A Privacy-Protecting Architecture for Collaborative Filtering via Forgery and Suppression of Ratings

Javier Parra-Arnau,

David Rebollo-Monedero and Jordi Forné

http://sites.google.com/site/javierparraarnau/

Department of Telematics Engineering
Technical University of Catalonia (**UPC**)
Barcelona, Spain

Leuven, Belgium

September 15, 2011

Outline

- Introduction
- State of the Art
- An Architecture for Privacy Protection in Collaborative Filtering based Recommendation Systems
- Formulation of the Optimal Trade-Off between Privacy and Utility
- Conclusions

Introduction

Information Overload

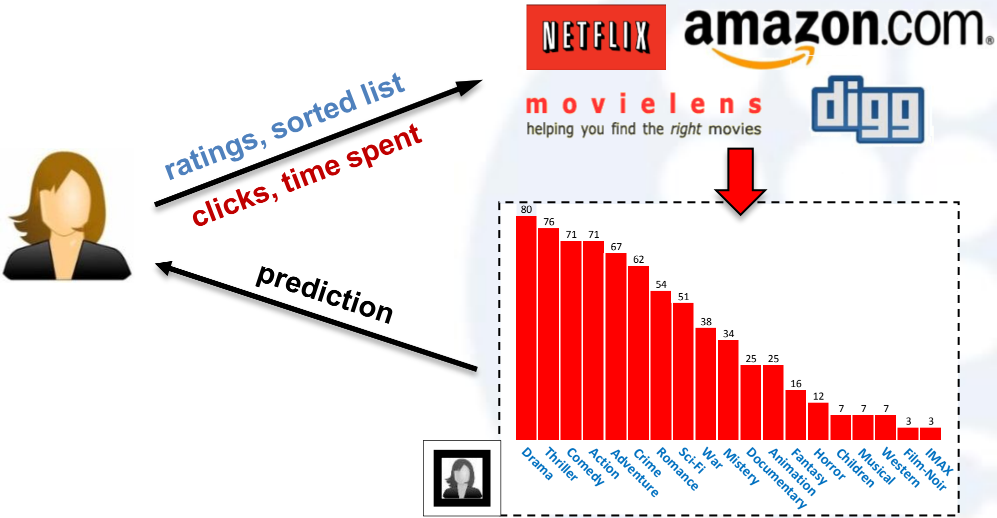
- The amount of information on the Web has grown exponentially since the advent of the Internet

Collaborative Filtering

- A recommendation system is a filtering system that suggest information items that are likely to be of interest to the user
  - Recommendation systems based on **collaborative filtering** (CF) algorithms
  - Examples include Amazon, Digg, Movielens and Netflix

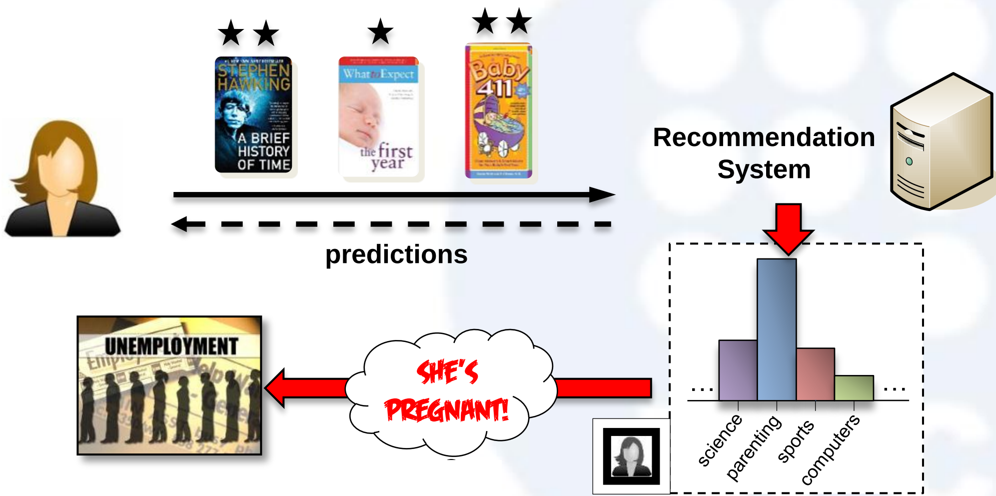
User Profiles

- Users need to communicate their preferences to the recommender in order to obtain a prediction for those items they have not yet considered



