Multi-Agent Modeling of Risk-Aware and Privacy-Preserving Recommender

Systems

By

Vishnu Srivastava

A thesis

Presented to the University of Waterloo

in fulfillment of the

thesis requirement for the degree of

Master of Mathematics

in

Computer Science

Waterloo, Ontario, Canada, 2017

© (Vishnu Srivastava) 2017

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners. I understand that my thesis may be made electronically available to the public.

Abstract

Recent progress in the field of recommender systems has led to increases in the accuracy and improvements in the personalization of the recommendations [18]. These results are being achieved in general by gathering more user data and generating relevant insights from it. However, user privacy concerns are often underestimated and recommendation risks are not usually addressed. In fact, many users are not sufficiently aware of what data is collected about them and how the data is collected (e.g., whether third parties are collecting and selling their personal information).

Research in the area of recommender systems should strive towards not only achieving high accuracy of the generated recommendations but also protecting user privacy and making recommender systems aware of the user’s context, which involves user intentions and user current situation [2, 4, 5, 6, 11, 12, 14, 128]. Through research it has been established that a tradeoff is required between the accuracy, the privacy and the risks in a recommender system and that it is highly unlikely to have recommender systems completely satisfying all the context-aware and privacy-preserving requirements[30, 7]. Nonetheless, a significant attempt can be made to describe a novel modeling approach that supports designing a recommender system encompassing some of these previously mentioned requirements.

This thesis focuses a multi-agent based system model of recommender systems by introducing both privacy and risk-related abstractions into traditional recommender systems by breaking the system down into three different subsystems. Such a description of a system will be able to represent a subset of recommender systems which can be classified as both risk-aware and privacy-preserving. The applicability of the approach is illustrated by a case study involving a job recommender system in which the general design model is instantiated to represent the required domain-specific abstractions.

Acknowledgements

I would like to thank Professor Paulo Alencar, for his patience, understanding, kindness and guidance. I learned a lot while working with him and I am proud to be his student. I am thankful to Professor Daniel Berry for serving as my co-supervisor. I also thank Professor Donald Cowan and Professor Gladimir Baranoski for agreeing to read my thesis and providing me valuable feedback.

Table of Contents

AUTHOR'S DECLARATION ii

Abstract iii

Acknowledgements iv

Table of Contents v

List of Figures vii

List of Tables ix

Chapter 1 Introduction 10

1.1 Research Issue 11

1.2 Thesis Statement 11

1.3 Major Contributions 12

1.4 Thesis Organization 12

Chapter 2 Recommender Systems 15

2.1 Context-Aware Recommender Systems 15

2.2 Privacy in Recommender Systems 16

2.3 Privacy Protection 16

2.3.1 User control 16

2.4 Risk Aware Recommender Systems 17

Chapter 3 Related Work 18

3.1 Modelling Recommender Systems 18

3.2 Risk-Aware Recommender Systems 18

3.3 Privacy Preserving Recommender Systems 18

3.4 Privacy-Preserving Methodologies for Recommender Systems 20

Chapter 4 Proposed Approach 21

4.1 UML Diagrams 24

4.1.1 Activity Diagrams 24

4.1.2 Sequence Diagrams 24

4.2 Goal Model 25

4.3 Multi-agent System Model and System Description 25

4.4 Goal Models for the Subsystems 28

4.4.1 Goal Model: Data Subsystem 28

4.4.2 Goal Model: Privacy Subsystem 29

4.4.3 Goal Model: Risk Subsystem 30

4.4.4 Combined Goal Model of the System 31

4.5 Activity Models for the Subsystems 33

4.5.1 Activity Model: Data Subsystem 33

4.5.2 Activity Model: Privacy Subsystem 34

4.5.3 Activity Model: Risk Subsystem 34

4.5.4 Combined Activity Model for the System 35

4.6 Sequence Diagrams for the Subsystems 37

4.6.1 Sequence Diagrams: Data Subsystem 37

4.6.2 Sequence Diagram: Privacy Subsystem 38

4.6.3 Sequence Diagram: Risk Subsystem 40

4.6.4 Combined Sequence Diagram 40

List of Figures

[Figure 1 Conceptual Diagram of the Risk-Aware Privacy-Preserving Recommender System 21](#_Toc479244187)

[Figure 2 Proposed Steps of the Modeling Approach 21](#_Toc479244188)

[Figure 3 Combining Subsystem Goals to Achieve the System Goal 25](#_Toc479244189)

[Figure 4 Relationship model for subsystems 26](#_Toc479244190)

[Figure 5 Goal Model for the Data Agent and the Aggregator Agent 27](#_Toc479244191)

[Figure 6 Goal model for the User Privacy Agent 28](#_Toc479244192)

[Figure 7 Goal Model for the User Risk Agent and the Context Analyzer Agent 29](#_Toc479244193)

[Figure 8 System Goal Model 31](#_Toc479244194)

[Figure 9 Activity Diagram of Data Subsystem 32](#_Toc479244195)

[Figure 10 Activity diagram for the User Privacy Subsystem 33](#_Toc479244196)

[Figure 11 Activity Diagram for the Risk Subsystem 34](#_Toc479244197)

[Figure 12 Complete Activity Model of the System 35](#_Toc479244198)

[Figure 13 Data Subsystem sequence diagram 36](#_Toc479244199)

[Figure 14 Privacy Subsystem Sequence Diagram 37](#_Toc479244200)

[Figure 15 Contextual Risk Subsystem Sequence Diagram 39](#_Toc479244201)

[Figure 16 Combined Sequence Diagram 40](#_Toc479244202)

List of Tables

[Table 1 Interaction Entities proposed in [9] 46](#_Toc479241945)

[Table 2 General Dimensional Analysis of various Algorithms 67](#_Toc479241946)

# Introduction

In recent times, recommender systems (RSs) can take advantage of the semantic reasoning capabilities to overcome common limitations and improve the recommendation quality [128]. These systems uses domain properties, types and relationships to enhance user personalization. Current research in the area of RSs has focussed on context-aware RSs [18]. A context-independent representation may lose predictive power because potentially useful information from multiple contexts is not taken into account [128]. The ideal context-aware RS would, therefore, be able to reliably associate each user action with an appropriate context and effectively modify the system output for the user in that given context. The majority of existing approaches to RSs focus on recommending the most relevant content to users using contextual information and do not take into account the risk of upsetting the user by not providing accurate recommendations. However, in many applications, such as recommending personalized content, it is also important to consider the risk of upsetting the user by not being aware of the user’s situation and intentions [7]. Therefore, the performance of a RS depends in part on the degree to which it has incorporated the risk into the recommendation process. Risks in RSs can involve, for example, the possibility of disturbing or to upsetting the user, which can lead to a negative feedback from the user. With the advent of enormous amounts of personal data collection for the sake of personalization and improving recommendation quality, the focus of the current research on RSs has been shifting to privacy protection [129]. Personalization provides convenience in the user experience, and it can have a direct impact on marketing, sales, and profit. On the other hand, privacy, which is a serious concern for many users, is the price users have to pay for the convenience of RSs can provide in a world with booming information. Users normally have no choice but to trust the service provider to keep their sensitive personal profile and information safe.

## Research Issue

Since a major focus in the area of RSs has been the improvement of the accuracy of the recommendations generated by the Recommender System, there is a lack of a modelling approach for the RSs that takes into account both sufficient knowledge of the user’s context and the privacy of the users. A novel model of RSs involving both contextual risk and privacy would make things much easier for domain experts to study and advance research in the area of risk- aware and privacy-preserving RSs, thereby contributing with methods that can produce more detailed designs of such systems.

