- Evaluation or test of privacy preserving mechanism/scheme

The majority of the studies were focused on suggestion of new privacy preserving schemes with 40.7% or dealing with the current environment of known threats with 38.9% Table 3.2.

Concern	**Percentage**
Suggestion of a new method	40.7%
Mechanism proposal against a current threat	38.9%
Improvement of existent techniques or scheme	13%
Evaluation or test of privacy preserving mechanism/scheme	13%
Solve a limitation	7.41%
Identification of new threats	1.85%

Table 3.2: Addressed Issues

From the entry *assessment_approach* were captured the tools used to evaluate the artefacts. The types of assessment are: a case study, experiment, theoretical, analytical and empirical validations or a small example. From the 54 articles 44, i.e. 81.48%, performed experiments or simulations. The objective pursued was to provide a reasonable level of privacy with an acceptable user experience.

3.3 SOLUTIONS and TRENDS

On this section, the proposed solutions and trends observed on this four years will be discussed and further directions projected. The entries on the Data Extraction form examined were: *techniques*,*combined_techniques*, *aims*, *solutions* and *constraints*.

The proposed solutions can be seen in Appendix A which lists the classes of techniques, Anonymization with 46.48%, Data perturbation with 40.85% and Encryption with 12.68%. From the total of studies, 31.48% have combined types of techniques. K-anonymity, dummyfication, differential privacy are the most used techniques. It is worrisome, since k-anonymity perform poorly against continuous behaviour and moving objects, therefore is commonly used combined with others techniques.

The techniques and their families can be seen in Appendix F and the threats which the proposed solutions address can be seen in Appendix F. In Table 3.3 and in Figure 3.5 it is verified that the solutions in general aim to provide location and trajectory privacy 77.77% or protect against a specific attack 25.92%. The solutions are rather general than specific in dealing with privacy threats.

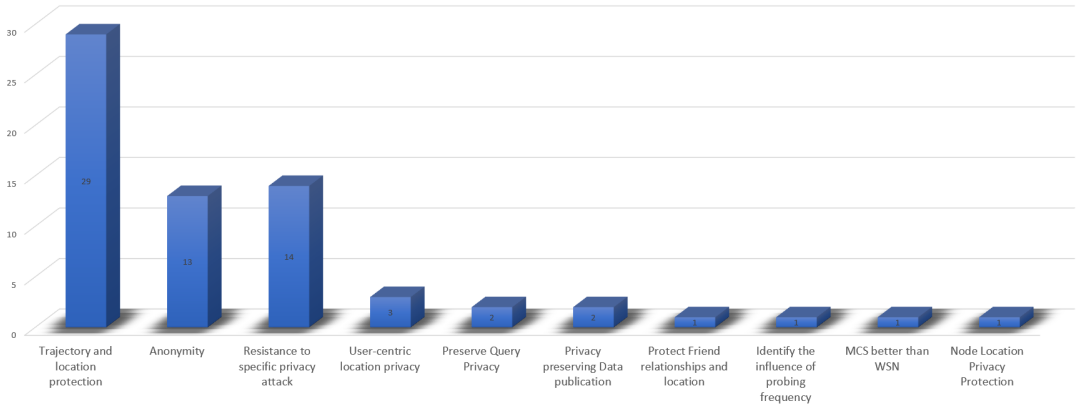

Figure 3.5: Solution's aims

Threats like the inference attacks and continuous query are still a challenge to privacy preserving mechanism. Consequently, a low number of threats addressed

solutions it is an ill-advised direction.

For Shokri (2013), the recurrent menace to locational privacy is classified in: i)tracking attack, ii)inference attack, iii)disclosure attack, iv)user profiling. On Appendix F the threats addressed by the solution proposed on the select articles are listed in categories partially based on his classification. Most of them are historical attackers, they collect, analyse and integrate to other sources of data, such as context information or other's entity data.

Aims	no.studies	Solutions
Trajectory and location protection	29	**DQE** S. Zhang, G. Wang, et al. 2018, Ma et al. 2018, Ye, Y. Li, et al. 2017, **CTPP** Peng, Liu, Meng, et al. 2017, **LTPPM** Gao et al. 2015, Chunguang et al. 2015, **LLB** G. Sun, Liao, et al. 2017 ,**TVM** Konstantinidis et al. 2015, Hara et al. 2016, J. Li et al. 2017, Seidl et al. 2016, **MobiMix** Palanisamy et al. 2015, **2SP-SP, Priv-2SP-SP** Aïvodji et al. 2016 ,S. Zhang, Choo, et al. 2018,Ye, Chen, et al. 2018, Ye, Chen, et al. 2018,Lahe et al. 2017,Peng, Liu, and G. Wang 2017,Chi et al. 2018,Y. Wang, Cai, Tong, et al. 2018,Schlegel et al. 2015,Ye, Y. Li, et al. 2017,**HISP-NC** Rios et al. 2015,Yi et al. 2016,Montazeri et al. 2017,Weiwei et al. 2016,Han, J. Wang, et al. 2018,Chi et al. 2018,H. Zhu et al. 2018
Anonymity	13	**DPMM** Memon et al. 2017, **PPVC** Shahid et al. 2017, Chunguang et al. 2015, **MobiMix** Palanisamy et al. 2015, **DLP** G. Sun, Chang, et al. 2017, Huang et al. 2018, Y. Zhang et al. 2016 ,**DPkA** J. Wang, Cai, et al. 2018, Graph-based X. Li et al. 2016, **SCGuard** To et al. 2018, Al-Dhubhani et al. 2018, **Ttcloak** Niu, X. Zhu, W. Li, et al. 2015, k-Trustee Jin et al. 2018

Aims and Solutions Synthesis – Continued on next page

Continued from previous page

Aims	**no.studies**	**Solutions**
Resistance to specific privacy attack	14	Niu, X. Zhu, Q. Li, et al. 2015 ,**ASA** Y. Sun et al. 2017 ,**DLP** G. Sun, Chang, et al. 2017, Y. Wang, Cai, Chi, et al. 2018 ,**TIS-BAD** Wightman et al. 2015, ILLIA Zhao et al. 2018, Chunguang et al. 2015, LLB G. Sun, Liao, et al. 2017, CTPP Peng, Liu, Meng, et al. 2017, Y. Wang, Cai, Chi, et al. 2018, Schlegel et al. 2015, **ILLIA** Zhao et al. 2018, k-Trustee Jin et al. 2018, Han, J. Li, et al. 2016
User-centric location privacy	3	G. Sun, Xie, et al. 2017 ,**ESOT** Ullah et al. 2018, L2P2 G. Sun, Liao, et al. 2017
Preserve Query Privacy	2	**EPLQ** L. Li et al. 2016,Yi et al. 2016
Privacy preserving Data publication	2	Terrovitis et al. 2017, Oksanen et al. 2015
Protect Friend relationships and location	1	CenLocShare Xiao et al. 2018
Identify the influence of probing frequency	1	Freudiger 2015
MCS better than WSN	1	He et al. 2015
Node Location Privacy Protection	1	J. Wang, R. Zhu, et al. 2018

Table 3.3: Aims and Solutions Synthesis

3.4 Risk Assessment and Architecture

On this section, the Privacy Risk Assessment and Adversaries model will be discussed. Together with the dimensions of the solutions and the quality of service.

In security networks, the risk assessment buils threats or attack models. The manager define its policy and analyse the potential risks for system entities, assets and network to be exposed. The assumptions of the severity, extent of an attack and the capabilities of an adversary need to be reasonable, otherwise the protection and consequently mitigation will be ineffective. In computer security the adversary and threat Model can be classified as following: Global/Local, Active/Passive, Static/Adaptive and Internal/External. The entries on the Data Extraction Form for this type of information are: *Internal_External*, *threat_model* and *topology*.

Mobile Applications and services schemes can present a centralised or decentralised architecture. Each arrange has its advantages and drawbacks. The centralised structure simplify control, but generate bottlenecks or become a weak spot. On the other hand, distributed architecture reduce the extent of damage when an entity is compromised and remove the role of third trusted party.

On Table 3.5 and Figure 3.4 it can be verified that 31.48% Implementation dependant or not informed, 27.78% Centralised, 40.74% Distributed. The existence of Trusted Third Party (TTP) entity percentages comprises 35.19% no TTP, 31.48% Implementation dependant or not informed, 22.22% TTP, 11.11% Semi trusted.

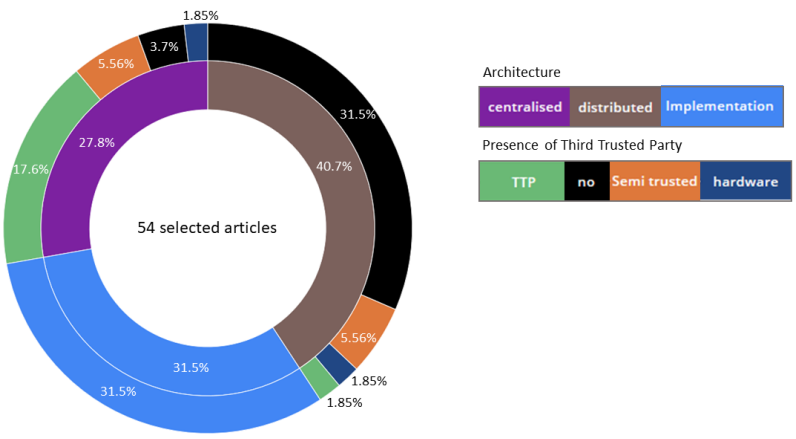

Figure 3.6: Architecture and presence of TTP

From the studies which were supposed to present a complete architecture described 30.23% succeed similar percentage, 25.58%, the studies without a clear description of the system design and threat model (Table 3.1).

On the entry *metrics*, the metrics used to evaluated the performance of the artefacts were captured as mostly computational, communication, storage cost and privacy level.

Privacy preserving mechanisms are highly complex, consuming massive resources either on device or Server, for this reason achieve a reasonable performance with privacy protection is hard. But with a rapid development of hardware, the accessibility to new technologies, the devices are become increasingly more powerful in terms of computation and storage. Thereof, potential usage on client-side and user centric applications with reasonable tradeoff between privacy and utility. Other consideration to be made regarding to QoS is the overhead and battery usage.

3.5 General Discussion of the findings

To perform an intensive working endeavour like SLR some limitations has to be taken into account, such as the time frame available, restrict resources and the manually executing of the tasks. The scope and selection criteria were affected by the restriction, whereas only four years articles will be investigated and Vehicular Networks excluded.

Bias is one of the risk in performing SLR, on this research it is worth to mention the difficulty on achieve the gold set of the studies. the total amount of studies existent that to be satisfied the criteria. the total amount is unknown, hence it is not possible to measure the bias of the selection of the studies.

Other limitation of the study rely on the Data extract Form filing up, since the process were mostly manual, with a significant amount of studies and entries. It possible an eventual omission of data on the Data Form.

