Multi-Agent Domain Model of Risk Aware and Privacy Preserving Web Recommender System

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 increase in the accuracy and better personalization of the recommendations. These results are being achieved by gathering more user data and generating insights from it. However the privacy concerns of the user are often under estimated and ignored. In fact, many users are not sufficiently aware of the data that is collected or if such data is sold to third party. Moreover, the generated recommendations do not take into account the factors such as user intention and the current situation of the user situation.

Research in the area of web recommender system should strive towards not only achieving high accuracy of the generated recommendations but also maintain user privacy and making recommender systems aware of the user context in terms of intentions of the user and the current situation of the user. Through research it has been established that a tradeoff is required between accuracy, privacy and risk in a recommender system and that it is highly unlikely to have recommender system having a high value of all those attributes. Nonetheless, a significant attempt can be made to describe a system based on the level of inclusion of those attributes within the recommender system.

This thesis focuses on the multi agent domain model of a web recommender system in which a system is described as a point in the privacy space and the risk space. The web recommender system is viewed as consisting of multiple subsystem, operated by an agent having a specific role in order to achieve a prescribed goal by performing activity in order to sustain that subsystem. Such a description of a system will be able to represent a small subset of web recommender systems which can be classified as risk aware and privacy preserving web recommender system. A case study of stock recommendation system will reveal that such system can be enabled to have risk aware and privacy preserving features to be enlisted as a subset of recommender systems that can be described by the multi agent domain model.

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.

Table of Contents

List of Figures

I

List of Tables

No table of figures entries found.

Chapter 1
Introduction

Introduction comes here.

1.1 Research Issue

Issues come here

1.2 Major Contributions

Contributions

1.3 Thesis Organization

The thesis is divided into three parts. The first part introduces and motivates the problem addressed, along with a survey of the Recommender Systems field and brings into light the risk and privacy issues, where this thesis is framed. The second part describes the related work in the recommender systems literature and provides an analysis of the design alternatives and statistical biases that may arise. It also provides a detailed discussion of the proposed approach to solve the issues with the existing domain models of the web recommender system. Towards the end of this part a brief case study of this domain model is show in context of portfolio recommender system. The last part describes the work to be done in the future to extend this domain model.

In more detail, the contents of this thesis are distributed as follows:

Part I. Introduction

Chapter 1 presents the motivation, research goals and contributions.

Chapter 2 provides an overview of the state of the art in recommender systems, considering 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 the risk and privacy issues in the recommender systems.

Part II. The Domain Model

Chapter 3 related work

Chapter 4 presents proposed approach

Chapter 5 presents the case study

Part III. Future work

Chapter 6 future work

Appendix A presents details for future work

Chapter 2
Recommender Systems

Recommender systems typically produce a list of recommendations in one of two ways – through collaborative and content-based filtering or the personality-based approach.[7] Collaborative filtering approaches building a model from a user's past behavior (items previously purchased or selected and/or numerical ratings given to those items) as well as similar decisions made by other users. This model is then used to predict items (or ratings for items) that the user may have an interest in.[8] Content-based filtering approaches utilize a series of discrete characteristics of an item in order to recommend additional items with similar properties.[9] These approaches are often combined into Hybrid Recommender Systems.

2.1 Context Aware Recommender Systems

When recommending a personalized content, it is not sufficient to consider only user's profiles and documents. It is also important to recommend documents adequate to the user's situation. Therefore, a good recommendation depends on how well the recommender system (RS) has incorporated the relevant contextual information into the recommendation process. Recently, some RS have taken the context into account, being called Context-Aware Recommendation System (CARS). However, for a long time many works deal with the context in other areas, like IR, mobile-learning and advertising since context become inescapable. The notion of context appeared in several disciplines, like computer science, linguistics, philosophy, psychology, etc., and every discipline gives its own definition, often different from the others, which is more specific than the generic definition i.e. "conditions or circumstances that have an effect on something". Therefore, there are several definitions of context across varied disciplines. In context-aware computing, the authors in [26] have considered the context as a key component to increase human-machine interactions, and they have given the subsequent definition of context that is now ordinarily accepted: "Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves." [37]. According to Grudin [39], the context acquisition is the process through which contextual information is captured. The context can be obtained by different methods, depending on the contextual information that the system needs. Context models formalize the representation of the context as a structure (ontology, class of vectors of terms, set of concepts,

etc.) or a set of specific and different information structures. We present now the most interesting models found in the literature. The most simple context models are based on attribute-value pairs to represent context, where attributes capture various characteristics of contextual elements.

2.2 Privacy in Recommender Systems

Because users need to reveal information in order to make use of the desired functionality of a recommender system, a trade-off exists between utility and user privacy. Obtaining accurate recommendations is one thing, but sharing personal information may also lead to privacy breaches. In this section, we will look into privacy in recommender systems and potential privacy concerns with a focus on user privacy.

2.2.1 Information in Recommender System

We will summarize the types of information typically used in a recommender system and the information flow in the recommender system. This is a brief discussion to explore the diversity of information used in recommender systems

Behavioral information is the implicit information that the recommender system can gather while the user interacts with the broader system. For example, product views in a webshop or not fully watching a movie on a video on demand site.

Contextual information describes to the context in which a recommendation query is made. Common examples of contextual information are location, social group, time, date, and purpose.

Domain knowledge specifies the relationship between a user stereotype and content items. Domain knowledge is usually static but can change over time. *Item metadata* is descriptive information about content items. Examples of metadata are kitchen for restaurants, genre for movies, and artist for music.