In the past few decades, collaboration of multiple teams in a large software project has become a usual path for developing large-scale software [15]. In spite of increasing adoption of collaborative software development, there is scope for a lot of improvements to fill the gap between what is needed and what has been provided today as the software development landscape changes rapidly. Multi-agent software development has emerged as a way to develop software by considering the different aspects of a software system as separate agents that working in coherence to achieve the overall goal of the system. However, although the area of multi-agent systems has experienced much growth in the last decade, there is still a need for multi-agent approaches that supports both context-aware and privacy-preserving mechanism [18].

## Thesis Statement

The aim of this research is to provide a multi-agent based system model of RSs by introducing both privacy and risk-related abstractions into traditional recommender systems. The model can support designing these systems when privacy and contextual risk related to user data and information needs to be taken into account. The applicability of the approach is illustrated by a case study involving a job recommender system in which the general design model is instantiated to represent the required domain-specific abstractions.

## Major Contributions

This research focuses on the importance of the privacy and the risk aspects of the Recommender Systems, that is, on how much a RS safeguards users’ privacy and also on how a RS addresses contextual risks.

The approach utilizes a multi-agent system model that divides the system into individual units. This breakdown of the Recommender System into small individual units enables the designers of the RS to focus on each of the small objectives that must be accomplished by the individual units in order to fulfil the overall objective of the entire system.

This approach combines two existing research areas within RSs, i.e. risk and privacy, into a unified system model. As part of this thesis, a sample case study that illustrates the applicability of the proposed in the field of job recommender systems approach is also provided.

## Thesis Organization

The thesis is divided into three parts. The first part introduces the problem addressed in the thesis, along with a survey of the RSs field that covers both risk and privacy issues, two fundamental concepts upon which this thesis is framed. The second part describes related work in the RSs literature and provides an analysis of the related design alternatives and statistical biases. It also provides a detailed discussion of the proposed approach to solve the identified issues related to existing multi-agent models. Towards the end of this part, a brief case study is provided, in which the proposed multi-agent model is used to model a job recommender system. The final part of the thesis describes conclusions and future work that can be done to extend the proposed system model. In the Appendix, a preliminary evaluation method for RSs based both the privacy and risk dimensions is discussed.

In more detail, the content of this thesis is organized as follows:

**Part I. Introduction**

**Chapter 1** In this chapter, a brief description of the current focus in the area of RS is provided, followed by the description of the issues currently faced by researchers and domain experts in the area of RSs. A thesis statement is then provided to give an idea of what this thesis is trying to achieve. This is followed by the description of the major contributions of the thesis.

**Chapter 2** provides an overview of the state of the art in the area of RSs, which includes a classification of the main types of recommendation approaches. We also describe the weaknesses of the different recommendation techniques and present a broader class of hybrid recommenders that aim to overcome these limitations. We also discuss risk and privacy issues in the RSs, and how these issues arise in these systems in the first place. The discussion is carried forward with the description of the some of the mitigating techniques that can be used to address some of the identified issues.

**Part II. The System Model**

**Chapter 3** describes some of the related research work in the field of RSs that has contributed toward the conceptualization of the proposed approach discussed in this thesis.

**Chapter 4** presents the proposed approach. In this section, a detailed description of the multi-agent system model is provided along with an explanation of different aspects of this model.

**Chapter 5** presents a case study to illustrate the applicability of the proposed approach, in which the multi-agent model is applied to a job RS. In this chapter a discussion about two previous job RSs is provided, and enhancements to these systems is provided in the form of a new multi-agent model for risk-aware and privacy-preserving job RSs.

**Part III. Future work**

**Chapter 6** discusses future work that can be carried out to improve or extend the proposed approach, including the instantiation of the multi-agent model for the RSs across different application areas.

**Appendix** This section discusses a preliminary method for the evaluation of RSs using privacy-preserving and risk-aware concepts.

# Recommender Systems

Recommender systems are software systems that produce a list of recommendations for its users by deploying in general two algorithms (i.e. collaborative filtering or content-based filtering) or a mix of these algorithms as a hybrid approach. The approach used in collaborative filtering utilizes the user’s historic data (i.e. items purchased by the user, browsing/navigation history on the website or the feedback provided for the purchased item). The result of this approach is a list produced by the system of recommendations of interest to the user [22]. On the other hand, content-based filtering approaches employ a set of attributes of an item in order to come up with a list of recommendations having items with similar attributes [23]. A hybrid approach can be used as a combination of the previously discussed approaches in order to find a solution with the best recommendation accuracy.

## Context-Aware Recommender Systems

Bouneffouf has briefly discussed the concept of context-aware RSs [7]. In order to make recommendations more accurate, the context at the time of generating recommendations is also an important factor. The contextual data can be added as a source of information for generating better recommendations or can help in filtering out non-relevant recommendations from the list of resultant recommendations generated by the system. Therefore, the introduction of context information into RSs leads to context-aware RSs [21].

## Privacy in Recommender Systems

A wide variety of information needs to be processed by RSs. Some authors discuss these diverse information types in detail [19]. Some of this information can be confidential and should not be revealed to any other person or organization, except the information owner. On the user’s end, there is always a trade-off between the amount of information to be provided to a RS and the accuracy of the resulting recommendations. This aspect is represented in their paper with the help of a three-dimensional representation that has the duration of information storage, the size of the audience and the extent of usage as its three axes [19].

## Privacy Protection

In order to alleviate the privacy concerns of the user to make the user provide more information to the system for better recommendations, some privacy-protection techniques can be employed. One of the methods is anonymization, which involves removing any link in the data to a specific user while preserving the structure in the data. Some authors use thi approach by introducing trust agents [34]. Other methods to deal with privacy concerns are based on randomization techniques or differential privacy servers.

### User control

Zhang, Na and Hogxia discuss two techniques to mitigate concerns over privacy risk breaches in the RSs that give users the option to manage the release of information to the RSs [14, 41] or provide appropriate reasons for the requirements of information release to users [42]. These two methods help in reducing breaches of user privacy.

## Risk Aware Recommender Systems

Bouneffouf discusses risk-aware RSs [7]. In this variation of RSs an approach is used to calculate the trade-off between discovering contextual information and upsetting users by providing them non-relevant recommendations. This trade-off factor is termed as risk and is calculated by using the multi-arm bandit optimization method. The techniques that are discussed in this paper are derived from the “variance cost” approach, “expected environment cost” approach and the hybrid approach [44, 43, 45, 46, 47, 48].

# Related Work

## Modelling Recommender Systems

Girardi and Marinho provide a description of an ontology-driven model for usage mining in the context of agent-based Recommender Systems is provided [1]. It first starts with a description of MADEM (Multi-Agent Domain Engineering Methodology) as a software development methodology for multi-agent domain engineering, followed by the description of the modeling concepts, tasks and products for the development of a family of multi-agent systems in a problem domain.

## Risk-Aware Recommender Systems

After introducing the concept of multi-agent system in context of RSs, we now introduce the dynamic risk-aware RS, as described in [7]. A dynamic risk-aware recommender system (DRARS) is essentially a context-aware RS which takes into account the exploration-exploitation trade-off using a multi-arm bandit optimization solution.