Background knowledge, collusion and contextual data are not considered on the system design of the solutions. The assumptions, when present at the article are naïve assuming in some cases entities to be fully trusted.

Architecture	**Category**	**TTP**	**no.Studies**
Users+LBS server	distributed	no	8
User+Anonymizer+LBS Server	centralized	Anonymizer	6
SN Server+query user (QU)+query user's friends (Ufs)	distributed	no	1
User + Location-Storing Social Network Server (LSSNS) + Cellular Tower (CT)	centralized	cellular towers	1
User+User'sfriends+LBS Server	distributed	no	1
User-centric architecture	distributed	yes	1
IoT devices+ obfuscation engine + LBS	centralized	no	1
nodes +access points (AP) +report server (RS)+App. Server (AS)	distributed	no	1
users+location Anonymizer +LBS	distributed	no	1
User + LBS Server +Base Station +Satellites	distributed	trusted hardware	1
User+AP	distributed	no	1
user+Anonymizer+Function Generator+ LBS	centralized	Semi trusted	1
user+Annonymizer+Converter+LBS Sever	centralized	Semi trusted	1

Scheme Architecture Synthesis – Continued on next page

Continued from previous page

Architecture	**Category**	**TTP**	**no.Studies**
User+OSN Server+LBS Server	centralized	Semi trusted	1
user+Pseudonym Identity Server+ LBS Server	centralized	no	1
User+semiTTP+Provider	distributed	Semi trusted	1
User+Social Network Server+Beacons	distributed	no	1
User+TTP+LBS	centralized	TTP	1
Users+CS+LBS	centralized	CS	1
users+ online social network server +LBS server and multiple location servers (MLS) implementation	distributed	no	1
Users+CA +Plataform Server	centralized	PS	1
Users+Access Point+Operator	distributed	no	1
Users+Fog server+LBS server	distributed	no	1
Users+LBS server	distributed	Semi trusted	1
users+service providers+ query servers	distributed	semi QS	1
Implementation dependant or not informed			17

Table 3.4: Scheme Architecture Synthesis

Chapter 4

Conclusions and future work

In conclusion to this work, some important issues need to be addressed. The understanding of the topic achieved from the summary and discussions and the implications of the summarised information to the research field.

It should start with the definition of location privacy which in some studies means only position, but for other studies position and its traces. The definition interferes how the mechanisms will be design. Regarding location privacy as only positional it will restrict the protection to just snapshot queries. However, most of the system operates using continuous queries and deals with moving objects not solely episodic position. Most of the algorithm deals with snapshot query instead of continuous query.

Regarding to the trend identified, the artefacts proposed are avoiding the centralised architecture with trusted entities design. The experiments run and the results achieved are promising regarding the tradeoff between the QoS and utility. Other trend identified is the user centric paradigm giving the user the control of its privacy.

Nevertheless, the privacy preserving technologies need to move towards to privacy aware system paradigm where privacy is part of the system design in early stages of the development. It is known that the structures and architectures that provide privacy preserving as an additional feature coupled but not part of the system it has been shown less effective. How difficult is patch and add layers to protect privacy if the systems and architectures were not devised for its purpose. The adoption of the principles of the privacy by design could help on this matter.

On need arose from this investigation the development and standardisation of metric to evaluate privacy, the need to create benchmarks to be applied by the industry and

developers. The metrics used to evaluate privacy is known already by its limitations, but they are the only existing ones to perform the task. Besides the privacy levels, there is a need to evaluate and measure the background knowledge and discovery success of an adversary in order to improve the adversary models and have a meaningful risk assessment regarding privacy.

Some definitions and premises arose as not realistic and acceptable anymore such as an assumption of an honest behaviour on behalf of system entities and the consideration of only external threats to the system.

One important thing to push a change in the business model of some companies is the paradigm of Personal/Locational Data ownership, the data belong to the user not the Services or Companies. This type of protection need to be enabled by law and need enforcement.

Some developers are not taking into account the physical constraints and urban structures on the schemes/systems design, just the theoretical ones. Considering solely Euclidean space in the measurements. There are some which are still relying on trusted third parties, not considering continuous queries nor a potential background knowledge of an adversary. The most challenging are the protect against continuous queries and even more challenging is to measure the background knowledge of an attacker. Some other challenges are: i) Usage of non encrypted communication; ii)Improvements in the trade-off between quality of service and locational privacy; iii)Combination of regulation and business models; iv)dataveillance; v)Accountability versus privacy; vi)Client-side costs and overhead in decentralised architectures;

For further investigations the regulation dimension of the theme will be more detailed, verifying the compliance to the GDPR and other data regulations. Along with the regulation the principles of the privacy by design and by default will be more deeply assessed and discussed.

References

1. *ACM Library* (2018). URL: https://dl.acm.org/ (visited on 12/03/2018).

2. Aïvodji, U. M., S. Gambs, M.-J. Huguet, and M.-O. Killijian (2016). "Meeting points in ridesharing: A privacy-preserving approach". In: *Transportation Research Part C: Emerging Technologies* 72, pp. 239–253. ISSN: 0968-090X. DOI: https://doi.org/10.1016/j.trc.2016.09.017. URL: http://www.sciencedirect.com/science/article/pii/S0968090X1630184X.

3. Asuquo, P., H. Cruickshank, J. Morley, C. P. A. Ogah, A. Lei, W. Hathal, S. Bao, and Z. Sun (2018). "Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges and Countermeasures". In: *IEEE Internet of Things Journal*, pp. 1–1. ISSN: 2327-4662. DOI: 10.1109/JIOT.2018.2820039.

4. Basili, V. R., F. Shull, and F. Lanubile (1999). "Building knowledge through families of experiments". In: *IEEE Transactions on Software Engineering* 25.4, pp. 456–473. ISSN: 0098-5589. DOI: 10.1109/32.799939.

5. Beresford, A. R. and F. Stajano (2003). "Location Privacy in Pervasive Computing". In: *IEEE Pervasive Computing* 2, pp. 46–55. ISSN: 1536-1268. DOI: 10.1109/MPRV.2003.1186725. URL: doi.ieeecomputersociety.org/10.1109/MPRV.2003.1186725.

6. Bettini, C. and D. Riboni (2015). "Privacy protection in pervasive systems: State of the art and technical challenges". In: *Pervasive and Mobile Computing* 17. 10 years of Pervasive Computing' In Honor of Chatschik Bisdikian, pp. 159–174. ISSN: 1574-1192. DOI: https://doi.org/10.1016/j.pmcj.2014.09.010. URL: http://www.sciencedirect.com/science/article/pii/S1574119214001631.

7. *Biblioteca do Conhecimento Online – b-on* (2018). URL: https://www.b-on.pt/en/ (visited on 12/03/2018).

8. Biolchini, J., P. G. Mian, A. C. C. Natali, and G. H. Travassos (2005). *Systematic Literature Review in Software Engineering*. Technical Report RT-ES679/05. Rio de Janeiro: Universidade Federal do Rio de Janeiro, p. 31.

9. Birnhack, M. D. (2011). “A QUEST FOR A THEORY OF PRIVACY: CONTEXT AND CONTROL”. In: *Jurimetrics* 51.4, pp. 447–479. ISSN: 08971277, 21544344. URL: http://www.jstor.org/stable/41307137.

10. Bouguettaya, A. R. A. and M. Y. Eltoweissy (2003). “Privacy on the Web: facts, challenges, and solutions”. In: *IEEE Security Privacy* 99.6, pp. 40–49. ISSN: 1540-7993. DOI: 10.1109/MSECP.2003.1253567.

11. Brereton, P., B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil (Apr. 1, 2007). “Lessons from applying the systematic literature review process within the software engineering domain”. In: *Journal of Systems and Software* 80.4, pp. 571–583. ISSN: 0164-1212. DOI: 10.1016/j.jss.2006.07.009. URL: http://www.sciencedirect.com/science/article/pii/S016412120600197X.

12. Carver, J. C., M. Burcham, S. A. Kocak, A. Bener, M. Felderer, M. Gander, J. King, J. Markkula, M. Oivo, C. Sauerwein, and L. Williams (2016). “Establishing a Baseline for Measuring Advancement in the Science of Security: An Analysis of the 2015 IEEE Security & Privacy Proceedings”. In: *Proceedings of the Symposium and Bootcamp on the Science of Security*. HotSos ’16. Pittsburgh, Pennsylvania: ACM, pp. 38–51. ISBN: 978-1-4503-4277-3. DOI: 10.1145/2898375.2898380. URL: http://doi.acm.org/10.1145/2898375.2898380.

13. Chi, Z., Y. Wang, Y. Huang, and X. Tong (2018). “The Novel Location Privacy-Preserving CKD for Mobile Crowdsourcing Systems”. In: *IEEE Access* 6, pp. 5678–5687. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2783322.

14. Chunguang, M., Z. Changli, and Y. Songtao (2015). “A Voronoi-Based Location Privacy-Preserving Method for Continuous Query in LBS”. In: *International Journal of Distributed Sensor Networks* 11.3, p. 326953. DOI: 10.1155/2015/326953. eprint: https://doi.org/10.1155/2015/326953. URL: https://doi.org/10.1155/2015/326953.

15. *dblp* (2018). URL: https://dblp.uni-trier.de/ (visited on 12/03/2018).

16. Dey, A. (Feb. 2001). “Understanding and Using Context”. In: *Personal and Ubiquitous Computing* 5, pp. 4–7. DOI: 10.1007/s007790170019.

17. Al-Dhubhani, R. and J. M. Cazalas (2018). "An adaptive geo-indistinguishability mechanism for continuous LBS queries". In: *Wireless Networks* 24.8, pp. 3221–3239. ISSN: 1572-8196. DOI: 10.1007/s11276-017-1534-x. URL: https://doi.org/10.1007/s11276-017-1534-x.

18. Dimitriou, T. and N. A. Ibrahim (2018). ""I wasn't there"—Deniable, privacy-aware scheme for decentralized Location-based Services". In: *Future Generation Computer Systems* 86, pp. 253–265. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2018.04.004. URL: http://www.sciencedirect.com/science/article/pii/S0167739X17304491.

19. Dwork, C. (2006). "Differential Privacy". In: *Automata, Languages and Programming*. Ed. by M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1–12. ISBN: 978-3-540-35908-1.

20. Dybå, T. and T. Dingsøyr (2008). "Strength of Evidence in Systematic Reviews in Software Engineering". In: *Proceedings of the Second ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*. ESEM '08. Kaiserslautern, Germany: ACM, pp. 178–187. ISBN: 978-1-59593-971-5. DOI: 10.1145/1414004.1414034. URL: http://doi.acm.org/10.1145/1414004.1414034.

21. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" (2016). In: *Official Journal of the European Union* L119, pp. 1–88. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.