Purchase or consumption history is the list of content that has previously been purchased or consumed by the user.

Recommendations are the output of a recommender system, typically a ranked list of items. In some systems, the relevance score for each content item is also given to the user.

Recommendation feedback is information about the recommendation provided by the user. Feedback can be expressed as positive, negative, or something more nuanced (stating a reason as well).

Social information describes the relationship between different users. Many sites allow users to specify a friendship relation (or similar) to other users, community membership, or both.

User attributes describe the user. Examples of user attributes are demographic information, income, and marital status.

User preferences are explicitly stated opinions about items or groups of items. Preferences are expressed by either a scalar measure (rating items on a scale of 1–5 stars), a binary indicator (keeping a list of favorites), or text (tags and comments).

2.2.2 Privacy and Confidentiality

The word privacy has many subtly different meanings, each with their own definition. Privacy on the Internet revolves mainly around *information privacy*. Kang [20] used the wording of the Information Infrastructure Task Force (IITF), as cited below:

Information privacy is "an individual's claim to control the terms under which personal information – information identifiable to the individual – is acquired, disclosed or used."

This concept of information privacy is strongly related to the notion of *confidentiality*, from the field of information security, but not to be used interchangeably. Confidentiality is concerned with the secrecy of individual pieces of information. Information privacy focusses on the individual who is the subject of said information, the effects that disclosure have on this person, and his or her control and consent. In our overview of privacy-protection technologies, the focus will lie on preventing unwanted disclosure and usage of information, but not on the effects on the person. When using online applications, users generally share a lot of (personal) information. Whether it is uploading ratings or comments, posting personal information on a profile, or making purchases, information is always shared within a particular *scope* [28]. Privacy involves keeping a piece of information in its intended scope. This scope is defined by the size of the audience (breadth), by extent of usage allowed (depth), and duration (lifetime). When a piece of information is moved beyond its intended scope in any of these dimensions (be it accidentally or maliciously), a privacy breach occurs. So, a breach may occur when information is disclosed to a party for whom it was not intended, when information is abused for a different purpose than was intended, or when information is stored beyond its intended lifetime. Weiss [39] stated that on the traditional Web, privacy is maintained by limiting data collection, hiding users' identities, and restricting access to authorized parties only. Often, in practice, information and identity become closely linked and visible to large groups of people.

Profiles may be publicly visible, comments can be seen by all viewers of a content item, and some sites list the last users to visit a particular page. It becomes harder for a user to monitor and control his personal information, as more of it becomes available online. This problem mainly applies to systems where the user logs in to an account and where tools are available to express a user's preferences. Often, users are not very aware of their (lack of) privacy. In a study on social network users in particular, Gross and Acquisti [18] showed that most users do not change the default privacy settings, while sharing a large amount of information on their profile. Tufekci [38] concluded in his case study that privacy-aware users are actually more reluctant to join social networks, but once they do join, they still disclose a lot of information. As opposed to social networks, in most recommender systems, privacy toward other users is probably not the largest issue. Users place a lot of implicit trust in service providers, expecting them to handle user information in a fair and conscientious way and continue to do so in the future. By using the system, users enter into a relationship with the service provider, who can generally view *all* information in the system, including private uploads, browsing and purchase behavior, and IP addresses. It is also the service provider who decides which information is stored, how long it is kept, and how it is used or distributed. Usually, privacy statements are offered to display the position the service provider takes and to acquire the user's consent. However, this leaves users little choice: they can either agree to the terms or will not benefit from using the system. The power balance is clearly in favor of the service provider.

Privacy breaches can involve a variety of parties (fellow users, the service provider, or outsiders) and may be a deliberate act (snooping, hacking), or accidental (mismanagement, lingering data). Depending on the sensitivity of information involved, such incidents may have serious consequences. Lam et al. [23] already identified some threats to privacy in recommender systems. Their concern is the amount of (personal) information that is collected by the service provider and the potential leakage of this information. Independent of their work, we explicitly identify the privacy concerns in recommender systems and classify them as follows:

Data Collection. Many users are not aware of the amount and extent of information that a service provider is able to collect and what can be derived from this information. This may be due to the fact that privacy statements are seldom read, and people have become used to pursuing online activities. Usually there is no way to opt-out of such data gathering, other than not using the system at all. As collection practices do not match with the users' expectations, this concern relates to the extent of information usage.

Data Retention. Online information is often difficult to remove, the service provider may even intentionally prevent or hinder removal of data. This is because there is commercial value in user information, for both competitive advantage through analysis and/or data sales. Furthermore, information that is apparently erased from one place may still reside somewhere else in the system, for example, in backups, to be found by others. The data retention concern relates to the intended lifetime, as information can be available longer than intended.

Data Sales. The wealth of information that is stored in online systems is likely to be of value to third parties and may be sold in some cases. Users' ratings, preferences, and purchase histories are all potentially interesting for marketing purposes. Data sales usually conflicts with the privacy expectations of users. Even though data is often anonymized before being sold to protect user privacy, re-identification is a threat that is often overlooked or ignored. For example, the information published by Netflix as part of their recommender systems prize, though anonymized, allowed for re-identification [27]. Narayanan and Shmatikov linked the anonymized records to publicly available records (such as IMDb) based on rating similarity and time of rating. If two records give a similar rating to a movie around the same time, they are likely to be from the same person. A higher number of similar movie ratings (in rating and in time) increases the confidence of the link between the records. This concern relates mainly to the extent of information usage.