## Privacy Preserving Recommender Systems

Elmiseri, Rho and Botvich present a collaborative privacy framework for preserving user profile privacy in social recommender services [5]. It is a description of a novel two stage concealment process that offers to the user’s privacy control over their ratings profiles. The concealment process utilizes a hierarchical topology, where users are organized in peer-groups. This paper also provides a performance test of the proposed framework on a real dataset and the evaluation of how the overall accuracy of the recommendations depends on the number of users and requests. The experimental and analysis results showed that privacy increases under the proposed middleware without hampering the accuracy of recommendations. Moreover, the approach used in the paper has been shown to reduce privacy breaches on the concealed data without severely affecting the accuracy of recommendations based on collaborative filtering techniques by realizing that there are many challenges in building a collaborative privacy framework for preserving privacy in social recommender services. Ma et al. provide an evidence that the disclosure of user preferences in a RS seriously threatens the users’ personal privacy, especially when service providers move the user data to an untrusted cloud [6]. In this paper, a novel solution, called APPLET is presented, to address the significant challenges in privacy-preserving location-aware RSs. In APPLET, multiple cryptography methodologies were introduced in order to highlight the aspect of protecting the privacy of the RS users without affecting the quality of the recommendations. Moreover, an evaluation has been provided which shows that the effectiveness and performance of APPLET turns out to be well-suited. Shokri et al. proposed a novel method for privacy preservation in collaborative filtering RSs [12]. The authors addressed the problem of protecting user privacy in the presence of an untrusted central server, where the server has access to the user profiles. To avoid privacy violation, a mechanism is proposed where users store locally an offline profile on their client side, hidden from the server, and an online profile on the server from which the server generates the recommendations. The online profiles of different users are frequently synchronized with their offline versions in an independent and distributed way. Using a graph theoretic approach, the authors developed a model where each user arbitrarily contacts other users over time, and modifies his own offline profile through a process known as aggregation. Through experiments discussed in the paper, it is concluded in the paper that such a mechanism can lead to a high level of privacy through a proper choice of aggregation functions, while having a very little effect on the accuracy of the recommendation system. The results illustrated that similarity-based aggregation functions, where users receive items from other users proportional to the similarity between them, yield a considerable privacy level at a very low accuracy loss. Other findings suggest that the users’ online information is multi-dimensional regarding privacy concerns, especially in a recommender context [14].

## Privacy-Preserving Methodologies for Recommender Systems

Traditional location-aware RSs are facing a significant challenge, namely, how to protect the location privacy of users while preserving the quality of the recommendations. There are several studies that have achieved location privacy, which are based on anonymity, differential privacy, and encryption schemes. Some authors proposed location-oriented privacy-preserving mechanisms based on anonymity to protect user location privacy [49-51]. To solve the shortcomings of these solutions, some authors introduced differential privacy mechanisms to protect the user’s exact location independently from any side information [52-54].

# Proposed Approach

In this chapter we will discuss the proposed approach to tackle the challenges described in the previous sections. Let us start with a conceptual model depicted in Figure 1of a RS as a system where the resultant recommendations are affected by the privacy factors (e.g. user controls, privacy settings etc.) and the contextual risk factors (e.g. location, social connections etc.). The privacy risk factors can be understood as the parameters which are formulated by taking privacy instructions from the user and then filtering out the data to be considered for generating recommendations based on those privacy parameters set by the users. On the other hand, the contextual risk factors are the parameters that are obtained from the continuous or periodical streams of user data followed by filtering by the privacy parameters, which are used as one of the data sources for generating the recommendations. Thus, in order to propose a model for the Risk-Aware Privacy-Preserving Recommender System (RPRS), we need to have model that takes into account these two factors affecting the system, namely privacy and contextual risk.

The proposed approach to model the RPRS follows a sequence of steps in order to produce a model of the system (Figure 2). In the first step the system is conceptually broken down into three subsystems (i.e. the Data Subsystem, the Contextual Risk Subsystem and the Privacy Subsystem) to consider the impact of the privacy and the risk factor on the overall objective of the system, which is to produce recommendations. This step also involves the introduction of an agent-based approach where each subsystem is assumed to be modeled by one or more agents in order to accomplish the objective of that subsystem.

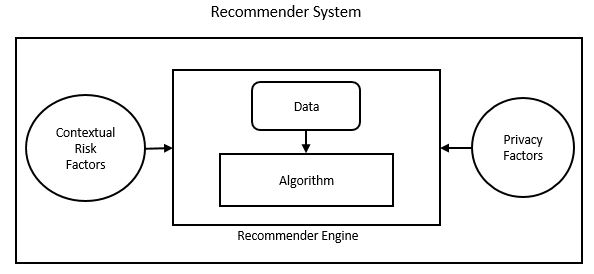


Figure 1 Conceptual Diagram of the Risk-Aware Privacy-Preserving Recommender System

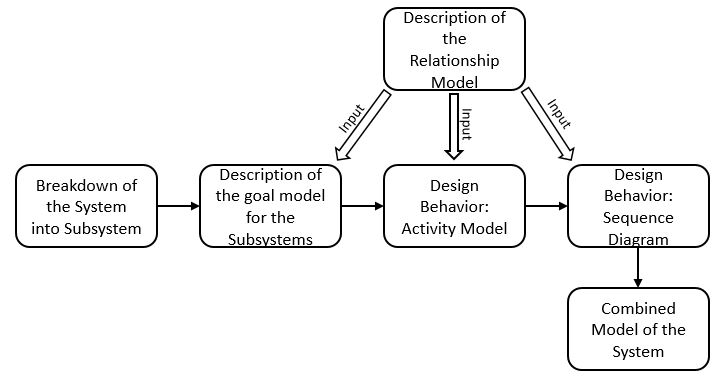


Figure 2 Proposed Steps of the Modeling Approach

In the next step, we provide a goal model for each subsystem within the entire system in order to specify the goal of these subsystems. The agents within these subsystems are described in terms of the roles they perform, the responsibilities they fulfill and the activities performed by these agents in order to achieve the objective of the subsystem. This is achieved partially by the introduction of the relationship model which provides a set of attributes displayed by each agent and their associated relationships in order to accomplish its responsibilities within the subsystem.

We introduce two design behaviors for the next two subsequent steps. These design behaviors help in understanding the system by providing the internal behavior of each subsystem. The first behavior design we discuss is the activity model of the subsystems. It describes the behavior of the subsystem in context of the relationship model discussed previously. The activity models for each subsystem are then combined to form an activity model of the entire RPRS.

The second behavior design which is discussed is the sequence diagrams of the subsystems. The sequence diagrams describe the sequence of events that occur within the subsystems. These sequence diagrams are then combined to form the sequence diagram of the whole RPRS. The behaviors defined by the sequence diagrams are based on the contextual information from a relationship model.

Before going further in the description of the system model, it is indispensable to describe the notations used in this approach, which involve UML modeling techniques. Various types of UML diagrams are used (e.g. activity diagram and sequence models) to provide the system models and to gain understanding of the behavior of the subsystems and the recommender systems as a whole. These diagrams are explained in the following section.

## UML Diagrams

UML stands for Unified Modeling Language and is used in object-oriented software engineering. Although typically used in software engineering, it is a rich language that can be used to model application structures, behavior and even business processes. There are 14 UML diagram types but for the purpose of this thesis, we will be focusing only on activity diagram and the sequence diagrams.

### Activity Diagrams

The basic purposes of activity diagrams is to capture the dynamic behavior of the system by showing the message flow from one activity to another. Activity is a particular operation of the system. Activity diagrams are not only used for visualizing dynamic nature of a system but they are also used to construct the executable system within forward and reverse engineering techniques. A missing element in activity diagrams is the message part: it does not show any message flow from one activity to another. Although activity diagrams bear some similarities to flow charts, they different in that they depict flow such as parallel, concurrent, single and branched flows.