22. Fang, W., X. Z. Wen, Y. Zheng, and M. Zhou (2017). "A Survey of Big Data Security and Privacy Preserving". In: *IETE Technical Review* 34.5, pp. 544–560. DOI: 10.1080/02564602.2016.1215269. eprint: https://doi.org/10.1080/02564602.2016.1215269. URL: https://doi.org/10.1080/02564602.2016.1215269.

23. Felizardo, K. R., G. F. Andery, J. C. Maldonado, and R. Minghim (2009). "Uma Abordagem Visual para Auxiliar a Revisão da Seleção de Estudos Primários na Revisão Sistemática". In: *Proceedings of 6th Experimental Software Engineering Latin American Workshop*. ESELAW09 -VI Experimental Software Engineering Latin American Worksh op. São Carlos, SP - Brazil, pp. 83–92. ISBN: 978-85-99673-03-4.

24. Freudiger, J. (2015). "How Talkative is Your Mobile Device?: An Experimental Study of Wi-Fi Probe Requests". In: *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. WiSec '15. New York, New York: ACM, 8:1–8:6. ISBN: 978-1-4503-3623-9. DOI: 10.1145/2766498.2766517. URL: http://doi.acm.org/10.1145/2766498.2766517.

25. Gao, S., J. Ma, W. Shi, and G. Zhan (2015). "LTPPM: a location and trajectory privacy protection mechanism in participatory sensing". In: *Wireless Communications and Mobile Computing* 15.1, pp. 155–169. DOI: 10.1002/wcm.2324. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/wcm.2324. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.2324.

26. Garousi, V., M. Felderer, and M. Mäntylä (2017). *Guidelines for including the grey literature and conducting multivocal literature reviews in software engineering*.

27. Greenhalgh, T. and R. Peacock (2005). "Effectiveness and Efficiency of Search Methods in Systematic Reviews of Complex Evidence: Audit of Primary Sources". In: *BMJ (Clinical research ed.)* 331, pp. 1064–5. DOI: 10.1136/bmj.38636.593461.68.

28. Han, M., J. Li, Z. Cai, and Q. Han (2016). "Privacy Reserved Influence Maximization in GPS-Enabled Cyber-Physical and Online Social Networks". In: *2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom)*, pp. 284–292. DOI: 10.1109/BDCloud-SocialCom-SustainCom.2016.51.

29. Han, M., J. Wang, M. Yan, C. Ai, Z. Duan, and Z. Hong (2018). "Near-Complete Privacy Protection: Cognitive Optimal Strategy in Location-Based Services". In: *Procedia Computer Science* 129. 2017 INTERNATIONAL CONFERENCE ON IDENTIFICATION,INFORMATION AND KNOWLEDGEIN THE INTERNET OF THINGS,

pp. 298–304. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2018.03.079. URL: http://www.sciencedirect.com/science/article/pii/S1877050918303041.

30. Hara, T., A. Suzuki, M. Iwata, Y. Arase, and X. Xie (2016). "Dummy-Based User Location Anonymization Under Real-World Constraints". In: *IEEE Access* 4, pp. 673–687. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2016.2526060.

31. He, D., S. Chan, and M. Guizani (2015). "User privacy and data trustworthiness in mobile crowd sensing". In: *IEEE Wireless Communications* 22.1, pp. 28–34. ISSN: 1536-1284. DOI: 10.1109/MWC.2015.7054716.

32. Herrmann, M. (2016). "Privacy in Location-Based Services". PhD thesis. Leuven, Belgium: KU Leuven – Faculty of Engineering Science. 255 pp.

33. Heurix, J., P. Zimmermann, T. Neubauer, and S. Fenz (2015). "A taxonomy for privacy enhancing technologies". In: *Computers Security* 53, pp. 1–17. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2015.05.002. URL: http://www.sciencedirect.com/science/article/pii/S0167404815000668.

34. Higgins, J. and S. Green (2011). *Cochrane Handbook for Systematic Reviews of Interventions Version 5.1.0*. updated March 2011. The Cochrane Collaboration. URL: www.handbook.cochrane.org.

35. Huang, Y., Z. Cai, and A. G. Bourgeois (2018). "Search locations safely and accurately: A location privacy protection algorithm with accurate service". In: *Journal of Network and Computer Applications* 103, pp. 146–156. ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2017.12.002. URL: http://www.sciencedirect.com/science/article/pii/S1084804517303983.

36. *IEEExplorer* (2018). URL: https://ieeexplore.ieee.org/Xplore/home.jsp.

37. J. Adams, R., P. Smart, and A. Huff (2016). "Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies". In: *International Journal of Management Reviews* In press. DOI: 10.1111/ijmr.12102.

38. Jin, L., C. Li, B. Palanisamy, and J. Joshi (2018). "k-Trustee: Location injection attack-resilient anonymization for location privacy". In: *Computers Security* 78, pp. 212–230. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2018.07.002. URL: http://www.sciencedirect.com/science/article/pii/S0167404818305200.

39. Kanellis, P. and T. Papadopoulos (2008). "Conducting research in information systems: An epistemological journey". In: *Information Systems Research Methods, Epistemology, and Applications*, pp. 1–34. DOI: 10.4018/978-1-60566-040-0.ch001.

40. Kitchenham, B. A. (2004). *Procedures for Undertaking Systematic Reviews*. Joint Technical Report, Computer Science Department, Keele University (TR/SE-0401) and National ICT Australia Ltd (0400011T.1).

41. — (2007). *Guidelines for performing Systematic Literature Reviews in software engineering. EBSE Technical Report EBSE-2007-01.*

42. Kitchenham, B. A., D. Budgen, and O. P. Brereton (2011). "Using mapping studies as the basis for further research – A participant-observer case study". In: *Information and Software Technology* 53.6. Special Section: Best papers from the APSEC, pp. 638–651. ISSN: 0950-5849. DOI: https://doi.org/10.1016/j.infsof.2010.12.011. URL: http://www.sciencedirect.com/science/article/pii/S0950584910002272.

43. Konstantinidis, A., G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, and Y. Theodoridis (2015). "Privacy-Preserving Indoor Localization on Smartphones". In: *IEEE Transactions on Knowledge and Data Engineering* 27.11, pp. 3042–3055. ISSN: 1041-4347. DOI: 10.1109/TKDE.2015.2441724.

44. Kounadi, O. and M. Leitner (2014). "Why Does Geoprivacy Matter? The Scientific Publication of Confidential Data Presented on Maps". In: *Journal of Empirical Research on Human Research Ethics* 9.4, pp. 34–45. DOI: 10.1177/1556264614544103.

45. L. Feng, Y. K. Chiam, and S. K. Lo (2017). "Text-Mining Techniques and Tools for Systematic Literature Reviews: A Systematic Literature Review". In: *2017 24th Asia-Pacific Software Engineering Conference (APSEC)*. 2017 24th Asia-Pacific Software Engineering Conference (APSEC), pp. 41–50. DOI: 10.1109/APSEC.2017.10.

46. Lacerda, D. P., A. Dresch, A. ProenÃ, and J. V. Antunes JÃ (2013). "Design Science Research: mÃde pesquisa para a engenharia de produÃ§Ã". pt. In: *GestÃ ProduÃ§Ã* 20, pp. 741–761. ISSN: 0104-530X. URL: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-530X2013000400001&nrm=iso.

47. Lahe, A. D. and P. Kulkarni (2017). "Location privacy preserving using semi-TTP server for LBS users". In: *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, pp. 605–610. DOI: 10.1109/RTEICT.2017.8256668.

48. Li, J., H. Yan, Z. Liu, X. Chen, X. Huang, and D. S. Wong (2017). "Location-Sharing Systems With Enhanced Privacy in Mobile Online Social Networks". In: *IEEE Systems Journal* 11.2, pp. 439–448. ISSN: 1932-8184. DOI: 10.1109/JSYST.2015.2415835.

49. Li, L., R. Lu, and C. Huang (2016). "EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data". In: *IEEE Internet of Things Journal* 3.2, pp. 206–218. ISSN: 2327-4662. DOI: 10.1109/JIOT.2015.2469605.

50. Li, X., C. Zhang, T. Jung, J. Qian, and L. Chen (2016). "Graph-based privacy-preserving data publication". In: *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9. DOI: 10.1109/INFOCOM.2016.7524584.

51. Long, J., A. Liu, M. Dong, and Z. Li (2015). "An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing". In: *Journal of Parallel and Distributed Computing* 81-82, pp. 47–65. ISSN: 0743-7315. DOI: https://doi.org/10.1016/j.jpdc.2015.04.003. URL: http://www.sciencedirect.com/science/article/pii/S0743731515000660.

52. Ma, T., J. Jia, Y. Xue, Y. Tian, A. Al-Dhelaan, and M. Al-Rodhaan (2018). "Protection of location privacy for moving kNN queries in social networks". In: *Applied Soft Computing* 66, pp. 525–532. ISSN: 1568-4946. DOI: https://doi.org/10.1016/j.asoc.2017.08.027. URL: http://www.sciencedirect.com/science/article/pii/S1568494617305094.

53. Memon, I., Q. A. Arain, A. Zubedi, and F. A. Mangi (2017). "DPMM: dynamic pseudonym-based multiple mix-zones generation for mobile traveler". In: *Multimedia Tools and Applications* 76.22, pp. 24359–24388. ISSN: 1573-7721. DOI: 10.1007/s11042-016-4154-z. URL: https://doi.org/10.1007/s11042-016-4154-z.

54. Moher, D., L. Shamseer, M. Clarke, D. Ghersi, A. Liberati, M. Petticrew, P. Shekelle, L. A. Stewart, and PRISMA-P Group (2015). "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement". In: *Systematic Reviews* 4.1, p. 1. ISSN: 2046-4053. DOI: 10.1186/2046-4053-4-1. URL: https://doi.org/10.1186/2046-4053-4-1.

55. Montazeri, Z., A. Houmansadr, and H. Pishro-Nik (2017). "Achieving Perfect Location Privacy in Wireless Devices Using Anonymization". In: *IEEE Transactions on Information Forensics and Security* 12.11, pp. 2683–2698. ISSN: 1556-6013. DOI: 10.1109/TIFS.2017.2713341.

56. Moritz, M. (June 2018). *China is winning the global tech race*. Newspaper. URL: https://www.ft.com/content/3530f178-6e50-11e8-8863-a9bb262c5f53 (visited on 02/12/2019).

57. Niu, B., X. Zhu, W. Li, H. Li, Y. Wang, and Z. Lu (2015). "A personalized two-tier cloaking scheme for privacy-aware location-based services". In: *2015 International Conference on Computing, Networking and Communications (ICNC)*, pp. 94–98. DOI: 10.1109/ICCNC.2015.7069322.

58. Niu, B., X. Zhu, Q. Li, J. Chen, and H. Li (2015). "A novel attack to spatial cloaking schemes in location-based services". In: *Future Generation Computer Systems* 49, pp. 125–132. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2014.10.026. URL: http://www.sciencedirect.com/science/article/pii/S0167739X14002209.