Employee Browsing Private Information. The service provider as an entity has full access to the information, and its employees might take advantage of this. This is in conflict with the intended breadth of the audience, and the privacy that the service provider has promised its users.

Recommendations Revealing Information. Recommendations inherently are based on the information contained in the recommender system. For example, in collaborative filtering that information is the ratings of all the users, or in knowledge-based recommender systems it is the expert knowledge. Each recommendation reveals a tiny piece of information about the private information. It is unclear how a large number of recommendations impact the disclosure of information. This could be used to reveal information about other users (compromising their privacy) or information about the recommender system itself (potentially leading to reverse engineering of the system). Here, we focus on the privacy of the user, not the security of the system. Ramakrishnan et al. [31] looked at the privacy of eccentric users (users with unusual ratings) from a graph perspective. When looking at recommendation results, these users are at a higher risk than average users. As eccentric users cannot hide in crowds of other users, when their data is used for making recommendation, other data is often not. The

recommendations output by the system are then based on only a few users, with a strong correlation between the input of the eccentric users and the recommendation output. This is in conflict with the intended breadth of the audience.

Shared Device or Service. Privacy at home can be just as important as privacy online. When sharing a device like a set-top box or computer, or a login to an online service, controlling privacy toward family and friends may be difficult. For example, a wife who wants to hide from her husband the fact that she purchased a gift for him. Unless she has a private account, her husband might inadvertently see her purchase or receive recommendations based on it. Many would want to keep some purchases private from their kids or their viewing behavior from their housemates. While some services allow for separate accounts, this is not always possible. For example, targeted advertising works with cookies that are stored in the browser, which is implicitly shared on a computer. This is related to the intended breadth of the audience.

Stranger Views Private Information. Users can falsely assume some information to be kept restricted to the service provider or a limited audience, when in reality it is not. This can be due to design flaws on the part of the service provider or a lack of the user's own understanding or attention to his privacy. When a stranger views such private information, there is a conflict with regard to the intended breadth of the audience. Rosenblum [33] showed, for example, that information in social networks is far more accessible to a widespread audience than perceived by its owners.

2.2.3 Privacy Protection

We have seen a wide variety of privacy issues associated with recommender systems. Research from many areas could be applied to alleviate some of the aforementioned concerns. We will provide an overview of research areas and briefly discuss their mechanisms, advantages, and limitations.

2.2.3.1 Anonymization, Randomization and Differential Privacy

Anonymization involves removing any identifying (or identifiable) information from the data, while preserving other structures of interest in the data. This mainly stems from the fact that information can only be *partially* removed or obfuscated, while other parts *must be kept intact* for the dataset to remain useful. In the real world, it is difficult to predict which external sources of information may become available, allowing pieces of data to be combined into identifiable information. When looking

at anonymization during recommendation, Ciss´ee and Albayrak [11] utilized trusted agents (essentially moving the trust around) to act as a relay and filter the information that is sent. This way, the user can interact (through the agent) with the recommender system in an anonymous way. The user hides his personal information from the service provider and is safe from the service provider linking his rating information to a person. However, the user still needs to trust that the agents (either hardware or software based) and the service provider do not collude.

Similar to anonymization is randomization. In randomization (sometimes referred to as perturbation), the information fed into the system is altered to add a degree of uncertainty. Polat and Du [29] proposed a singular value decomposition predictor based on random perturbation of data. The user's data is perturbed by adding a random value (from a fixed distribution) to each of the ratings; unknown ratings are filled in with the mean rating. They go on to show the impact on privacy and accuracy and their inherent trade-off due to perturbation. In later work [30], their setting is different. A user wants two companies to collaboratively compute recommendations for him. This user acts as a relay for the two companies. The user's privacy is based on randomizing values. Berkovsky et al. [6] proposed to combine random perturbation with a peer-to-peer structure to create a form of dynamic random perturbation. For each request, the user can decide what data to reveal and how much protection is put on the data. Different perturbation strategies are compared based on accuracy and perceived privacy. Shokri et al. [35] added privacy by aggregating user information instead of perturbing. Aggregation occurs between users, without interaction with the recommender system. Thus, the recommender system cannot identify which information is part of the original user information and what is added by aggregation. A degree of uncertainty is added to the user's information similar to randomization. Recently the field of randomization is shifting toward differential privacy [13], which aims to obscure the link between single users' information in the input (the user's information) and output (the recommendation). This is accomplished by making users in released data computationally indistinguishable from most of the other users in that dataset. This is typically accomplished by adding noise to the inputs or output, to hide small changes that arise from a single user's contribution. The required level of noise depends on how and how often the data will be used and typically involves a balancing act between accuracy of the output and privacy of the input. Such indistinguishability also applies strongly to collaborative recommender systems, where a user should be unable to identify individual peers' ratings in the output he receives. As each recommendation leaks a little bit of information about the input (even with noise), with a larger number of recommendations, the added noise should be greater to provide the same level of privacy.

McSherry and Mironov [26] proposed collaborative filtering algorithms in the differential privacy framework. Noise is added to the item covariance matrix (for item similarity). Since the item covariance matrix is smaller than the user covariance matrix, less noise needs to be added and more accuracy is preserved. The drawback of these techniques is that the security of these methods is hard to be *formally proven*, as is done in classical cryptography. The noise levels in differential privacy techniques must not overwhelm the initial output data and thus remove utility of the results completely. At the same time, enough noise must be added in order to hide the contribution of a user. When combined with multiple computational results and external information, even more noise is needed to protect the privacy of a user.