### Sequence Diagrams

UML sequence diagrams are used to represent or model the flow of messages, events and actions between the objects or components of a system. Time is represented in the vertical direction showing the sequence of interactions of the header elements, which are displayed horizontally at the top of the diagram. Sequence Diagrams are used primarily to design, document and validate the architecture, interfaces and logic of the system by describing the sequence of actions that need to be performed to complete a task or scenario. UML sequence diagrams are useful design tools because they provide a dynamic view of the system behavior which can be difficult to extract from static diagrams or specifications. Although UML sequence diagrams are typically used to describe object-oriented software systems, they are also extremely useful as system engineering tools to design system architectures, in business process engineering as process flow diagrams and as message sequence charts for protocol stack design and analysis.

## Goal Model

Goal models for the RSs were introduced in [1]. In this thesis, goal models are used to model subsystems of the RPRS in order to describe the objectives of the subsystems. This is an agent-based model in which the goals of each subsystem is represented diagrammatically and that relies on information provided by a relationship model.

## Multi-agent System Model and System Description

In the proposed approach, we will start by breaking-down the system into subsystems. Each subsystem will be responsible for accomplishing a pre-defined task and will be modeled using agents. We will focus on modeling the goals of the subsystems, the roles of the agents, the activities performed by the agents, and finally the interactions of the agents. Agents possess knowledge that is used to help reach their goals. A subsystem is composed of agents having specific goals that establish what the subsystem intends to accomplish. The achievement of specific goals by the agents within a subsystem allows the entire system to reach its goal when the subsystems are put together.

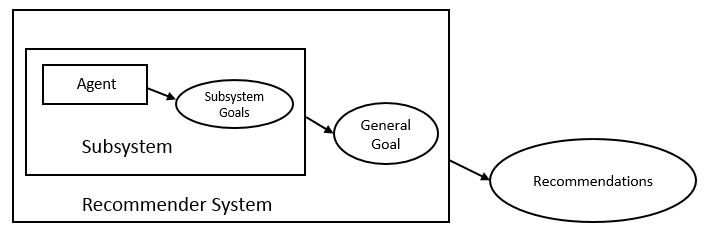


Figure 3 Combining Subsystem Goals to Achieve the System Goal

Specific goals of an agent within a subsystem are reached through the performance of responsibilities that agents have, in which the agent plays roles with a certain degree of autonomy. Responsibilities are exercised through the execution of activities by each individual agent within the subsystem. The set of activities associated with a responsibility are a functional decomposition of it. Roles have skills on one or a set of techniques that support the execution of responsibilities and activities in an effective way within the subsystem. Pre-conditions and post-conditions may need to be satisfied before or after the execution of an activity by each agent within the subsystem. Knowledge can be consumed and produced through the execution of an activity. Skills can be, for instance, the rules of the subsystem that agents know in order to access and structure its information sources. Sometimes, agents have to communicate with other agents to cooperate in the execution of an activity. This approach allows for such communication to take place between the agents within the subsystems.



Figure 4 Relationship model for subsystems

## Goal Models for the Subsystems

We will now discuss the goal models of the subsystems which make up a RPRS and also explain the contribution of each subsystem and the agents involved in these subsystems.

### Goal Model: Data Subsystem



Figure 5 Goal Model for the Data Agent and the Aggregator Agent

Let us start with the data management subsystem. This subsystem is responsible for managing the data inflow and outflow from the RPRS. The subsystem consists of two agents, the Data Manager Agent and the Aggregator Agent. The goal of the Data Manager Agent is to maintain the authenticity of the data by preventing it from getting corrupted and also to manage the piping of data from data sources to the desired destinations. This goal of the data agent is achieved by fulfilling two responsibilities: the responsibility of properly encrypting and decrypting the data from the source and the destination, respectively, and of updating the proper locations of source and destination of the data to be used by the system. The main task of the Aggregator Agent is to channel between the user interface and the various servers to support computation, storage and generating recommendations. This specific goal is achieved by the proper distribution and redistribution of data within the system.

### Goal Model: Privacy Subsystem



Figure 6 Goal model for the User Privacy Agent

The privacy subsystem manages the privacy aspect of the RPRS. This subsystem relies on the User Privacy Agent to carry out its operations. The main role of this subsystem is to provide user contextual data and the historic data to the computation server in order to generate recommendations for the users. The contextual information about the users can involve user location and social user information, combined with the timing of the information. The user history data refers to the user behavior that is recorded at runtime for analysis purposes.

To understand the role of the privacy subsystem within the RPRS, we need to look at the goals of the User Privacy Agent. The User Privacy Agent performs the task of maintaining user privacy settings for the contextual data and is responsible for filtering out the noise from the contextual data that is obtained from the users. These two responsibilities form the specific goal of filtering and maintaining the users’ contextual privacy information. On the other hand, the User Privacy Agent also fulfills the responsibility of maintaining the access to the users’ historic data based on the settings provided by the users and of selecting the most appropriate data for generating the recommendations after filtering out the noise from of historic data.

### Goal Model: Risk Subsystem



Figure 7 Goal Model for the User Risk Agent and the Context Analyzer Agent

This subsystem handles the contextual risk by getting the contextual information (i.e. time, location and social information) from the user and then feeding this information to the RPRS. It consists of two agents: the Context Analyzer Agent and the User Risk Agent.

The information processed in this step is utilized by the RPRS to produce a more context-aware system not only by providing more relevant information to its users but also by keeping itself aware of the risks associated with disturbing or negatively affecting the user with inconvenient recommendations. This tradeoff between providing relevant recommendations and the associated risks of doing so is the part of the risk calculation through the exploration and exploitation approach [7].

The two agents involved in this subsystem have some specific goals and responsibilities. The responsibility of the User Risk Agent is to ensure that no noise remains in the data and to calculate the risk tradeoff for generating the recommendations and the relevance of these recommendations to the user from the user feedback related to the previously generated recommendations. These two responsibilities help in achieving the goal of carrying out the risk calculation and the analysis of the user data. The Context Analyzer Agent is responsible for cleaning the data obtained from the risk calculation stage, selecting the best possible algorithm for the analysis and securing the generated data to be forwarded as recommendations to the users. This helps in achieving the task of semantic analysis of the user data and, finally, in providing the analysis results as recommendations to the users of the system.

### Combined Goal Model of the System

The combined goal model of the RPRS consists of the aggregation of the individual subsystems and the combination of the goals of the agents within each subsystem in order to achieve the goal of the entire system.



Figure 8 System Goal Model

## Activity Models for the Subsystems

We will now discuss the activity models of the subsystems which make up a RPRS and also in terms of these models the contribution of each subsystem and the agents involved in the respective subsystems.

### Activity Model: Data Subsystem



Figure 9 Activity Diagram of Data Subsystem

This subsystem receives data in form of User Preferences and User Feedback. Its multiple elements perform the tasks that brings out the functioning of the data subsystem. The Data Manager Agent uses hashing, SHA, and MD5 checking to ensure data authenticity. An example of an Aggregator Agent is the typical messaging broker used in modern applications. Apache Kafa and RabbitMQ are two types of such message brokers. Together, these two agents fulfill the objective of the Data Subsystem, i.e. the management and maintenance of the data pipelines within the system.

### Activity Model: Privacy Subsystem



Figure 10 Activity diagram for the User Privacy Subsystem

Within this subsystem the contextual and personal information is extracted from the user and fed into the RPRS. An addition differential privacy server is used to handle the differential privacy aspect of the subsystem. The contextual data from the user along with the historic data of the user provides valuable insights that help to provide quality recommendations to the user.

### Activity Model: Risk Subsystem

The information processed in this step is utilized by the RPRS to generate a more context-aware system by not only providing more relevant information to its users but also keeping itself aware of the risks associated with disturbing or negatively affecting the user with inconvenient recommendations. This tradeoff between providing relevant recommendations and the associated risks is captured in the risk calculation using the exploration and exploitation approach [7].