59. Oksanen, J., C. Bergman, J. Sainio, and J. Westerholm (2015). "Methods for deriving and calibrating privacy-preserving heat maps from mobile sports tracking application data". In: *Journal of Transport Geography* 48, pp. 135–144. ISSN: 0966-6923. DOI: https://doi.org/10.1016/j.jtrangeo.2015.09.001. URL: http://www.sciencedirect.com/science/article/pii/S0966692315001647.

60. Palanisamy, B. and L. Liu (2015). "Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms". In: *IEEE Transactions on Mobile Computing* 14.3, pp. 495–508. ISSN: 1536-1233. DOI: 10.1109/TMC.2014.2321747.

61. Peng, T., Q. Liu, and G. Wang (2017). "Enhanced Location Privacy Preserving Scheme in Location-Based Services". In: *IEEE Systems Journal* 11.1, pp. 219–230. ISSN: 1932-8184. DOI: 10.1109/JSYST.2014.2354235.

62. Peng, T., Q. Liu, D. Meng, and G. Wang (2017). "Collaborative trajectory privacy preserving scheme in location-based services". In: *Information Sciences* 387, pp. 165–179. ISSN: 0020-0255. DOI: https://doi.org/10.1016/j.ins.2016.08.010. URL: http://www.sciencedirect.com/science/article/pii/S0020025516305801.

63. Petersen, K., R. Feldt, S. Mujtaba, and M. Mattsson (2008). "Systematic Mapping Studies in Software Engineering". In: *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering*. EASE'08. Italy: BCS Learning & Development Ltd., pp. 68–77. URL: http://dl.acm.org/citation.cfm?id=2227115.2227123.

64. Pfitzmann, A. and M. Hansen (2010). "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management". In: *URL: http://dud. inf. tu-dresden. de/literatur/Anon$_T$erminology$_v$0* 34.

65. Pickard, L. M., B. A. Kitchenham, and P. W. Jones (1998). "Combining empirical results in software engineering". In: *Information and Software Technology* 40.14, pp. 811–821. ISSN: 0950-5849. DOI: https://doi.org/10.1016/S0950-5849(98)00101-3. URL: http://www.sciencedirect.com/science/article/pii/S0950584998001013.

66. Rios, R., J. Cuellar, and J. Lopez (2015). "Probabilistic receiver-location privacy protection in wireless sensor networks". In: *Information Sciences* 321. Security and privacy information technologies and applications for wireless pervasive computing environments, pp. 205–223. ISSN: 0020-0255. DOI: https://doi.org/10.1016/j.ins.2015.01.016. URL: http://www.sciencedirect.com/science/article/pii/S0020025515000547.

67. Rosenberger, P. and D. Gerhard (2018). "Context-awareness in industrial applications: definition, classification and use case". In: *Procedia CIRP* 72. 51st CIRP Conference on Manufacturing Systems, pp. 1172–1177. ISSN: 2212-8271. DOI: https://doi.org/10.1016/j.procir.2018.03.242. URL: http://www.sciencedirect.com/science/article/pii/S2212827118304128.

68. Russo, M. W. (2007). "How to Review a Meta-analysis". In: *Gastroenterology & hepatology* 3.8, pp. 637–642. ISSN: 1554-7914. URL: https://www.ncbi.nlm.nih.gov/pubmed/21960873.

69. Schlegel, R., C. Chow, Q. Huang, and D. S. Wong (2015). "User-Defined Privacy Grid System for Continuous Location-Based Services". In: *IEEE Transactions on Mobile Computing* 14.10, pp. 2158–2172. ISSN: 1536-1233. DOI: 10.1109/TMC.2015.2388488.

70. *Scopus Library* (2018). URL: https://www.scopus.com/search/ (visited on 12/03/2018).

71. Seidl, D. E., P. Jankowski, and M.-H. Tsou (2016). "Privacy and Spatial Pattern Preservation in Masked GPS Trajectory Data". In: *Int. J. Geogr. Inf. Sci.* 30.4, pp. 785–800. ISSN: 1365-8816. DOI: 10.1080/13658816.2015.1101767. URL: http://dx.doi.org/10.1080/13658816.2015.1101767.

72. Shahid, A. R., L. Jeukeng, W. Zeng, N. Pissinou, S. S. Iyengar, S. Sahni, and M. Varela-Conover (2017). "PPVC: Privacy Preserving Voronoi Cell for location-based services". In: *2017 International Conference on Computing, Networking and Communications (ICNC)*, pp. 351–355. DOI: 10.1109/ICCNC.2017.7876153.

73. Shokri, R. (2013). "Quantifying and Protecting Location Privacy". PhD thesis. LAUSANNE: ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE. 79 pp.

74. Shokri, R., G. Theodorakopoulos, J.-Y. L. Boudec, and J.-P. Hubaux (2011). "Quantifying Location Privacy". In: IEEE Symposium on Security and Privacy. Oakland, CA, USA, pp. 247–262. DOI: DOI10.1109/SP.2011.18.

75. Solove, D. J. (2006). "A taxonomy of privacy". In: *University of Pennsylvania Law Review* 154, pp. 477–564.

76. Sun, G., V. Chang, M. Ramachandran, Z. Sun, G. Li, H. Yu, and D. Liao (2017). "Efficient location privacy algorithm for Internet of Things (IoT) services and applications". In: *Journal of Network and Computer Applications* 89. Emerging Services for Internet of Things (IoT), pp. 3–13. ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2016.10.011. URL: http://www.sciencedirect.com/science/article/pii/S1084804516302429.

77. Sun, G., D. Liao, H. Li, H. Yu, and V. Chang (2017). "L2P2: A location-label based approach for privacy preserving in LBS". In: *Future Generation Computer Systems* 74, pp. 375–384. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2016.08.023. URL: http://www.sciencedirect.com/science/article/pii/S0167739X16302953.

78. Sun, G., Y. Xie, D. Liao, H. Yu, and V. Chang (2017). "User-defined privacy location-sharing system in mobile online social networks". In: *Journal of Network and Computer Applications* 86. Special Issue on Pervasive Social Networking, pp. 34–45. ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2016.11.024. URL: http://www.sciencedirect.com/science/article/pii/S1084804516302934.

79. Sun, Y., M. Chen, L. Hu, Y. Qian, and M. M. Hassan (2017). "ASA: Against statistical attacks for privacy-aware users in Location Based Service". In: *Future Generation Computer Systems* 70, pp. 48–58. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2016.06.017. URL: http://www.sciencedirect.com/science/article/pii/S0167739X16302023.

80. Tavani, H. and J. Moor (2001). "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies". In: *ACM Sigcas Computers and Society* 31, pp. 6–11. DOI: 10.1145/572277.572278.

81. Terrovitis, M., G. Poulis, N. Mamoulis, and S. Skiadopoulos (2017). "Local Suppression and Splitting Techniques for Privacy Preserving Publication of Trajectories". In: *IEEE Transactions on Knowledge and Data Engineering* 29.7, pp. 1466–1479. ISSN: 1041-4347. DOI: 10.1109/TKDE.2017.2675420.

82. To, H., C. Shahabi, and L. Xiong (2018). "Privacy-Preserving Online Task Assignment in Spatial Crowdsourcing with Untrusted Server". In: *2018 IEEE 34th International Conference on Data Engineering (ICDE)*, pp. 833–844.

83. Ullah, I., M. A. Shah, A. Wahid, A. Mehmood, and H. Song (2018). "ESOT: a new privacy model for preserving location privacy in Internet of Things". In: *Telecommunication Systems* 67.4, pp. 553–575. ISSN: 1572-9451. DOI: 10.1007/s11235-017-0352-x. URL: https://doi.org/10.1007/s11235-017-0352-x.

84. Uzun, B. and B. Tekinerdogan (2018). "Model-driven architecture based testing: A systematic literature review". In: *Information and Software Technology* 102, pp. 30–48. ISSN: 0950-5849. DOI: 10.1016/j.infsof.2018.05.004. URL: http://www.sciencedirect.com/science/article/pii/S0950584918300880.

85. Wang, J., Z. Cai, Y. Li, D. Yang, J. Li, and H. Gao (2018). "Protecting query privacy with differentially private k-anonymity in location-based services". In: *Personal and Ubiquitous Computing* 22.3, pp. 453–469. ISSN: 1617-4917. DOI: 10.1007/s00779-018-1124-7. URL: https://doi.org/10.1007/s00779-018-1124-7.

86. Wang, J., R. Zhu, S. Liu, and Z. Cai (2018). "Node Location Privacy Protection Based on Differentially Private Grids in Industrial Wireless Sensor Networks". In: *Sensors* 18.2. ISSN: 1424-8220. DOI: 10.3390/s18020410. URL: http://www.mdpi.com/1424-8220/18/2/410.

87. Wang, S., Q. Hu, Y. Sun, and J. Huang (2018). "Privacy Preservation in Location-Based Services". In: *IEEE Communications Magazine* 56.3, pp. 134–140. ISSN: 0163-6804. DOI: 10.1109/MCOM.2018.1700288.

88. Wang, T., J. Zeng, M. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong (2017). "Trajectory Privacy Preservation Based on a Fog Structure for Cloud Location Services". In: *IEEE Access* 5, pp. 7692–7701. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2698078.

89. Wang, Y., D. Xu, and F. Li (2016). "Providing location-aware location privacy protection for mobile location-based services". In: *Tsinghua Science and Technology* 21.3, pp. 243–259. ISSN: 1007-0214. DOI: 10.1109/TST.2016.7488736.

90. Wang, Y., Z. Cai, Z. Chi, X. Tong, and L. Li (2018). "A differentially k-anonymity-based location privacy-preserving for mobile crowdsourcing systems". In: *Procedia Computer Science* 129. 2017 INTERNATIONAL CONFERENCE ON IDENTIFICATION,INFORMATION AND KNOWLEDGEIN THE INTERNET OF THINGS, pp. 28–34. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2018.03.040. URL: http://www.sciencedirect.com/science/article/pii/S1877050918302618.

91. Wang, Y., Z. Cai, X. Tong, Y. Gao, and G. Yin (2018). "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems". In: *Computer Networks* 135, pp. 32–43. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2018.02.008. URL: http://www.sciencedirect.com/science/article/pii/S1389128618300756.

92. Weiwei, N., G. Mingzhu, and C. Xiao (2016). "Location privacy-preserving k nearest neighbor query under user's preference". In: *Knowledge-Based Systems* 103, pp. 19–27. ISSN: 0950-7051. DOI: https://doi.org/10.1016/j.knosys.2016.03.016. URL: http://www.sciencedirect.com/science/article/pii/S0950705116300089.

93. Wernke, M., P. Skvortsov, F. Dürr, and K. Rothermel (2014). "A Classification of Location Privacy Attacks and Approaches". In: *Personal Ubiquitous Computing* 18.1, pp. 163–175. ISSN: 1617-4909. DOI: 10.1007/s00779-012-0633-z. URL: http://dx.doi.org/10.1007/s00779-012-0633-z.