2.2.4 User control

In addressing privacy concern issues in recommender systems, much attention has been put on creating solutions, such as granting users control over information release [31] or providing disclosure justifications [27]. In principle, control enables users to better manage their information flow and make decisions on information sharing, so as to reduce concerns about privacy.

2.3 Risk Aware Recommender Systems

This requirement expresses the ability to be aware of the risk level of the user's situation during the recommendation process in order to not recommend documents in risky situations for example. Three techniques are pro- posed to compute the risk. The "variance of the cost" approaches ([80, 1]) have the advantage to be not user dependent but they still have the deal with the cold start problem. The expected environment cost" approaches [60, 122, 55] have the disadvantage to depend on manually tuning techniques. The hybrid approaches ([41]) have been developed by combining the two latest techniques so that, the inability of the "expected environment cost approach" to detect new dangerous states (cold start) is reduced by "the variance of the cost approach" [41], but they suffer from the lack of semantic.

Chapter 3
Related Work

Introduction comes but how are you at all if.

Chapter 4
Proposed Approach

In this chapter we will discuss a multi-agent domain model of the web recommender system. In this model we will break-down the system into subsystems which achieves a pre-defined task. Each sub system will consist of an agent. For the specification of the problem domain to be solved, we will focuses on modeling goals, roles, activities and interactions of the agents. Agents have knowledge and use it to exhibit autonomous behavior. A subsystem is composed of agents with specific goals that establish what the subsystem intends to reach. The achievement of specific goals allows reaching the general goal of the entire system.

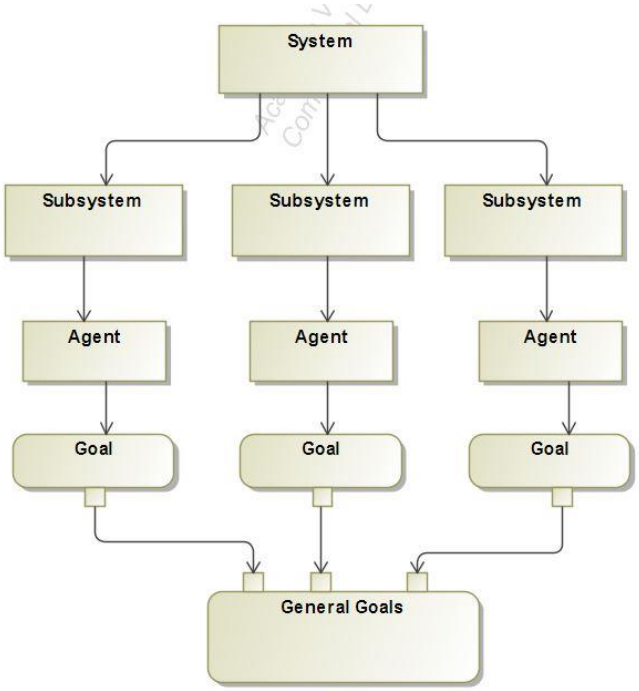

Figure 1 Description of system constituents

Specific goals are reached through the performance of responsibilities that agents have by playing roles with a certain degree of autonomy. Responsibilities are exercised through the execution of activities. 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. Preconditions and post-conditions may need to be satisfied for/after the execution of an activity. 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 to access and structure its information sources. Sometimes, agents have to communicate with other agents to cooperate in the execution of an activity.