Figure 11 Activity Diagram for the Risk Subsystem

### Combined Activity Model for the System

The combined Activity model of the RPRS consists of the aggregation of the individual subsystems and the combination of the activity diagrams of the individual agents within each subsystem to achieve the goals of the entire system.



Figure 12 Complete Activity Model of the System

## Sequence Diagrams for the Subsystems

We will now discuss the sequence diagrams of the subsystems involved in the RPRS and also explain the sequence of actions that takes place within each subsystem.

### Sequence Diagrams: Data Subsystem



Figure 13 Data Subsystem sequence diagram

The sequence diagram of the data subsystem is provided in Figure 13. In this diagram, a recommendation generation process starts when a connection is established between the user-data database and the computation server where the data to be used is decrypted. This data is then piped to the computation server. After the processing at the communication server, the recommendations are generated and are then forwarded to the user through an interface. Based on the quality of recommendation, the user provides a feedback which is stored in the user-data database. The transfer of data between the servers, including the encryption and the decryption process, is carried out within the data subsystem. These tasks are carried out by the Data Agent and the Aggregator Agent within the data subsystem, and a summarized description of their behavior has been provided in the previous section.

### Sequence Diagram: Privacy Subsystem



Figure 14 Privacy Subsystem Sequence Diagram

In order to understand the privacy subsystem it is necessary to know the flow of control within this subsystem. The first step involves establishing a connection with the user data server and with the privacy server. This is followed by extracting the user data and the user privacy settings from the server. Once this data has been extracted from the server, it is filtered against the user settings. The user data includes the contextual data (i.e. location, time and social) data as well as the user’s previous behavior patterns obtained while the user interacted with the system. The user is made aware of the data through user controls and is asked permission to utilize his or her data for generating recommendations.

Once the data has been filtered of the noise and against the user settings, it is piped through the computation server to generate the recommendations to the user. After the recommendations have been generated, they are forwarded to the user via a specific interface.

Based on the quality of the recommendations, the user provides a feedback or exhibits certain behavior patterns (e.g. clicks, navigation, dismiss) which indicate the user’s opinion about the quality of the generated recommendations. This feedback data is then encrypted and stored in the user-data database to serve as an input for future computations for recommendation generation.

### Sequence Diagram: Risk Subsystem



Figure 15 Contextual Risk Subsystem Sequence Diagram

The sequence diagram helps in understanding the steps that take place within the contextual risk subsystem. First, a connection is established with a sensing device at the user’s end, through an interface. After this step, the low-level abstraction of the user’s data is sent to the servers running the semantic analysis. As a result the risk is calculated and based on the value of this parameter the recommendations are forwarded to the user.

### Combined Sequence Diagram

The sequence diagram of the RPRS consists of the combination of the actions taking place within the system to achieve the goals of the entire system.



Figure 16 Combined Sequence Diagram

Bibliography

[1] Girardi R, Marinho LB. A domain model of Web recommender systems based on usage mining and collaborative filtering. Requirements Engineering. 2007 Jan 1;12(1):23-40.

[2] Rasmussen C, Dara R. Recommender Systems for Privacy Management: A Framework. InHigh-Assurance Systems Engineering (HASE), 2014 IEEE 15th International Symposium on 2014 Jan 9 (pp. 243-244). IEEE.

[3] Sankar CP, Vidyaraj R, Kumar KS. Trust Based Stock Recommendation System–A Social Network Analysis Approach. Procedia Computer Science. 2015 Jan 1;46:299-305.

[4] Zhao VN, Moh M, Moh TS. Contextual-Aware Hybrid Recommender System for Mixed Cold-Start Problems in Privacy Protection. InBig Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on 2016 Apr 9 (pp. 400-405). IEEE.

[5] Elmisery AM, Rho S, Botvich D. Collaborative privacy framework for minimizing privacy risks in an IPTV social recommender service. Multimedia Tools and Applications. 2016 Nov 1;75(22):14927-57.

[6] Ma X, Li H, Ma J, Jiang Q, Gao S, Xi N, Lu D. APPLET: a privacy-preserving framework for location-aware recommender system. Science China Information Sciences. 2017 Sep 1;60(9):092101.1.

[7] Bouneffouf D. *DRARS, A Dynamic Risk-Aware Recommender System* (Doctoral dissertation, Institut National des Télécommunications).

[8] Wang Z, Liao J, Cao Q, Qi H, Wang Z. Friendbook: a semantic-based friend recommendation system for social networks. IEEE Transactions on Mobile Computing. 2015 Mar 1;14(3):538-51.

[9] Guo S, Alamudun F, Hammond T. RésuMatcher: A personalized résumé-job matching system. Expert Systems with Applications. 2016 Oct 30;60:169-82.

[10] Lu Y, El Helou S, Gillet D. A recommender system for job seeking and recruiting website. InProceedings of the 22nd International Conference on World Wide Web 2013 May 13 (pp. 963-966). ACM.

[11] McSherry F, Mironov I. Differentially private recommender systems: building privacy into the net. InProceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining 2009 Jun 28 (pp. 627-636). ACM.

[12] Shokri R, Pedarsani P, Theodorakopoulos G, Hubaux JP. Preserving privacy in collaborative filtering through distributed aggregation of offline profiles. InProceedings of the third ACM conference on Recommender systems 2009 Oct 23 (pp. 157-164). ACM.

[13] Shang S, Hui Y, Hui P, Cuff P, Kulkarni S. Beyond personalization and anonymity: Towards a group-based recommender system. InProceedings of the 29th Annual ACM Symposium on Applied Computing 2014 Mar 24 (pp. 266-273). ACM.

[14] Zhang B, Wang N, Jin H. Privacy concerns in online recommender systems: influences of control and user data input. InSymposium on Usable Privacy and Security (SOUPS) 2014 Jul 9 (pp. 159-173).

[15] Zimmermann T, Bird C. Collaborative software development in ten years: Diversity, tools, and remix culture. InProceedings of the Workshop on The Future of Collaborative Software Development 2012.

[16] El Helou S, Salzmann C, Sire S, Gillet D. The 3A contextual ranking system: simultaneously recommending actors, assets, and group activities. InProceedings of the third ACM conference on Recommender systems 2009 Oct 23 (pp. 373-376). ACM.

[17] Adomavicius G, Tuzhilin A. Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. IEEE transactions on knowledge and data engineering. 2005 Jun;17(6):734-49.

[18] Beel J, Gipp B, Langer S, Breitinger C. Research-paper recommender systems: a literature survey. International Journal on Digital Libraries. 2016 Nov 1;17(4):305-38.

[19] Jeckmans AJ, Beye M, Erkin Z, Hartel P, Lagendijk RL, Tang Q. Privacy in recommender systems. InSocial media retrieval 2013 (pp. 263-281). Springer London.

[20] Jafarkarimi H, Sim AT, Saadatdoost R. A naive recommendation model for large databases. International Journal of Information and Education Technology. 2012 Jun 1;2(3):216.

[21] Dey AK. Understanding and using context. Personal and ubiquitous computing. 2001 Jan 2;5(1):4-7.

[22] Melville P, Sindhwani V. Recommender systems. InEncyclopedia of machine learning 2011 (pp. 829-838). Springer US.

[23] Mooney RJ, Roy L. Content-based book recommending using learning for text categorization. InProceedings of the fifth ACM conference on Digital libraries 2000 Jun 1 (pp. 195-204). ACM.