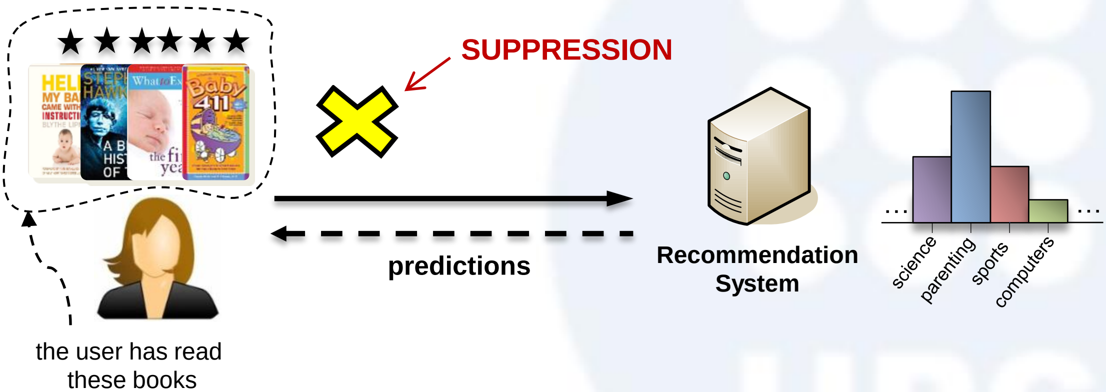
Privacy Risk

- The privacy risks perceived by users include computers "figuring things out" about them, unsolicited marketing, court subpoenas, and government surveillance [Cranor 03]



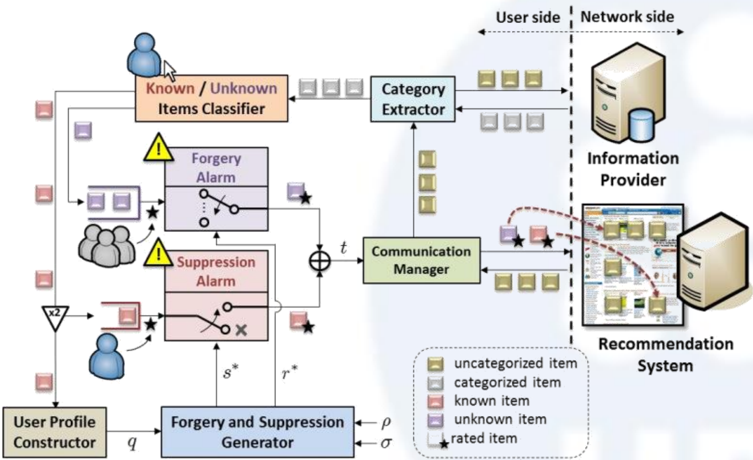
Forgery and Suppression of Ratings

- Submitting false information and refusing to give private information are strategies accepted by users concerned with their privacy [Fox 00, Hoffman 99]
- Our approach relies upon the **forgery and suppression of ratings**



Contribution (I)

- Our architecture protects user privacy to a certain extent
  - utility loss measured as forgery rate and suppression rate



Contribution (II)

- Mathematical formulation of the optimal trade-off among privacy, forgery rate ρ and suppression rate σ
  - Privacy as the Shannon entropy of the user's apparent profile

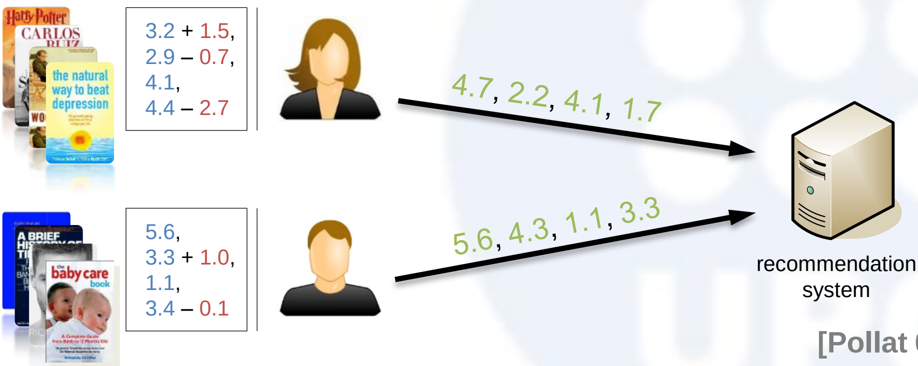
$$\mathcal{P}(\rho,\sigma) = \max_{\substack{r,s \\ r_i \geqslant 0,\, \sum r_i = \rho \\ q_i \geqslant s_i \geqslant 0,\, \sum s_i = \sigma}} \mathrm{H}\left(\frac{q+r-s}{1+\rho-\sigma}\right)$$