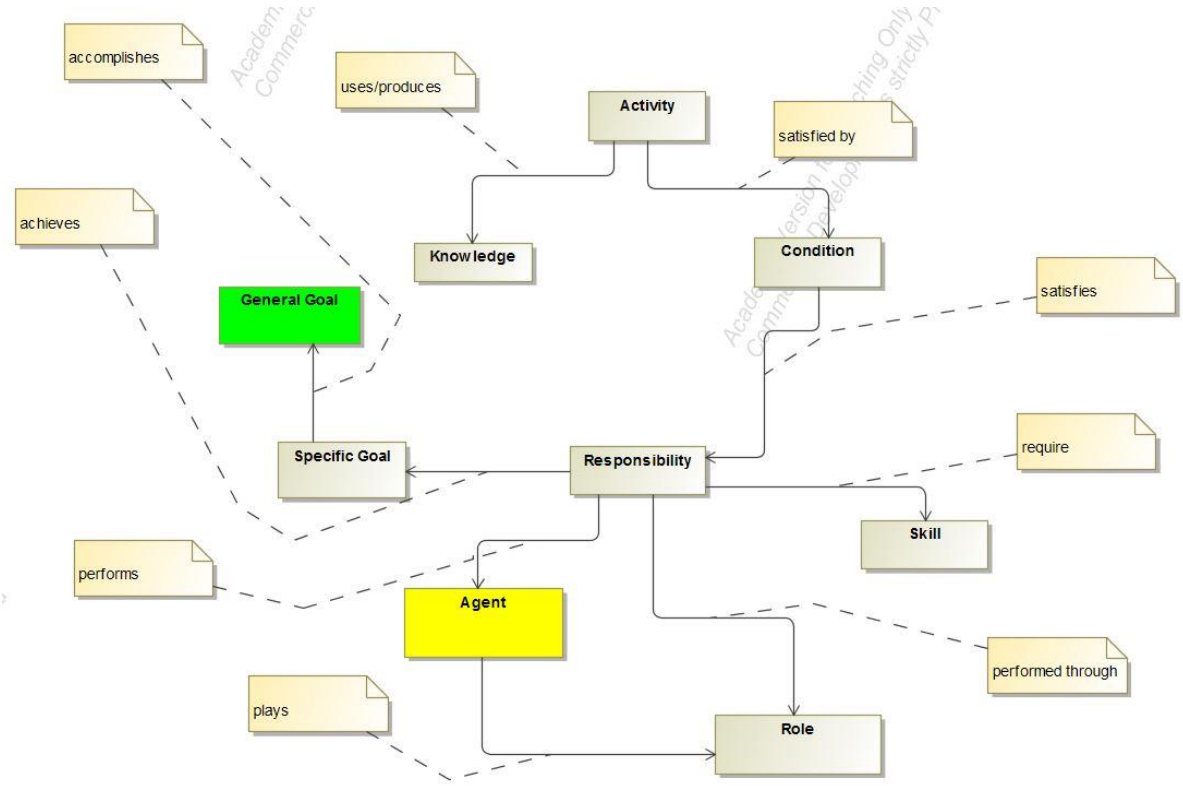

Figure 2 Relationship model for subsystems

4.1 Subsystems

We will now list out the subsystems which makes up a risk aware and privacy preserving web recommender system and also explain the contribution of each sub systems and the agents involved in the respective subsystems.

4.1.1 Data Subsystem

The data subsystem manages is responsible for managing the data in and out of the recommender system. This subsystem absorbs data in form of User Preferences and User feedback. It has multiple elements which performs the task that brings out the functioning of the data subsystems. This subsystem consists of two agent which are the Data Manager Agent and the Aggregator Agent.

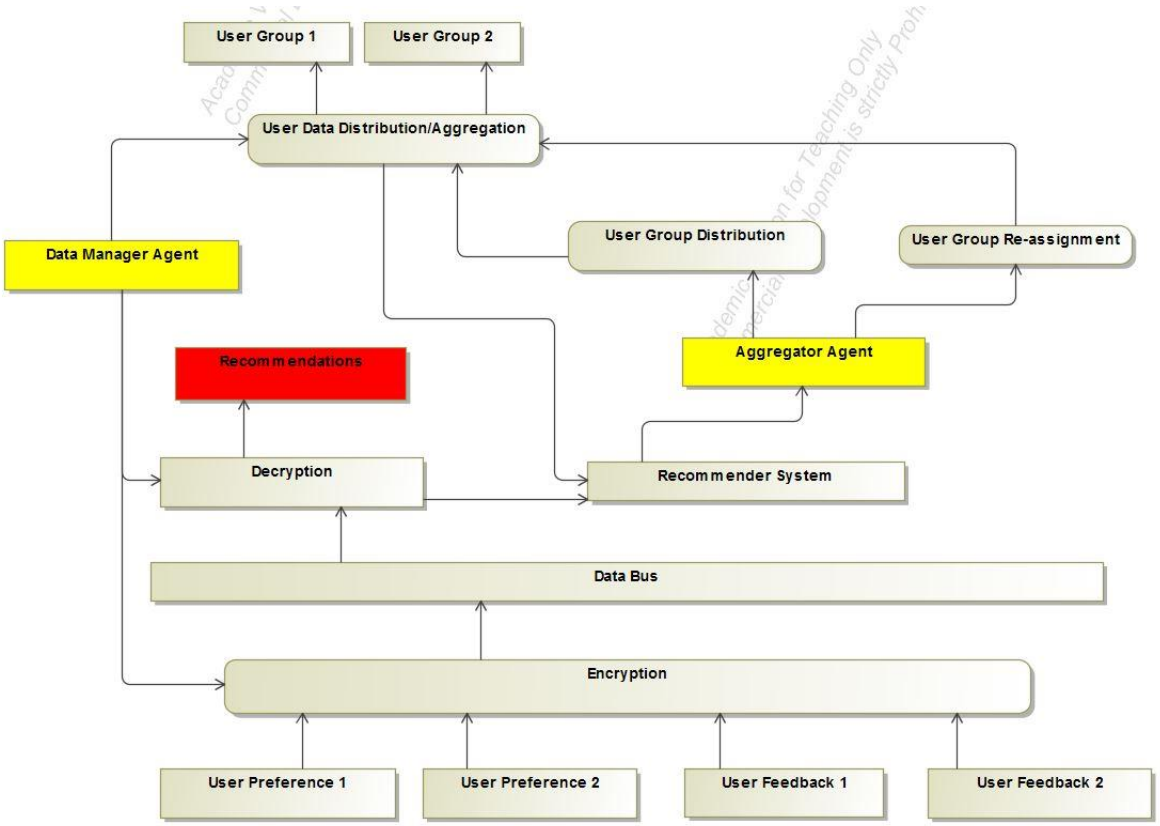

Figure 3 Data Subsystem

4.1.2 Privacy Subsystems

The Privacy subsystem manages the privacy aspect of the web recommender system. Within this subsystem the contextual and personal information is extracted from the user and fed into the recommender system. An addition differential privacy server is used to handle the differential privacy aspect of the subsystem. This sub system consist of the User Privacy Agent.