[24] Grudin J. Partitioning digital worlds: focal and peripheral awareness in multiple monitor use. InProceedings of the SIGCHI conference on Human factors in computing systems 2001 Mar 1 (pp. 458-465). ACM. [25] Kang, Jerry. "Information privacy in cyberspace transactions." *Stanford Law Review* (1998): 1193-1294.

[26] Palen L, Dourish P. Unpacking privacy for a networked world. InProceedings of the SIGCHI conference on Human factors in computing systems 2003 Apr 5 (pp. 129-136). ACM.

[27] Hong JI, Landay JA. An architecture for privacy-sensitive ubiquitous computing. InProceedings of the 2nd international conference on Mobile systems, applications, and services 2004 Jun 6 (pp. 177-189). ACM.

[28] Gross R, Acquisti A. Information revelation and privacy in online social networks. InProceedings of the 2005 ACM workshop on Privacy in the electronic society 2005 Nov 7 (pp. 71-80). ACM.

[29] Tufekci Z. Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society. 2008 Feb 1;28(1):20-36.

[30] Lam S, Frankowski D, Riedl J. Do you trust your recommendations? An exploration of security and privacy issues in recommender systems. Emerging Trends in Information and Communication Security. 2006:14-29.

[31] Konstas I, Stathopoulos V, Jose JM. On social networks and collaborative recommendation. InProceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval 2009 Jul 19 (pp. 195-202). ACM.

[32] Ramakrishnan N, Keller BJ, Mirza BJ, Grama AY, Karypis G. Privacy risks in recommender systems. IEEE Internet Computing. 2001 Nov 1;5(6):54.

[33] Rosenblum D. What anyone can know: The privacy risks of social networking sites. IEEE Security & Privacy. 2007 May;5(3).

[34] Cissée R, Albayrak S. An agent-based approach for privacy-preserving recommender systems. InProceedings of the 6th international joint conference on Autonomous agents and multiagent systems 2007 May 14 (p. 182). ACM.

[35] Polat H, Du W. SVD-based collaborative filtering with privacy. InProceedings of the 2005 ACM symposium on Applied computing 2005 Mar 13 (pp. 791-795). ACM.

[36] Polat H, Du W. Privacy‐preserving top‐N recommendation on distributed data. Journal of the American Society for Information Science and Technology. 2008 May 1;59(7):1093-108.

[37] Berkovsky S, Eytani Y, Kuflik T, Ricci F. Enhancing privacy and preserving accuracy of a distributed collaborative filtering. InProceedings of the 2007 ACM conference on Recommender systems 2007 Oct 19 (pp. 9-16). ACM.

[38] Shokri R, Pedarsani P, Theodorakopoulos G, Hubaux JP. Preserving privacy in collaborative filtering through distributed aggregation of offline profiles. InProceedings of the third ACM conference on Recommender systems 2009 Oct 23 (pp. 157-164). ACM.

[39] Bugliesi M, Preneel B, Sassone V, Wegener I, editors. Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings. Springer; 2006 Jun 29.

[40] McSherry F, Mironov I. Differentially private recommender systems: building privacy into the net. InProceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining 2009 Jun 28 (pp. 627-636). ACM.

[41] Lampe C, Ellison NB, Steinfield C. Changes in use and perception of Facebook. InProceedings of the 2008 ACM conference on Computer supported cooperative work 2008 Nov 8 (pp. 721-730). ACM.

[42] Knijnenburg BP, Kobsa A. Making decisions about privacy: information disclosure in context-aware recommender systems. ACM Transactions on Interactive Intelligent Systems (TiiS). 2013 Oct 1;3(3):20.

[43] Filar JA, Krass D, Ross KW. Percentile performance criteria for limiting average Markov decision processes. IEEE Transactions on Automatic Control. 1995 Jan;40(1):2-10.

[44] Marcus SI, Fernández-Gaucherand E, Hernández-Hernandez D, Coraluppi S, Fard P. Risk sensitive Markov decision processes. InSystems and control in the twenty-first century 1997 (pp. 263-279). Birkhäuser Boston.

[45] Geibel P, Wysotzki F. Risk-sensitive reinforcement learning applied to control under constraints. J. Artif. Intell. Res.(JAIR). 2005 Jul 1;24:81-108.

[46] Yu X, Li Y, Wang X, Zhao K. An autonomous robust fault tolerant control system. InInformation Acquisition, 2006 IEEE International Conference on 2006 Aug 20 (pp. 1191-1196). IEEE.

[47] Hans A, Schneegaß D, Schäfer AM, Udluft S. Safe exploration for reinforcement learning. InESANN 2008 Apr (pp. 143-148).

[48] Castro DD, Tamar A, Mannor S. Policy gradients with variance related risk criteria. InProceedings of the 29th International Conference on Machine Learning (ICML-12) 2012 (pp. 935-942).

[49] Gao S, Ma J, Shi W, Zhan G, Sun C. TrPF: A trajectory privacy-preserving framework for participatory sensing. IEEE Transactions on Information Forensics and Security. 2013 Jun;8(6):874-87.

[50] Niu B, Li Q, Zhu X, Cao G, Li H. Enhancing privacy through caching in location-based services. InComputer Communications (INFOCOM), 2015 IEEE Conference on 2015 Apr 26 (pp. 1017-1025). IEEE.

[51] Cicek AE, Nergiz ME, Saygin Y. Ensuring location diversity in privacy-preserving spatio-temporal data publishing. The VLDB Journal. 2014 Aug 1;23(4):609-25.

[52] Andrés ME, Bordenabe NE, Chatzikokolakis K, Palamidessi C. Geo-indistinguishability: Differential privacy for location-based systems. InProceedings of the 2013 ACM SIGSAC conference on Computer & communications security 2013 Nov 4 (pp. 901-914). ACM.

[53] Xiao Y, Xiong L. Protecting locations with differential privacy under temporal correlations. InProceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security 2015 Oct 12 (pp. 1298-1309). ACM.

[54] To H, Ghinita G, Shahabi C. A framework for protecting worker location privacy in spatial crowdsourcing. Proceedings of the VLDB Endowment. 2014 Jun 1;7(10):919-30.

[55] Shao J, Lu R, Lin X. Fine: A fine-grained privacy-preserving location-based service framework for mobile devices. InINFOCOM, 2014 Proceedings IEEE 2014 Apr 27 (pp. 244-252). IEEE.

[56] Popa RA, Redfield C, Zeldovich N, Balakrishnan H. CryptDB: processing queries on an encrypted database. Communications of the ACM. 2012 Sep 1;55(9):103-11.

[57] Calandrino JA, Kilzer A, Narayanan A, Felten EW, Shmatikov V. " You Might Also Like:" Privacy Risks of Collaborative Filtering. InSecurity and Privacy (SP), 2011 IEEE Symposium on 2011 May 22 (pp. 231-246). IEEE.

[58] Bhagat S, Weinsberg U, Ioannidis S, Taft N. Recommending with an agenda: Active learning of private attributes using matrix factorization. InProceedings of the 8th ACM Conference on Recommender systems 2014 Oct 6 (pp. 65-72). ACM.

[59] Staff CA. Recommendation algorithms, online privacy, and more. Communications of the ACM. 2009 May 1;52(5):10-1.

[60] Celdrán AH, Pérez MG, Clemente FG, Pérez GM. PRECISE: Privacy-aware recommender based on context information for cloud service environments. IEEE Communications Magazine. 2014 Aug;52(8):90-6.

[61] Zhu J, He P, Zheng Z, Lyu MR. A privacy-preserving qos prediction framework for web service recommendation. InWeb Services (ICWS), 2015 IEEE International Conference on 2015 Jun 27 (pp. 241-248). IEEE.