94. Westin, A. F. (1967). *Privacy and Freedom*. English. Ig Publishing. ISBN: 1-935439-97-9.

95. Wightman, P., A. Santander Mercado, D. J. Molinares, M. Jimeno, and M. Labrador (2015). "Tis-Bad: A Time Series-Based Deobfuscation Algorithm". In: *Investigación en Innovación en las Ingeneirías* 3, p. 1. DOI: 10.17081/invinno.3.1.2035.

96. Xiao, X., C. Chen, A. Kumar Sangaiah, G. Hu, R. Ye, and Y. Jiang (2018). "CenLocShare: A centralized privacy-preserving location-sharing system for mobile online social networks". In: *Future Generation Computer Systems* 86, pp. 863–872. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2017.01.035. URL: http://www.sciencedirect.com/science/article/pii/S0167739X17301723.

97. Ye, A., Q. Chen, L. Xu, and W. Wu (2018). "The flexible and privacy-preserving proximity detection in mobile social network". In: *Future Generation Computer Systems* 79, pp. 271–283. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2016.12.012. URL: http://www.sciencedirect.com/science/article/pii/S0167739X16307518.

98. Ye, A., Y. Li, and L. Xu (2017). "A novel location privacy-preserving scheme based on l-queries for continuous LBS". In: *Computer Communications* 98, pp. 1–10. ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2016.06.005. URL: http://www.sciencedirect.com/science/article/pii/S0140366416302560.

99. Yi, X., R. Paulet, E. Bertino, and V. Varadharajan (2016). "Practical Approximate k Nearest Neighbor Queries with Location and Query Privacy". In: *IEEE Transactions on Knowledge and Data Engineering* 28.6, pp. 1546–1559. ISSN: 1041-4347. DOI: 10.1109/TKDE.2016.2520473.

100. Zhang, S., K.-K. R. Choo, Q. Liu, and G. Wang (2018). "Enhancing privacy through uniform grid and caching in location-based services". In: *Future Generation Computer Systems* 86, pp. 881–892. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2017.06.022. URL: http://www.sciencedirect.com/science/article/pii/S0167739X17312384.

101. Zhang, S., G. Wang, Q. Liu, and J. H. Abawajy (2018). "A trajectory privacy-preserving scheme based on query exchange in mobile social networks". In: *Soft Computing* 22.18, pp. 6121–6133. ISSN: 1433-7479. DOI: 10.1007/s00500-017-2676-6. URL: https://doi.org/10.1007/s00500-017-2676-6.

102. Zhang, Y., W. Tong, and S. Zhong (2016). "On Designing Satisfaction-Ratio-Aware Truthful Incentive Mechanisms for$k$-Anonymity Location Privacy". In: *IEEE Transactions on Information Forensics and Security* 11.11, pp. 2528–2541. ISSN: 1556-6013. DOI: 10.1109/TIFS.2016.2587241.

103. Zhao, P., J. Li, F. Zeng, F. Xiao, C. Wang, and H. Jiang (2018). "ILLIA: Enabling$k$-Anonymity-Based Privacy Preserving Against Location Injection Attacks in Continuous LBS Queries". In: *IEEE Internet of Things Journal* 5.2, pp. 1033–1042. ISSN: 2327-4662. DOI: 10.1109/JIOT.2018.2799545.

104. Zheng, X., Z. Cai, J. Li, and H. Gao (May 2017). "Location-privacy-aware review publication mechanism for local business service systems". In: *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9. DOI: 10.1109/INFOCOM.2017.8056976.

105. Zhu, H., F. Wang, R. Lu, F. Liu, G. Fu, and H. Li (2018). "Efficient and Privacy-Preserving Proximity Detection Schemes for Social Applications". In: *IEEE Internet of Things Journal* 5.4, pp. 2947–2957. ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2766701.

APPENDIX-A: Selected Studies

Article	Technique type	Issues Adressed
[1] Aïvodji et al. 2016	Encryption and Perturbation	Privacy preserving approach for ridesharing systems
[2] Chi et al. 2018	Anonymization	Privacy-Preserving for Mobile Crowdsourcing Systems
[3] Chunguang et al. 2015	Anonymization and Pertubation	Voronoi-Based for Continuous Query in LBS
[4] Al-Dhubhani et al. 2018	Perturbation	Adaptive noise based on the correlation level with its previous obfuscated locations
[5] Freudiger 2015	No information	Wi-Fi probe requests and privacy threat quantification
[6] Gao et al. 2015	Anonymization	Location and trajectory privacy in participatory sensing
[7] Han, J. Li, et al. 2016	Perturbation	Influence Maximization and Location privacy
[8] Han, J. Wang, et al. 2018	Perturbation	Cognitive Architecture and Differential Privacy Mechanism
[9] Hara et al. 2016	Perturbation	Dummy-Based User Location Anonymization
[10] He et al. 2015	Anonymization	Trustfulness in Mobile crowd sensing
[11] Huang et al. 2018	Perturbation	Algorithm to offer privacy protection and accuracy in LSSs
[12] Jin et al. 2018	Anonymization	location injection attacks
[13] Konstantinidis et al. 2015	Anonymization	Privacy-Preserving Indoor Localization

Continued on next page

Selected Studies – *Continued from previous page*

Article	**Technique type**	**Issues Adressed**
[14] Lahe et al. 2017	Anonymization	Semi trusted Third Party
[15] J. Li et al. 2017	Anonymization, Encryption and Perturbation	Location sharing in mobile online social networks (mOSNs)
[16] L. Li et al. 2016	Perturbation	Privacy-Preserving Location-Based Query
[17] X. Li et al. 2016	Perturbation	Privacy-preserving data publication
[18] Ma et al. 2018	Perturbation	Moving kNN queries in social networks
[19] Memon et al. 2017	Anonymization	Road traffic information
[20] Montazeri et al. 2017	Perturbation	Differential privacy-based mechanisms
[21] Niu, X. Zhu, W. Li, et al. 2015	Anonymization	Personalized spatial cloaking scheme
[22] Niu, X. Zhu, Q. Li, et al. 2015	Anonymization	Attack analysis in spatial cloaking schemes
[23] Oksanen et al. 2015	Anonymization	Privacy-preserving for data publication
[24] Palanisamy et al. 2015	Anonymization	Theoretical Limitations in mix zones and placement improvement
[25] Peng, Liu, and G. Wang 2017	Anonymization and Perturbation	Enhanced Location Privacy Preserving Scheme
[26] Peng, Liu, Meng, et al. 2017	Anonymization	Continuous queries attack
[27] Rios et al. 2015	Perturbation	Location privacy protection in wireless sensor networks
[28] Schlegel et al. 2015	Encryption	Range and Continuous queries attack
[29] Seidl et al. 2016	Anonymization and Perturbation	Obfuscation of trajectories

Continued on next page

Selected Studies – *Continued from previous page*

Article	**Technique type**	**Issues Adressed**
[30] Shahid et al. 2017	Anonymization	Privacy Preserving Voronoi Cell cloaking
[31] G. Sun, Chang, et al. 2017	Perturbation	theoretical analysis of Dummy-Location selection algorithms and proposal new algorithm
[32] G. Sun, Liao, et al. 2017	Anonymization and Perturbation	Location-label based approach for privacy preserving
[33] G. Sun, Xie, et al. 2017	Anonymization and Encryption	Query algorithm on social network server
[34] Y. Sun et al. 2017	Anonymization and Perturbation	Statistical attacks
[35] Terrovitis et al. 2017	Anonymization	Privacy Preserving Publication of Trajectories
[36] To et al. 2018	Perturbation	Privacy-Preserving Online Task Assignment
[37] Ullah et al. 2018	Perturbation	Privacy Model proposal
[38] J. Wang, Cai, et al. 2018	Anonymization and Perturbation	Query privacy with differentially private k-anonymity
[39] J. Wang, R. Zhu, et al. 2018	Perturbation	Improvements in privacy performance
[40] T. Wang et al. 2017	Perturbation	Fog computing in a decentralized architecture and obfuscation of trajectories proposal
[41] Y. Wang, Xu, et al. 2016	Anonymization	Location-aware Location Privacy Protection (L2P2) optimization
[42] Y. Wang, Cai, Chi, et al. 2018	Anonymization and Perturbation	k-anonymity-based location privacy-preserving
[43] Y. Wang, Cai, Tong, et al. 2018	Anonymization and Perturbation	Eficiency and truthfulness of mobile crowdsourcing systems
[44] Weiwei et al. 2016	Anonymization	Improve privacy performance

Continued on next page

Selected Studies – *Continued from previous page*

Article	**Technique type**	**Issues Adressed**
[45] Wightman et al. 2015	Perturbation	Evaluate the noise Based obfuscation methods
[46] Xiao et al. 2018	Perturbation and Encryption	Centralized privacy-preserving location-sharing system
[47] Ye, Chen, et al. 2018	Anonymization and Encryption	proximity detection based on the transfer of neighbour relation
[48] Ye, Y. Li, et al. 2017	Anonymization and Perturbation	Fake queries in continuous location-based services
[49] Yi et al. 2016	Anonymization and Encryption	Approximate k nearest neighbor (kNN) queries
[50] S. Zhang, Choo, et al. 2018	Anonymization and Encryption	Enhanced privacy through uniform grid and caching scheme proposal
[51] S. Zhang, G. Wang, et al. 2018	Perturbation and Encryption	applying private matching algorithm for trajectory privacy protection and overhead reduction
[52] Y. Zhang et al. 2016	Anonymization	participatory stimulation of privacy-indifferent users in the anonymity set and provision of k-anonymity location to privacy sensitive users
[53] Zhao et al. 2018	Anonymization	Location Injection Attacks in Continuous LBS Queries
[54] H. Zhu et al. 2018	Anonymization	Privacy-Preserving Proximity Detection Schemes

Selected Articles

1. Aïvodji, U. M., S. Gambs, M.-J. Huguet, and M.-O. Killijian (2016). "Meeting points in ridesharing: A privacy-preserving approach". In: *Transportation Research Part C: Emerging Technologies* 72, pp. 239–253. ISSN: 0968-090X. DOI: https://doi.org/10.1016/j.trc.2016.09.017. URL: http://www.sciencedirect.com/science/article/pii/S0968090X1630184X.

2. Chi, Z., Y. Wang, Y. Huang, and X. Tong (2018). "The Novel Location Privacy-Preserving CKD for Mobile Crowdsourcing Systems". In: *IEEE Access* 6, pp. 5678–5687. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2783322.

3. Chunguang, M., Z. Changli, and Y. Songtao (2015). "A Voronoi-Based Location Privacy-Preserving Method for Continuous Query in LBS". In: *International Journal of Distributed Sensor Networks* 11.3, p. 326953. DOI: 10.1155/2015/326953. eprint: https://doi.org/10.1155/2015/326953. URL: https://doi.org/10.1155/2015/326953.