- Our proposal could be used in combination with other existing approaches

State of the Art

Privacy Protection in Recommendation Systems

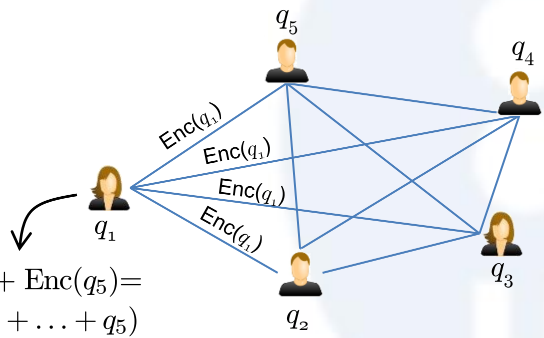
- The state-of-the-art approaches may be classified according to these main strategies
  - perturbing the information provided by users [Pollat 03, 05, Agrawal 01, Kargupta 03, Huang 05],
  - using cryptographic techniques [Canny 02, Ahmad 07, Zhan 10], and
  - distributing the information collected [Miller 04, Berkovsky 07]



[Pollat 03]

Privacy Protection in Recommendation Systems

- The state-of-the-art approaches may be classified according to these main strategies
  - perturbing the information provided by users [Pollat 03, 05, Agrawal 01, Kargupta 03, Huang 05],
  - using cryptographic techniques [Canny 02, Ahmad 07, Zhan 10], and
  - distributing the information collected [Miller 04, Berkovsky 07]

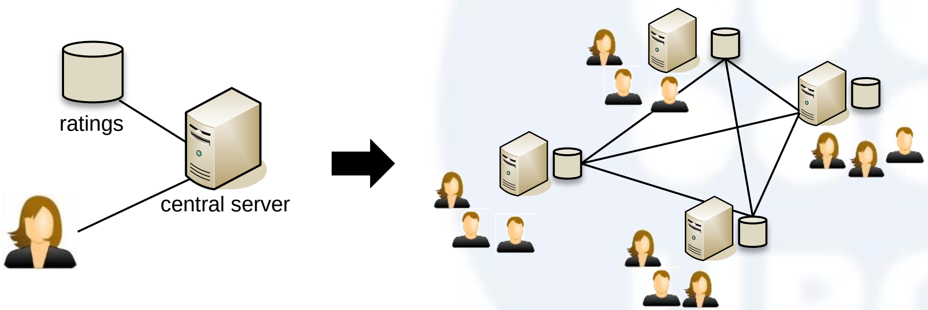


$$\mathrm{Enc}(q_1)+\ldots+\mathrm{Enc}(q_5)= \\ =\mathrm{Enc}(q_1+\ldots+q_5)$$

[Canny 02]

Privacy Protection in Recommendation Systems

- The state-of-the-art approaches may be classified according to these main strategies
  - perturbing the information provided by users [Pollat 03, 05, Agrawal 01, Kargupta 03, Huang 05],
  - using cryptographic techniques [Canny 02, Ahmad 07, Zhan 10], and
  - distributing the information collected [Miller 04, Berkovsky 07]



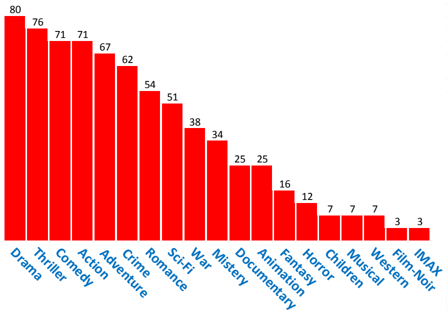
[Miller 04]

An Architecture for Privacy Protection in CF-based Recommendation Systems

Overview

- Profiling is accomplished on the basis of user ratings
- Information items are classified as **known** or **unknown**
- Users may wish to submit ratings to unknown items (forgery) and refrain from rating known items (suppression)

User Profile Model



Movielens

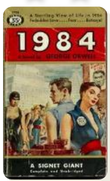
Jinni

- [Toubiana 10, Fredrikson 11] suggest representing user profiles as histograms of absolute frequencies
- We model the profile of a user as a probability mass function (PMF)

User Profile Construction

- Our architecture requires to estimate the actual profile of a user to help them decide which items should be rated and which should not
  - Histogram based on the categories provided by the recommender
  - Categorize items by exploring web pages and using the vector space model [Salton 75]