[62] Jorgensen Z, Yu T. A Privacy-Preserving Framework for Personalized, Social Recommendations. InEDBT 2014 (pp. 571-582).

[63] Guerraoui R, Kermarrec AM, Patra R, Taziki M. D 2 P: distance-based differential privacy in recommenders. Proceedings of the VLDB Endowment. 2015 Apr 1;8(8):862-73.

[64] Shen Y, Jin H. Privacy-preserving personalized recommendation: An instance-based approach via differential privacy. InData Mining (ICDM), 2014 IEEE International Conference on 2014 Dec 14 (pp. 540-549). IEEE.

[65] Liu B, Hengartner U. pTwitterRec: a privacy-preserving personalized tweet recommendation framework. InProceedings of the 9th ACM symposium on Information, computer and communications security 2014 Jun 4 (pp. 365-376). ACM.

[66] Samanthula BK, Cen L, Jiang W, Si L. Privacy-Preserving and Efficient Friend Recommendation in Online Social Networks. Trans. Data Privacy. 2015 Aug 1;8(2):141-71.

[67] Gong Y, Cai Y, Guo Y, Fang Y. A privacy-preserving scheme for incentive-based demand response in the smart grid. IEEE Transactions on Smart Grid. 2016 May;7(3):1304-13.

[68] Hoens TR, Blanton M, Steele A, Chawla NV. Reliable medical recommendation systems with patient privacy. ACM Transactions on Intelligent Systems and Technology (TIST). 2013 Sep 1;4(4):67.

[69] Guo L, Zhang C, Fang Y. A trust-based privacy-preserving friend recommendation scheme for online social networks. IEEE Transactions on Dependable and Secure Computing. 2015 Jul 1;12(4):413-27.

[70] Xin Y, Jaakkola T. Controlling privacy in recommender systems. InAdvances in Neural Information Processing Systems 2014 (pp. 2618-2626).

[71] Tinghuai MA, Jinjuan ZH, Meili TA, Yuan TI, Abdullah AD, Mznah AR, Sungyoung LE. Social network and tag sources based augmenting collaborative recommender system. IEICE transactions on Information and Systems. 2015 Apr 1;98(4):902-10.

[72] Aïmeur E, Brassard G, Fernandez JM, Onana FS. Alambic: a privacy-preserving recommender system for electronic commerce. International Journal of Information Security. 2008 Oct 1;7(5):307-34.

[73] Zhu H, Xiong H, Ge Y, Chen E. Mobile app recommendations with security and privacy awareness. InProceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining 2014 Aug 24 (pp. 951-960). ACM.

[74] Lao N. *Efficient random walk inference with knowledge bases* (Doctoral dissertation, Carnegie Mellon University).

[75] N. Lao and W. W. Cohen, “Personalized Reading Recommendations for Saccharomyces Genome Database,” *Unpublished Paper, http://www.cs.cmu.edu/ nlao/publication/2012/2012.dils.pdf*, pp. 1–15, 2012.

[76] N. Lao and W. W. Cohen, “Personalized Reading Recommendations for Saccharomyces Genome Database,” *Unpublished Poster, http://www.cs.cmu.edu/ nlao/publication/2012/2012.dils.poster.portrat.pdf*, 2012.

[77] N. Lao and W. W. Cohen, “Contextual Recommendation with Path Constrained Random Walks,” *Unpublished, http://www.cs.cmu.edu/ nlao/doc/2011.cikm.pdf*, pp. 1–9, 2011.

[78] P. Lakkaraju, S. Gauch, and M. Speretta, “Document similarity based on concept tree distance,” in *Proceedings of the nineteenth ACM conference on Hypertext and hypermedia*, 2008, pp. 127–132.

[79] N. Lao and W. W. Cohen, “Relational retrieval using a combination of path-constrained random walks,” *Machine learning*, vol. 81, no. 1, pp. 53–67, 2010.

[80] K. D. B. S. Lawrence, “A System For Automatic Personalized Tracking of Scientific Literature on the Web,” in *Proceedings of the fourth ACM conference on Digital libraries*, 1999, pp. 105–113.

[81] S. R. Lawrence, K. D. Bollacker, and C. L. Giles, “Autonomous citation indexing and literature browsing using citation context,” U.S. Patent US 6,738,780 B2Summer-2004.

[82] S. R. Lawrence, C. L. Giles, and K. D. Bollacker, “Autonomous citation indexing and literature browsing using citation context,” U.S. Patent US 6,289,342 B1Nov-2001.

[83] H. Li, I. Councill, W.-C. Lee, and C. L. Giles, “CiteSeerx: an architecture and web service design for an academic document search engine,” in *Proceedings of the 15th international conference on World Wide Web*, 2006, pp. 883–884.

[84] Y. Liang, Q. Li, and T. Qian, “Finding relevant papers based on citation relations,” in *Proceedings of the 12th international conference on Web-age information management*, 2011, pp. 403–414.

[85] J. Lin and W. J. Wilbur, “PubMed Related Articles: a Probabilistic Topic-based Model for Content Similarity,” *BMC Bioinformatics*, vol. 8, no. 1, pp. 423–436, 2007.

[86] Y. Lu, J. He, D. Shan, and H. Yan, “Recommending citations with translation model,” in *Proceedings of the 20th ACM international conference on Information and knowledge management*, 2011, pp. 2017–2020.

[87] S. M. McNee, N. Kapoor, and J. A. Konstan, “Don’t look stupid: avoiding pitfalls when recommending research papers,” in *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*, 2006, pp. 171–180.

[88] S. E. Middleton, H. Alani, and D. C. De Roure, “Exploiting synergy between ontologies and Recommender Systems,” in *Proceedings of the Semantic Web Workshop*, 2002, pp. 1–10.

[89] S. E. Middleton, D. De Roure, and N. R. Shadbolt, “Ontology-based Recommender Systems,” in *Handbook on Ontologies*, Springer, 2009, pp. 779–796.

[90] S. E. Middleton, D. C. De Roure, and N. R. Shadbolt, “Foxtrot Recommender System: User profiling, ontologies and the World Wide Web,” in *Proceedings of the WWW Conference*, 2002, pp. 1–3.

[91] S. E. Middleton, D. C. De Roure, and N. R. Shadbolt, “Capturing knowledge of user preferences: ontologies in Recommender Systems,” in *Proceedings of the 1st international conference on Knowledge capture*, 2001, pp. 100–107.

[92] M. Mönnich and M. Spiering, “Adding value to the library catalog by implementing a recommendation system,” *D-Lib Magazine*, vol. 14, no. 5, pp. 4–11, 2008.

[93] S. M. McNee, I. Albert, D. Cosley, P. Gopalkrishnan, S. K. Lam, A. M. Rashid, J. A. Konstan, and J. Riedl, “On the Recommending of Citations for Research Papers,” in *Proceedings of the ACM Conference on Computer Supported Cooperative Work*, 2002, pp. 116–125.

[94] S. E. Middleton, N. R. Shadbolt, and D. C. De Roure, “Ontological user profiling in Recommender Systems,” *ACM Transactions on Information Systems (TOIS)*, vol. 22, no. 1, pp. 54–88, 2004.

[95] M. Monnich and M. Spiering, “Einsatz von BibTip als Recommendersystem im Bibliothekskatalog,” *Bibliotheksdienst*, vol. 42, no. 1, pp. 54–54, 2008.

[96] A. Naak, “Papyres: un système de gestion et de recommandation d’articles de recherche,” Master Thesis. Université de Montréal, 2009.

[97] A. W. Neumann, “Recommender Systems for Information Providers,” Springer, 2009, pp. 91–119.