4. Al-Dhubhani, R. and J. M. Cazalas (2018). "An adaptive geo-indistinguishability mechanism for continuous LBS queries". In: *Wireless Networks* 24.8, pp. 3221–3239. ISSN: 1572-8196. DOI: 10.1007/s11276-017-1534-x. URL: https://doi.org/10.1007/s11276-017-1534-x.

5. Freudiger, J. (2015). "How Talkative is Your Mobile Device?: An Experimental Study of Wi-Fi Probe Requests". In: *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. WiSec '15. New York, New York: ACM, 8:1–8:6. ISBN: 978-1-4503-3623-9. DOI: 10.1145/2766498.2766517. URL: http://doi.acm.org/10.1145/2766498.2766517.

6. Gao, S., J. Ma, W. Shi, and G. Zhan (2015). "LTPPM: a location and trajectory privacy protection mechanism in participatory sensing". In: *Wireless Communications and Mobile Computing* 15.1, pp. 155–169. DOI: 10.1002/wcm.2324. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/wcm.2324. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.2324.

7. Han, M., J. Li, Z. Cai, and Q. Han (2016). "Privacy Reserved Influence Maximization in GPS-Enabled Cyber-Physical and Online Social Networks". In: *2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom) (BDCloud-SocialCom-SustainCom)*, pp. 284–292. DOI: 10.1109/BDCloud-SocialCom-SustainCom.2016.51.

8. Han, M., J. Wang, M. Yan, C. Ai, Z. Duan, and Z. Hong (2018). "Near-Complete Privacy Protection: Cognitive Optimal Strategy in Location-Based Services". In: *Procedia Computer Science* 129. 2017 INTERNATIONAL CONFERENCE ON IDENTIFICATION,INFORMATION AND KNOWLEDGEIN THE INTERNET OF THINGS, pp. 298–304. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2018.03.079. URL: http://www.sciencedirect.com/science/article/pii/S1877050918303041.

9. Hara, T., A. Suzuki, M. Iwata, Y. Arase, and X. Xie (2016). "Dummy-Based User Location Anonymization Under Real-World Constraints". In: *IEEE Access* 4, pp. 673–687. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2016.2526060.

10. He, D., S. Chan, and M. Guizani (2015). "User privacy and data trustworthiness in mobile crowd sensing". In: *IEEE Wireless Communications* 22.1, pp. 28–34. ISSN: 1536-1284. DOI: 10.1109/MWC.2015.7054716.

11. Huang, Y., Z. Cai, and A. G. Bourgeois (2018). "Search locations safely and accurately: A location privacy protection algorithm with accurate service". In: *Journal of Network and Computer Applications* 103, pp. 146–156. ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2017.12.002. URL: http://www.sciencedirect.com/science/article/pii/S1084804517303983.

12. Jin, L., C. Li, B. Palanisamy, and J. Joshi (2018). "k-Trustee: Location injection attack-resilient anonymization for location privacy". In: *Computers Security* 78, pp. 212–230. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2018.07.002. URL: http://www.sciencedirect.com/science/article/pii/S0167404818305200.

13. Konstantinidis, A., G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, and Y. Theodoridis (2015). "Privacy-Preserving Indoor Localization on Smartphones". In: *IEEE Transactions on Knowledge and Data Engineering* 27.11, pp. 3042–3055. ISSN: 1041-4347. DOI: 10.1109/TKDE.2015.2441724.

14. Lahe, A. D. and P. Kulkarni (2017). "Location privacy preserving using semi-TTP server for LBS users". In: *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, pp. 605–610. DOI: 10.1109/RTEICT.2017.8256668.

15. Li, J., H. Yan, Z. Liu, X. Chen, X. Huang, and D. S. Wong (2017). "Location-Sharing Systems With Enhanced Privacy in Mobile Online Social Networks". In: *IEEE Systems Journal* 11.2, pp. 439–448. ISSN: 1932-8184. DOI: 10.1109/JSYST.2015.2415835.

16. Li, L., R. Lu, and C. Huang (2016). "EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data". In: *IEEE Internet of Things Journal* 3.2, pp. 206–218. ISSN: 2327-4662. DOI: 10.1109/JIOT.2015.2469605.

17. Li, X., C. Zhang, T. Jung, J. Qian, and L. Chen (2016). "Graph-based privacy-preserving data publication". In: *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9. DOI: 10.1109/INFOCOM.2016.7524584.

18. Ma, T., J. Jia, Y. Xue, Y. Tian, A. Al-Dhelaan, and M. Al-Rodhaan (2018). "Protection of location privacy for moving kNN queries in social networks". In: *Applied Soft Computing* 66, pp. 525–532. ISSN: 1568-4946. DOI: https://doi.org/10.1016/j.asoc.2017.08.027. URL: http://www.sciencedirect.com/science/article/pii/S1568494617305094.

19. Memon, I., Q. A. Arain, A. Zubedi, and F. A. Mangi (2017). "DPMM: dynamic pseudonym-based multiple mix-zones generation for mobile traveler". In: *Multimedia Tools and Applications* 76.22, pp. 24359–24388. ISSN: 1573-7721. DOI: 10.1007/s11042-016-4154-z. URL: https://doi.org/10.1007/s11042-016-4154-z.

20. Montazeri, Z., A. Houmansadr, and H. Pishro-Nik (2017). "Achieving Perfect Location Privacy in Wireless Devices Using Anonymization". In: *IEEE Transactions on Information Forensics and Security* 12.11, pp. 2683–2698. ISSN: 1556-6013. DOI: 10.1109/TIFS.2017.2713341.

21. Niu, B., X. Zhu, W. Li, H. Li, Y. Wang, and Z. Lu (2015). "A personalized two-tier cloaking scheme for privacy-aware location-based services". In: *2015 International Conference on Computing, Networking and Communications (ICNC)*, pp. 94–98. DOI: 10.1109/ICCNC.2015.7069322.

22. Niu, B., X. Zhu, Q. Li, J. Chen, and H. Li (2015). "A novel attack to spatial cloaking schemes in location-based services". In: *Future Generation Computer Systems* 49, pp. 125–132. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2014.10.026. URL: http://www.sciencedirect.com/science/article/pii/S0167739X14002209.

23. Oksanen, J., C. Bergman, J. Sainio, and J. Westerholm (2015). "Methods for deriving and calibrating privacy-preserving heat maps from mobile sports tracking application data". In: *Journal of Transport Geography* 48, pp. 135–144. ISSN: 0966-6923. DOI: https://doi.org/10.1016/j.jtrangeo.2015.09.001. URL: http://www.sciencedirect.com/science/article/pii/S0966692315001647.

24. Palanisamy, B. and L. Liu (2015). "Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms". In: *IEEE Transactions on Mobile Computing* 14.3, pp. 495–508. ISSN: 1536-1233. DOI: 10.1109/TMC.2014.2321747.

25. Peng, T., Q. Liu, and G. Wang (2017). "Enhanced Location Privacy Preserving Scheme in Location-Based Services". In: *IEEE Systems Journal* 11.1, pp. 219–230. ISSN: 1932-8184. DOI: 10.1109/JSYST.2014.2354235.

26. Peng, T., Q. Liu, D. Meng, and G. Wang (2017). "Collaborative trajectory privacy preserving scheme in location-based services". In: *Information Sciences* 387, pp. 165–179. ISSN: 0020-0255. DOI: https://doi.org/10.1016/j.ins.2016.08.010. URL: http://www.sciencedirect.com/science/article/pii/S0020025516305801.

27. Rios, R., J. Cuellar, and J. Lopez (2015). "Probabilistic receiver-location privacy protection in wireless sensor networks". In: *Information Sciences* 321. Security and privacy information technologies and applications for wireless pervasive computing environments, pp. 205–223. ISSN: 0020-0255. DOI: https://doi.org/10.1016/j.ins.2015.01.016. URL: http://www.sciencedirect.com/science/article/pii/S0020025515000547.

28. Schlegel, R., C. Chow, Q. Huang, and D. S. Wong (2015). "User-Defined Privacy Grid System for Continuous Location-Based Services". In: *IEEE Transactions on Mobile Computing* 14.10, pp. 2158–2172. ISSN: 1536-1233. DOI: 10.1109/TMC.2015.2388488.

29. Seidl, D. E., P. Jankowski, and M.-H. Tsou (2016). "Privacy and Spatial Pattern Preservation in Masked GPS Trajectory Data". In: *Int. J. Geogr. Inf. Sci.* 30.4, pp. 785–800. ISSN: 1365-8816. DOI: 10.1080/13658816.2015.1101767. URL: http://dx.doi.org/10.1080/13658816.2015.1101767.

30. Shahid, A. R., L. Jeukeng, W. Zeng, N. Pissinou, S. S. Iyengar, S. Sahni, and M. Varela-Conover (2017). "PPVC: Privacy Preserving Voronoi Cell for location-based services". In: *2017 International Conference on Computing, Networking and Communications (ICNC)*, pp. 351–355. DOI: 10.1109/ICCNC.2017.7876153.

31. Sun, G., V. Chang, M. Ramachandran, Z. Sun, G. Li, H. Yu, and D. Liao (2017). "Efficient location privacy algorithm for Internet of Things (IoT) services and applications". In: *Journal of Network and Computer Applications* 89. Emerging Services for Internet of Things (IoT), pp. 3–13. ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2016.10.011. URL: http://www.sciencedirect.com/science/article/pii/S1084804516302429.

32. Sun, G., D. Liao, H. Li, H. Yu, and V. Chang (2017). "L2P2: A location-label based approach for privacy preserving in LBS". In: *Future Generation Computer Systems* 74, pp. 375–384. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2016.08.023. URL: http://www.sciencedirect.com/science/article/pii/S0167739X16302953.

33. Sun, G., Y. Xie, D. Liao, H. Yu, and V. Chang (2017). "User-defined privacy location-sharing system in mobile online social networks". In: *Journal of Network and Computer Applications* 86. Special Issue on Pervasive Social Networking, pp. 34–45. ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2016.11.024. URL: http://www.sciencedirect.com/science/article/pii/S1084804516302934.

34. Sun, Y., M. Chen, L. Hu, Y. Qian, and M. M. Hassan (2017). "ASA: Against statistical attacks for privacy-aware users in Location Based Service". In: *Future Generation Computer Systems* 70, pp. 48–58. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2016.06.017. URL: http://www.sciencedirect.com/science/article/pii/S0167739X16302023.

35. Terrovitis, M., G. Poulis, N. Mamoulis, and S. Skiadopoulos (2017). "Local Suppression and Splitting Techniques for Privacy Preserving Publication of Trajectories". In: *IEEE Transactions on Knowledge and Data Engineering* 29.7, pp. 1466–1479. ISSN: 1041-4347. DOI: 10.1109/TKDE.2017.2675420.