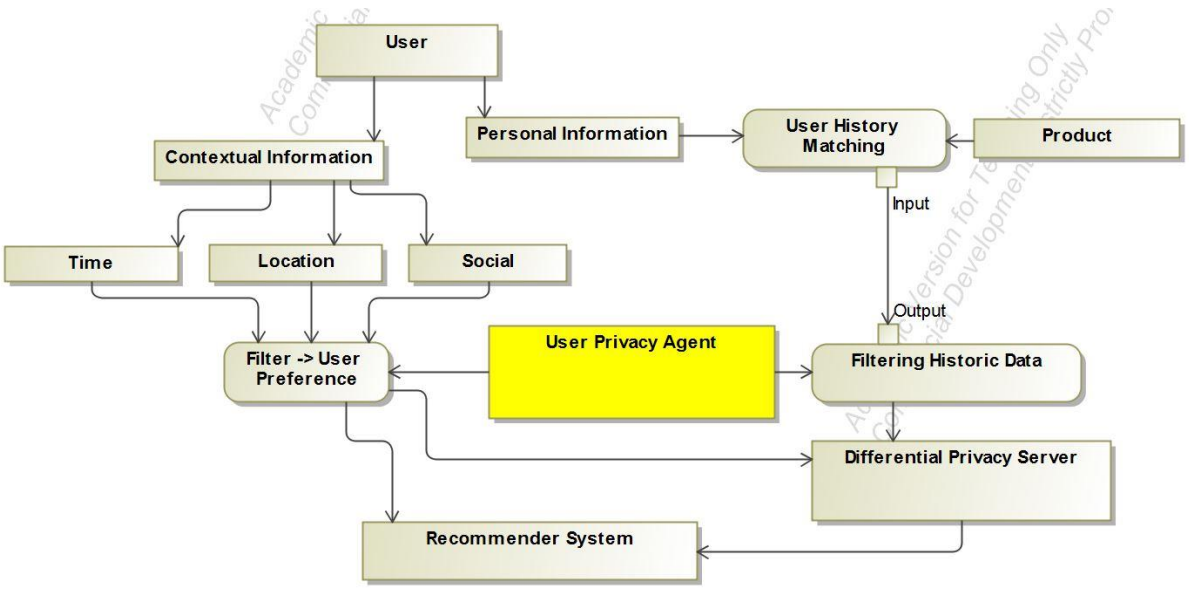

Figure 4 Privacy Agent

4.1.3 Contextual Risk Subsystem

This sub system 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 recommender system. It consists of two agents the Context Analyzer Agent and the User Risk Agent.

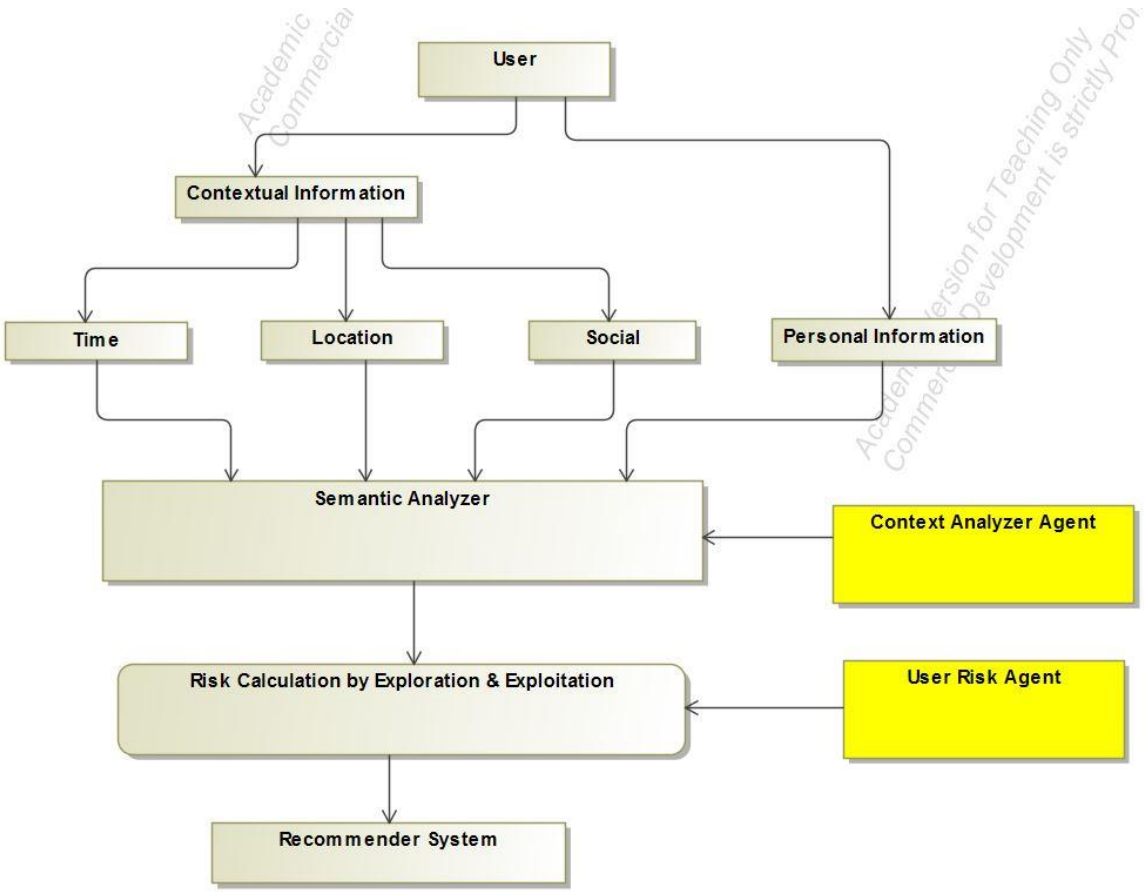

Figure 5 Risk Agent

4.1.4 Domain Model of the System

The domain model of the web recommender system consists of the aggregation of the individual subsystems and the coherence of the agents working within each work system to achieve the goals of the entire system. The advantage of breaking down the web recommender system is to provide error detection and fault tolerance within the system.