[98] A. Naak, H. Hage, and E. Aimeur, “A multi-criteria collaborative filtering approach for research paper recommendation in papyres,” in *Proceedings of the 4th International Conference MCETECH*, 2009, pp. 25–39.

[99] A. Naak, H. Hage, and E. Aimeur, “Papyres: A Research Paper Management System,” in *Proceedings of the 10th E-Commerce Technology Conference on Enterprise Computing, E-Commerce and E-Services*, 2008, pp. 201–208.

[100] R. M. Nallapati, A. Ahmed, E. P. Xing, and W. W. Cohen, “Joint latent topic models for text and citations,” in *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2008, pp. 542–550.

[101] C. Nascimento, A. H. Laender, A. S. da Silva, and M. A. Gonçalves, “A source independent framework for research paper recommendation,” in *Proceedings of the 11th annual international ACM/IEEE joint conference on Digital libraries*, 2011, pp. 297–306.

[102] T. Ozono, S. Goto, N. Fujimaki, and T. Shintani, “P2p based knowledge source discovery on research support system papits,” in *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1*, 2002, pp. 49–50.

[103] T. Ozono and T. Shintani, “P2P based Information Retrieval on Research Support System Papits,” in *Proceedngs of the IASTED International Conference on Artificial and Computational Intelligence*, 2002, pp. 136–141.

[104] T. Ozono and T. Shintani, “Paper classification for recommendation on research support system papits,” *IJCSNS International Journal of Computer Science and Network Security*, vol. 6, pp. 17–23, 2006.

[105] T. Ozono, T. Shintani, T. Ito, and T. Hasegawa, “A feature selection for text categorization on research support system Papits,” in *Proceedings of the 8th Pacific Rim International Conference on Artificial Intelligence*, 2004, pp. 524–533.

[106] D. M. Pennock, E. Horvitz, S. Lawrence, and C. L. Giles, “Collaborative filtering by personality diagnosis: A hybrid memory-and model-based approach,” in *Proceedings of the Sixteenth conference on Uncertainty in artificial intelligence*, 2000, pp. 473–480.

[107] Y. Petinot, C. L. Giles, V. Bhatnagar, P. B. Teregowda, and H. Han, “Enabling interoperability for autonomous digital libraries: an API to citeseer services,” in *Digital Libraries, 2004. Proceedings of the 2004 Joint ACM/IEEE Conference on*, 2004, pp. 372–373.

[108] Y. Petinot, C. L. Giles, V. Bhatnagar, P. B. Teregowda, H. Han, and I. Councill, “A service-oriented architecture for digital libraries,” in *Proceedings of the 2nd international conference on Service oriented computing*, 2004, pp. 263–268.

[109] S. Pohl, “Using Access Data for Paper Recommendations on ArXiv. org,” Master Thesis. Technical University of Darmstadt, 2007.

[110] S. Pohl, F. Radlinski, and T. Joachims, “Recommending related papers based on digital library access records,” in *Proceedings of the 7th ACM/IEEE-CS joint conference on Digital libraries*, 2007, pp. 417–418.

[111] T. Researchgate, “Researchgate Recommender,” *http://www.researchgate.net/directory/publications/*, 2011.

[112] L. Rokach, P. Mitra, S. Kataria, W. Huang, and L. Giles, “A Supervised Learning Method for Context-Aware Citation Recommendation in a Large Corpus,” in *Proceedings of the Large-Scale and Distributed Systems for Information Retrieval Workshop (LSDS-IR)*, 2013, pp. 17–22.

[113] Sarkanto, “About the Sarkanto Recommender Demo,” *http://lab.cisti-icist.nrc-cnrc.gc.ca/Sarkanto/about.jsp*. 2013.

[114] T. Strohman, W. B. Croft, and D. Jensen, “Recommending citations for academic papers,” in *Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval*, 2007, pp. 705–706.

[115] K. Sugiyama and M.-Y. Kan, “Scholarly paper recommendation via user’s recent research interests,” in *Proceedings of the 10th ACM/IEEE Annual Joint Conference on Digital Libraries (JCDL)*, 2010, pp. 29–38.

[116] D. Thomas, A. Greenberg, and P. Calarco, “Scholarly Usage Based Recommendations: Evaluating bX for a Consortium,” *Presentation, http://igelu.org/wp-content/uploads/2011/09/bx\_igelu\_presentation\_updated\_september-13.pdf*. 2011.

[117] R. Torres, S. M. McNee, M. Abel, J. A. Konstan, and J. Riedl, “Enhancing digital libraries with TechLens+,” in *Proceedings of the 4th ACM/IEEE-CS joint conference on Digital libraries*, 2004, pp. 228–236.

[118] K. Uchiyama, H. Nanba, A. Aizawa, and T. Sagara, “OSUSUME: cross-lingual Recommender System for research papers,” in *Proceedings of the 2011 Workshop on Context-awareness in Retrieval and Recommendation*, 2011, pp. 39–42.

[119] A. Vellino, “A comparison between usage-based and citation-based methods for recommending scholarly research articles,” in *Proceedings of the American Society for Information Science and Technology*, 2010, vol. 47, no. 1, pp. 1–2.

[120] A. Vellino and D. Zeber, “A hybrid, multi-dimensional recommender for journal articles in a scientific digital library,” in *Proceedings of the 2007 IEEE/WIC/ACM International Conference on Web Intelligence*, 2007, pp. 111–114.

[121] Y. Wang, E. Zhai, J. Hu, and Z. Chen, “Claper: Recommend classical papers to beginners,” in *Seventh International Conference on Fuzzy Systems and Knowledge Discovery*, 2010, vol. 6, pp. 2777–2781.

[122] S. Watanabe, T. Ito, T. Ozono, and T. Shintani, “A paper recommendation mechanism for the research support system papits,” in *Proceedings of the International Workshop on Data Engineering Issues in E-Commerce*, 2005, pp. 71–80.

[123] A. Woodruff, R. Gossweiler, J. Pitkow, E. H. Chi, and S. K. Card, “Enhancing a digital book with a reading recommender,” in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2000, pp. 153–160.

[124] C. Yang, B. Wei, J. Wu, Y. Zhang, and L. Zhang, “CARES: a ranking-oriented CADAL Recommender System,” in *Proceedings of the 9th ACM/IEEE-CS joint conference on Digital libraries*, 2009, pp. 203–212.

[125] F. Zarrinkalam and M. Kahani, “SemCiR - A citation recommendation system based on a novel semantic distance measure,” *Program: electronic library and information systems*, vol. 47, no. 1, pp. 92–112, 2013.

[126] F. Zarrinkalam and M. Kahani, “A New Metric for Measuring Relatedness of Scientific Papers Based on Non-Textual Features,” *Intelligent Information Management*, vol. 4, no. 4, pp. 99–107, 2012.

[127] D. Zhou, S. Zhu, K. Yu, X. Song, B. L. Tseng, H. Zha, and C. L. Giles, “Learning multiple graphs for document recommendations,” in *Proceedings of the 17th international conference on World Wide Web*, 2008, pp. 141–150.

[128] Adomavicius G, Tuzhilin A. Context-aware recommender systems. InRecommender systems handbook 2015 (pp. 191-226). Springer US.

[129] Zhan J, Hsieh CL, Wang IC, Hsu TS, Liau CJ, Wang DW. Privacy-preserving collaborative recommender systems. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). 2010 Jul;40(4):472-6.

[130] Zhou T, Kuscsik Z, Liu JG, Medo M, Wakeling JR, Zhang YC. Solving the apparent diversity-accuracy dilemma of recommender systems. Proceedings of the National Academy of Sciences. 2010 Mar 9;107(10):4511-5.