36. To, H., C. Shahabi, and L. Xiong (2018). "Privacy-Preserving Online Task Assignment in Spatial Crowdsourcing with Untrusted Server". In: *2018 IEEE 34th International Conference on Data Engineering (ICDE)*, pp. 833–844.

37. Ullah, I., M. A. Shah, A. Wahid, A. Mehmood, and H. Song (2018). "ESOT: a new privacy model for preserving location privacy in Internet of Things". In: *Telecommunication Systems* 67.4, pp. 553–575. ISSN: 1572-9451. DOI: 10.1007/s11235-017-0352-x. URL: https://doi.org/10.1007/s11235-017-0352-x.

38. Wang, J., Z. Cai, Y. Li, D. Yang, J. Li, and H. Gao (2018). "Protecting query privacy with differentially private k-anonymity in location-based services". In: *Personal and Ubiquitous Computing* 22.3, pp. 453–469. ISSN: 1617-4917. DOI: 10.1007/s00779-018-1124-7. URL: https://doi.org/10.1007/s00779-018-1124-7.

39. Wang, J., R. Zhu, S. Liu, and Z. Cai (2018). "Node Location Privacy Protection Based on Differentially Private Grids in Industrial Wireless Sensor Networks". In: *Sensors* 18.2. ISSN: 1424-8220. DOI: 10.3390/s18020410. URL: http://www.mdpi.com/1424-8220/18/2/410.

40. Wang, T., J. Zeng, M. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong (2017). "Trajectory Privacy Preservation Based on a Fog Structure for Cloud Location Services". In: *IEEE Access* 5, pp. 7692–7701. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2698078.

41. Wang, Y., D. Xu, and F. Li (2016). "Providing location-aware location privacy protection for mobile location-based services". In: *Tsinghua Science and Technology* 21.3, pp. 243–259. ISSN: 1007-0214. DOI: 10.1109/TST.2016.7488736.

42. Wang, Y., Z. Cai, Z. Chi, X. Tong, and L. Li (2018). "A differentially k-anonymity-based location privacy-preserving for mobile crowdsourcing systems". In: *Procedia Computer Science* 129. 2017 INTERNATIONAL CONFERENCE ON IDENTIFICATION,INFORMATION AND KNOWLEDGEIN THE INTERNET OF THINGS, pp. 28–34. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2018.03.040. URL: http://www.sciencedirect.com/science/article/pii/S1877050918302618.

43. Wang, Y., Z. Cai, X. Tong, Y. Gao, and G. Yin (2018). "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems". In: *Computer Networks* 135, pp. 32–43. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2018.02.008. URL: http://www.sciencedirect.com/science/article/pii/S1389128618300756.

44. Weiwei, N., G. Mingzhu, and C. Xiao (2016). "Location privacy-preserving k nearest neighbor query under user's preference". In: *Knowledge-Based Systems* 103, pp. 19–27. ISSN: 0950-7051. DOI: https://doi.org/10.1016/j.knosys.2016.03.016. URL: http://www.sciencedirect.com/science/article/pii/S0950705116300089.

45. Wightman, P., A. Santander Mercado, D. J. Molinares, M. Jimeno, and M. Labrador (2015). "Tis-Bad: A Time Series-Based Deobfuscation Algorithm". In: *Investigación en Innovación en las Ingeneirías* 3, p. 1. DOI: 10.17081/invinno.3.1.2035.

46. Xiao, X., C. Chen, A. Kumar Sangaiah, G. Hu, R. Ye, and Y. Jiang (2018). "CenLocShare: A centralized privacy-preserving location-sharing system for mobile online social networks". In: *Future Generation Computer Systems* 86, pp. 863–872. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2017.01.035. URL: http://www.sciencedirect.com/science/article/pii/S0167739X17301723.

47. Ye, A., Q. Chen, L. Xu, and W. Wu (2018). "The flexible and privacy-preserving proximity detection in mobile social network". In: *Future Generation Computer Systems* 79, pp. 271–283. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2016.12.012. URL: http://www.sciencedirect.com/science/article/pii/S0167739X16307518.

48. Ye, A., Y. Li, and L. Xu (2017). "A novel location privacy-preserving scheme based on l-queries for continuous LBS". In: *Computer Communications* 98, pp. 1–10. ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2016.06.005. URL: http://www.sciencedirect.com/science/article/pii/S0140366416302560.

49. Yi, X., R. Paulet, E. Bertino, and V. Varadharajan (2016). "Practical Approximate k Nearest Neighbor Queries with Location and Query Privacy". In: *IEEE Transactions on Knowledge and Data Engineering* 28.6, pp. 1546–1559. ISSN: 1041-4347. DOI: 10.1109/TKDE.2016.2520473.

50. Zhang, S., K.-K. R. Choo, Q. Liu, and G. Wang (2018). "Enhancing privacy through uniform grid and caching in location-based services". In: *Future Generation Computer Systems* 86, pp. 881–892. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2017.06.022. URL: http://www.sciencedirect.com/science/article/pii/S0167739X17312384.

51. Zhang, S., G. Wang, Q. Liu, and J. H. Abawajy (2018). "A trajectory privacy-preserving scheme based on query exchange in mobile social networks". In: *Soft Computing* 22.18, pp. 6121–6133. ISSN: 1433-7479. DOI: 10.1007/s00500-017-2676-6. URL: https://doi.org/10.1007/s00500-017-2676-6.

52. Zhang, Y., W. Tong, and S. Zhong (2016). "On Designing Satisfaction-Ratio-Aware Truthful Incentive Mechanisms for$k$-Anonymity Location Privacy". In: *IEEE Transactions on Information Forensics and Security* 11.11, pp. 2528–2541. ISSN: 1556-6013. DOI: 10.1109/TIFS.2016.2587241.

53. Zhao, P., J. Li, F. Zeng, F. Xiao, C. Wang, and H. Jiang (2018). "ILLIA: Enabling$k$-Anonymity-Based Privacy Preserving Against Location Injection Attacks in Continuous LBS Queries". In: *IEEE Internet of Things Journal* 5.2, pp. 1033–1042. ISSN: 2327-4662. DOI: 10.1109/JIOT.2018.2799545.

54. Zhu, H., F. Wang, R. Lu, F. Liu, G. Fu, and H. Li (2018). "Efficient and Privacy-Preserving Proximity Detection Schemes for Social Applications". In: *IEEE Internet of Things Journal* 5.4, pp. 2947–2957. ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2766701.

APPENDIX-B: Search Strings

B-ON

Boolean/Sentence:

ABSTRACT+KEYWORDS+TITLE: (("Privacy-enhancing technologies" OR "location obfuscation" OR "spatial obfuscation" OR "geo-indistinguishability" OR "spatial cloaking" OR "location cloaking") OR ("mix-zones" AND privacy) OR ((*anonymity AND (spatial OR location) AND privacy)

Publication Date: 2015/01/01-2018/11/31

ACM Digital Library

"query": recordAbstract:(("Privacy-enhancing technologies" OR "location obfuscation" OR "spatial obfuscation" OR "geo-indistinguishability" OR "spatial cloaking" OR "location cloaking") OR ("mix-zones" AND privacy) OR ((*anonymity AND (spatial OR location) AND privacy) OR keywords.author.keyword:(("Privacy-enhancing technologies" OR "location obfuscation" OR "spatial obfuscation" OR "geo-indistinguishability" OR "spatial cloaking" OR "location cloaking") OR ("mix-zones" AND privacy) OR ((*anonymity AND (spatial OR location) AND privacy) OR acmdlTitle:(("Privacy-enhancing technologies" OR "location obfuscation" OR "spatial obfuscation" OR "geo-indistinguishability" OR "spatial cloaking" OR "location cloaking") OR ("mix-zones" AND privacy) OR ((*anonymity AND (spatial OR location) AND privacy)

"filter": "publicationYear": "gte":2015, "lte":2018 , owners.owner=HOSTED

IEEExplorer

"Privacy-enhancing technologies" OR "location obfuscation" OR "spatial obfuscation" OR "geo-indistinguishability" OR "spatial cloaking" OR "location cloaking") OR (*anonymity AND location) OR ((*anonymity AND (spatial OR location) AND privacy) Full Text and Metadata

Data de publicação: 2015-2018

dblp

Combined dblp search

"Privacy-enhancing technologies"

"location| spatial obfuscation"

"spatial | location cloaking"

(*anonymity AND (spatial | location) AND privacy "mix-zones" AND privacy

"geo-indistinguishability"

Scopus

TITLE-ABS-KEY ("location obfuscation" OR "spatial obfuscation" OR "geo-indistinguishability" OR "spatial cloaking" OR "location cloaking") OR ("mix-zones" AND privacy) AND PUBYEAR > 2014 AND PUBYEAR < 2019 Total:468 TITLE-ABS-KEY ("Privacy-enhancing technologies") AND PUBYEAR > 2014 AND PUBYEAR < 2019 Total:168 TITLE-ABS-KEY ((*anonymity AND (spatial OR location) AND privacy) AND PUBYEAR > 2014 AND PUBYEAR < 2019 Total:436

Peer reviewed journal, Search on: Abstract, Keyword and Title.

APPENDIX-C: Data Extraction Form

Information	Description
id	id
Title	Title of the study
Authors	Authors of the study
publisherDate	Publication Date
publisherYear	Publication Year
publication	Publication's Name
publisher	Publisher's Name
abstract	Abstract
citedCount	Number of citations according to the Digital Library
keywords	Keywords of the study
included	Selection status id
repository	Repository, Digital Library searched
impact_factor	Impact factor of the Journal
doi	Digital Object ID
bibtex_id	bibtex entry
country	Country of the author's Institution
language_paper	Study language
paper_type	Study Type
addressed_concern	Research Question: Addressed concern
obs_addconcern	Additional information to the concern addressed
technique_type	Technique types used, described
countermeasures	Countermeasures
threats	Locational Privacy threats
assessment_approach	How the evaluations was performed
quality_assessment	Quality Assessment within the study
architecture	Architecture
combine_technologies	Combined Technologies
sensors	Sensors

Continued on next page

Data Extraction Form – *Continued from previous page*

Information	**Description**
development_enviroment	Development Environment
operational_system	Operational System
platform	Platform
battery_consumption	Battery Consumption
localization_accuracy	Localization accuracy
network_usage	Network Usage
APIs	APIs used
complexity	Complexity of the preserving privacy algorithms
programming_language	Programming Language
solutions	Research Question: Solutions
obs_solutions	Additional information to the solutions question
research_directions	Research Question: research directions
obs_research_directions	Additional information to the research directions
tradeoff	Overheads or costs of using the techniques
obstradeoff	Additional information to the tradeoffs
metrics_signals	Evaluation measures and type of signals
obs	Additional information
sections	Sections of publication
settings	Settings of the experiments
category	Category of technology
threat_model	Threat Model or privacy risk assessment
policy	Privacy Policy
comparison	Algorithms or other schemes in comparison
Why not	Reasons for pos exclusion
artifact	Type of Design Science artifact
system_topology	Placement of the artifact in the system
constrains	Constraints to the artifact development
TTP	Existence of Trusted Third Party
aim	Aims of the locational privacy preserving mechanism
Internal x External Threats	Type of the threats related to Threat Model
QA	Check list of the quality QA criteria met (1-6)