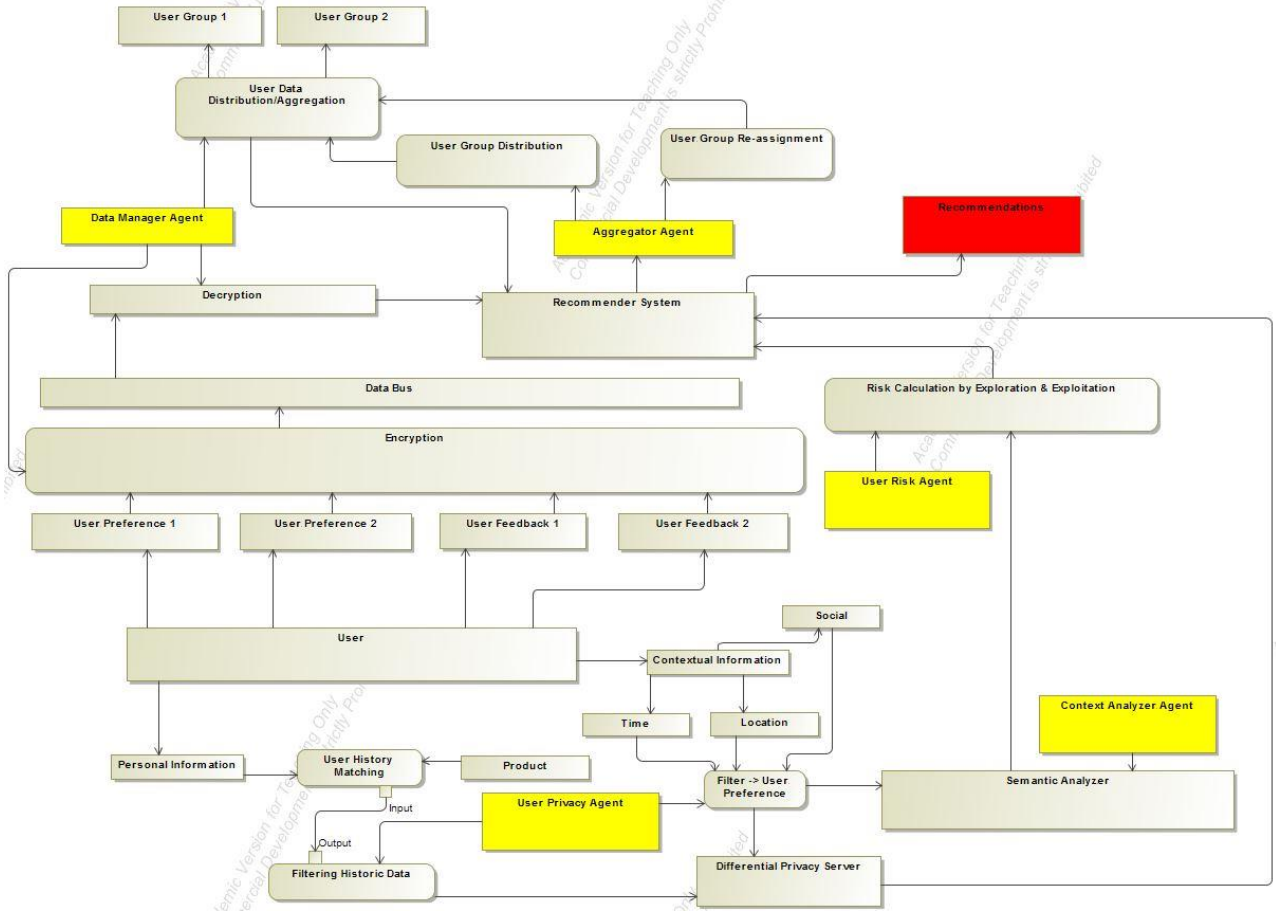

Figure 6 Complete system model

4.2 Agents

We will now discuss each agent in detail and focus on the knowledge, activities, roles, conditions, skill, responsibility and specific goals for each agent.

4.2.1 Aggregator Agent

4.2.2 Data Manager Agent

4.2.3 User Privacy Agent

4.2.4 Context Analyzer Agent

4.2.5 User Risk Agent

User Risk agent

4.3 System State Evaluation

We will now discuss the system evaluation method to determine the state of a web recommender system in terms of the degree of privacy protection and risk aware a system exhibits.

4.3.1 Privacy scope of a system

We introduce a coordinate system to describe the state of a web recommender system in terms of the privacy it offers to the user.

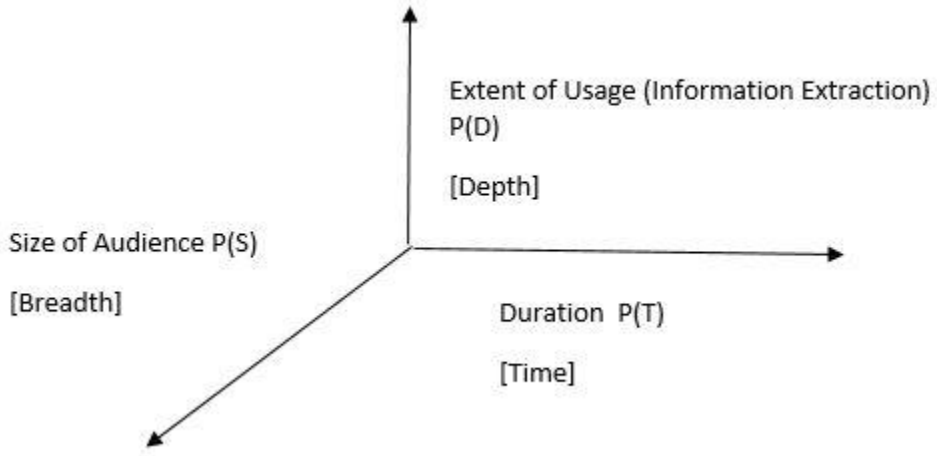

Figure 7 Privacy Scope

4.3.2 Contextual risk scope

This section describe the contextual risk scope of the system,

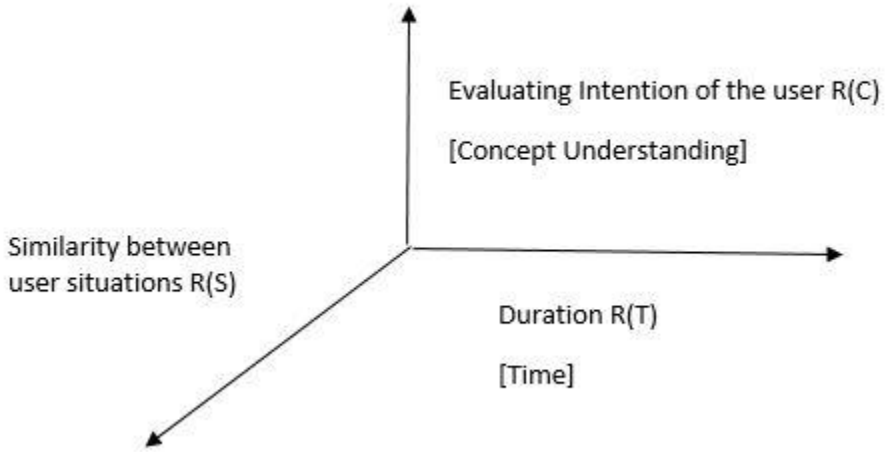

Figure 8 Contextual Risk Scope

4.3.3 Multidimensional system state

We are now in position to describe a web recommender system in five dimensions.

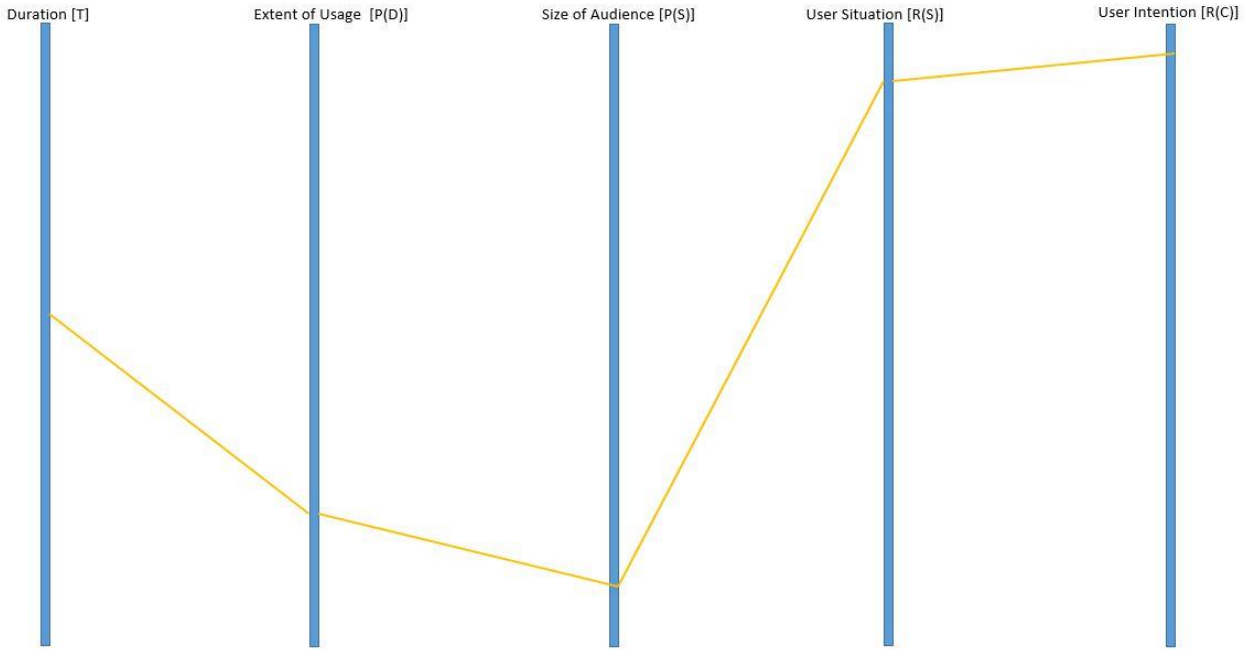

Figure 9 Dimensional Plot of a recommender System

Chapter 5
Case Study: Portfolio Recommendation

Introduction comes here.

Chapter 6
Conclusion & Future Work

Introduction comes here.

Appendix A

Formulas of the risk calculation and formulas for the differential privacy.

Bibliography

[1] Bouneffouf, Djallel, Amel Bouzeghoub, and Alda Lopes Ganarski. "Risk-aware recommender systems." *International Conference on Neural Information Processing*. Springer Berlin Heidelberg, 2013.

[2] Bouneffouf, Djallel. *DRARS, A Dynamic Risk-Aware Recommender System*. Diss. Institut National des Télécommunications, 2013.