APPENDIX-D: Search Strings Results

Selection Status	ACM	B-on	dblp	IEEExplorer	Scopus	Total
EC1	0	7	0	0	11	18
EC2	2	33	5	205	10	255
EC3	0	16	2	0	2	20
EC4	0	18	0	2	17	37
EC5	0	2	0	1	31	34
EC6	0	0	0	0	2	2
EC7	0	3	0	0	21	24
EC8	0	0	0	0	19	19
Not Included	17	118	8	38	783	964
Included	0	9	0	2	46	54
Total	19	206	15	248	939	1427

APPENDIX-E: Description of the Online Libraries

Scopus

Scopus is the largest peer-reviewed literature database containing journals, proceedings and books. *Scopus Library* 2018

B-on

Biblioteca do Conhecimento Online – b-on (Online Knowledge Library) is a digital Library maintained by the Portuguese Science, Technology and Higher Education Ministry and other Portuguese institutions via subscriptions. It provides access to References Databases and scientific publications over 16750 journals from 16 publishers. *Biblioteca do Conhecimento Online – b-on* 2018

References Database, Full Text Database, Publisher, Journals, Search engines

ACM Library

ACM Library is platform with Full-Text Collection of all ACM publications, such as: journals, conference proceedings, technical magazines, newsletters and books. The ACM has also a guide focused exclusively on the field of computing." *ACM Library* 2018

IEEExplorer

The IEEE Xplore digital library is source to access the vast material published by the IEEE (Institute of Electrical and Electronics Engineers) and its publishing partners. It provides web access from some of the world's most highly-cited publications in Information Technology field. *IEEExplorer* 2018

dblp Library

The dblp computer science bibliography is the on-line library on major computer science publications.It indexes about 40000 journal volumes, more than 38000 conference or workshop proceedings." *dblp* 2018

APPENDIX-F: Threats Addressed by Solutions

Disclosure attack

Position and trajectory disclosure

Happens when an adversary has access to historical POI as well as routings requests. If a data custodian is compromised the data is leaked.

Preference leakage

Happens when an adversary has access to historical data of uses of certain services which can lead a preferences identification. If a data custodian is compromised the data is leaked.

User identification

When an adversary has access to the PII information of an individual.

Inference attack

An adversary acquire historical statistical data from a compromised data custodian and can infer user identity, positions and trajectories.

Some specific statistical types addressed by the articles solutions are: *Location-based inference attacks*,*Long-term Statistical Attack*, *Regional Statistical Attack*, *variance-based attack*, *Statistics-based inference attacks*, *Known-sample attack*, *Inference attack*, *Correlation attack*, *Farthest POI attack*, *Access-pattern attack*.

Collusion attack, **Background knowledge attack**

It is a type of attack where the adversary has access to quasi identifier gather from commonly from different sources of information and integrate them, reverting re-identifying an individual, undermining unlinkability.

Deobfuscation attacks

It happens when an adversary is capable to reverse the mechanism of obfuscation, consequently, obtaining access to the original information.

Location injection attacks

It is a type of attack to circumvent cloaking and dummy mechanism. The adversary injected his dummies, have the information which ones are fake it is possible to identify the actual users or queries.

Homogeneity attack

An adversary can inflict this kind of attack within a k anonymity set, if the subjects contains the same quasi-identifiers and share the same sensitive attribute.

Linking attack

An adversary can inflict a linking attack on data colluding information and liking the once anonymized or pseudoanonymized data to its identity.

Tracking Attack

The adversary can reconstruct the a subject's trajectory from to the sequence of individual positions.

Some types of tracking attacks are, namely:*Location tracking*, *Sequential tracking attacks*, *Task tracing attacks*,*Traffic analysis attacks*, *Overlapping circle attack*, *Trajectory tracking attack*, *Timing and transition attacks*

Continuous Query attack

Continuous queries are moving queries over static objects, static queries over moving objects and moving queries over moving objects.

Ad targeting

According to the data collected and respective profiling, application can use this assembly of information to provide "personalized" advertisement to data subjects without requiring a prior consent for this purpose.

User profiling

Profiling, **Preference inference**

The location data can reveal the heath state, frequency of hospital/clinics visits, favourite restaurants, bar, shops. Having access of preferences information and behaviours, the adversary can clustering and classified the data subjects and create profile to a specific the purpose.

Stalking

The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.

Oxford entry

Eavesdropping

It is possible when a adversary can have access to the network, server or devices

been able to monitor the network traffic analysis, read unencrypted transitions. It is characteristics is just have access and gather information without been noticed or act.

Interference threats

Erroneous and malicious contributions

In participatory and collaborative systems a subjected purposely input wrong and inaccurate information and data.

Denial of Service attacks (DOS)

Overload a Server or service with requests beyond of the reasonable capacity, with the purpose to make it unavailable.

LBS server is hijacked

Happens when the Server is taken over by a malicious third party which depending on the level of trustworthiness and knowledge can compromised the security and privacy entity evolved with it.

Message Suppression attacks, **Fabrication attacks**, **Alteration attacks**

In systems which rely in messages transmitions between entities, such ITS, an adversaries can pose as a trusted entity and hamper the message dissemination. Beside a suppression attack, an adversary can inflict alteration or fake diffusion of messages. For that reason, mechanism of reputation are implemented, as well as revocation authorities.

Replay attacks

It is a type of network attack on which an adversary can repeat or delay a message transmition.

worms

It is a malicious implanted in low level application in hardware, like the ones in Internet of Things.

Cryptographic attacks

Ciphertext-only attack

An adversary knows a set of cipher text but he does not know which plain-text is related to each cipher text to solve the encryption problem. The objective is solve

the original message or even the key.

Known-plain text attack

An adversary knows plain-text and cipher text but he does not know which plain-text is related to each cipher text to solve the encryption problem. The objective is get the key.

APPENDIX-G: Top 10 Publication

Publication Name	No.articles	Articles
Future Generation Computer Systems	6	Ye, Chen, et al. 2018, Niu, X. Zhu, Q. Li, et al. 2015, S. Zhang, Choo, et al. 2018, G. Sun, Liao, et al. 2017, Xiao et al. 2018, Y. Sun et al. 2017
IEEE Access	3	Hara et al. 2016, T. Wang et al. 2017, Chi et al. 2018
Journal of Network and Computer Applications	3	Huang et al. 2018, G. Sun, Chang, et al. 2017, G. Sun, Xie, et al. 2017
IEEE Internet of Things Journal	3	H. Zhu et al. 2018, L. Li et al. 2016, Zhao et al. 2018
IEEE Transactions on Knowledge and Data Engineering	3	Konstantinidis et al. 2015, Terrovitis et al. 2017, Yi et al. 2016
IEEE Systems Journal	2	J. Li et al. 2017, Peng, Liu, and G. Wang 2017
IEEE Transactions on Information Forensics and Security	2	Montazeri et al. 2017, Y. Zhang et al. 2016
IEEE Transactions on Mobile Computing	2	Palanisamy et al. 2015, Schlegel et al. 2015
Information Sciences	2	Rios et al. 2015, Peng, Liu, Meng, et al. 2017
Int. Conference on Computing, Networking and Communications	2	Niu, X. Zhu, W. Li, et al. 2015, Shahid et al. 2017
Procedia Computer Science	2	Y. Wang, Cai, Chi, et al. 2018, Han, J. Wang, et al. 2018

APPENDIX-H: Techniques

Techniques	Articles
k nearest neighbor (kNN) queries	Yi et al. 2016, Weiwei et al. 2016, Ma et al. 2018, Lahe et al. 2017
Data obfuscation Noise-based	X. Li et al. 2016, Wightman et al. 2015,Al-Dhubhani et al. 2018, Seidl et al. 2016, G. Sun, Liao, et al. 2017
differential privacy	To et al. 2018,J. Wang, Cai, et al. 2018, Han, J. Wang, et al. 2018, J. Wang, R. Zhu, et al. 2018, Y. Wang, Cai, Tong, et al. 2018, Han, J. Li, et al. 2016, Chi et al. 2018, Y. Wang, Cai, Chi, et al. 2018
dummies and fake location	Hara et al. 2016, Gao et al. 2015, G. Sun, Chang, et al. 2017, J. Li et al. 2017, Xiao et al. 2018, Y. Sun et al. 2017, Rios et al. 2015, T. Wang et al. 2017, S. Zhang, G. Wang, et al. 2018
grid masking	Seidl et al. 2016
k anonymity	Palanisamy et al. 2015, S. Zhang, Choo, et al. 2018, Chi et al. 2018, Oksanen et al. 2015, Y. Wang, Xu, et al. 2016, J. Li et al. 2017, Chunguang et al. 2015, Y. Wang, Cai, Chi, et al. 2018, Peng, Liu, and G. Wang 2017, Gao et al. 2015, Y. Zhang et al. 2016, G. Sun, Liao, et al. 2017, J. Wang, Cai, et al. 2018, Niu, X. Zhu, Q. Li, et al. 2015, Chi et al. 2018, Niu, X. Zhu, W. Li, et al. 2015, Jin et al. 2018, Zhao et al. 2018, Weiwei et al. 2016, He et al. 2015, Y. Wang, Cai, Tong, et al. 2018, Konstantinidis et al. 2015, Y. Sun et al. 2017
l-anonymity	Ye, Y. Li, et al. 2017
l-diversity	Niu, X. Zhu, W. Li, et al. 2015, Jin et al. 2018, G. Sun, Liao, et al. 2017, Terrovitis et al. 2017
Markov Chain	Montazeri et al. 2017
Mix zones	Memon et al. 2017, He et al. 2015, Palanisamy et al. 2015, Al-Dhubhani et al. 2018
routing algorithms	Aïvodji et al. 2016, Han, J. Li, et al. 2016
pseudoanonymity	G. Sun, Xie, et al. 2017, G. Sun, Liao, et al. 2017
spatial cloaking	Ye, Y. Li, et al. 2017, Y. Wang, Xu, et al. 2016, Weiwei et al. 2016, Ma et al. 2018, Zhao et al. 2018, Chunguang et al. 2015, Y. Sun et al. 2017, Lahe et al. 2017, Shahid et al. 2017, Peng, Liu, Meng, et al. 2017,L. Li et al. 2016, H. Zhu et al. 2018, Huang et al. 2018
Voronoi partition	Chunguang et al. 2015

Masters Program in **Geospatial Technologies**

Supported by:
Education and Culture
ERASMUS MUNDUS