★ ★



amazon.com

books \ literature & fiction \ genre fiction

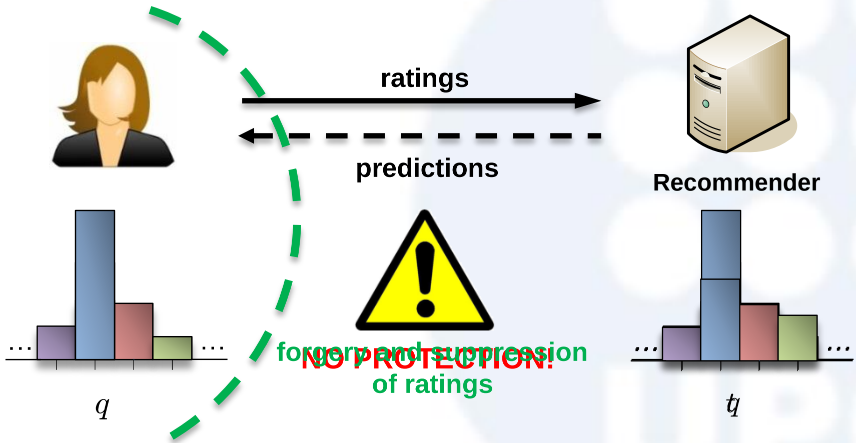

140
Undigg
Study: Why Maternity Leave Is Important
healthland.time.com — Are working moms somehow lacking as parents compared to stay-at-home mothers? According to a new demographic analysis from the National Bureau of E... Jul 21, 2011

digg

...?

Adversarial Model

- Passive attacker capable of crawling through the items rated by a user
- The attacker observes the **apparent user profile** t, a perturbed version of the **actual user profile** q



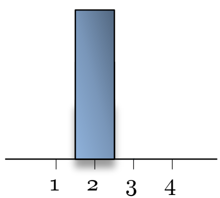
Privacy Measure

- We measure privacy as the Shannon entropy of the user's apparent profile t

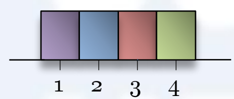
number of categories

$$\mathrm{H}(t) = \sum_{i=1}^{n} t_i \log_2 t_i$$

- Accordingly, privacy is compromised whenever the user's preferences are biased towards certain categories of interest

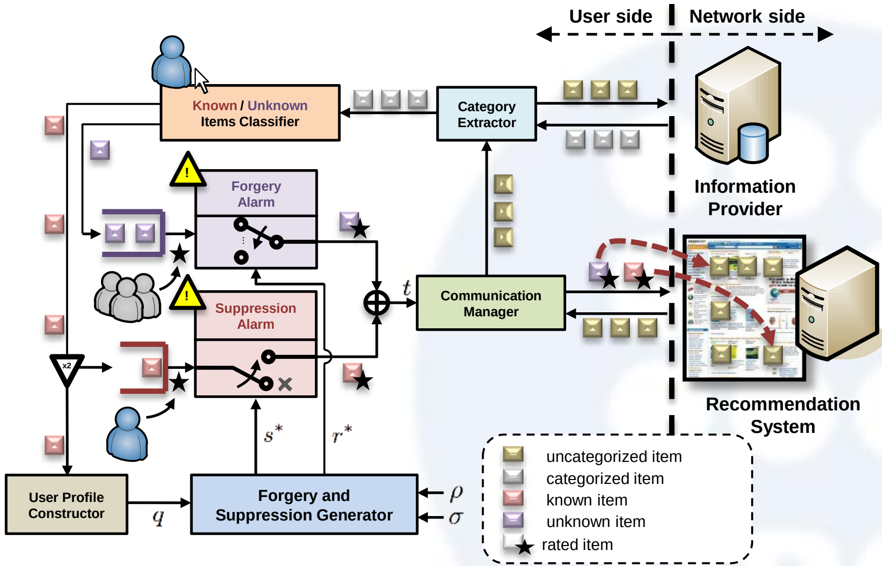


minimum privacy



maximum privacy

Architecture



Architecture

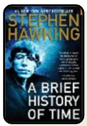
Block Functionali

- Communication with the recommender
- Retrieve information abou the items explore by the user

Description - Starting at the beginning, the book explores how JavaScript originated and evolved into what it is today. A detailed discussion of the components that make up a JavaScript implementation follows, with specific focus on standards such as ECMAScript and the Document Object Model (DOM).

Category - books \ computers & internet \ web development

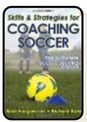
Average Customer Review 4.5/5



Description - Stephen Hawking, one of the most brilliant theoretical physicists in history, wrote the modern classic A Brief History of Time to help nonscientists understand the questions being asked by scientists today.

Category - books \ science

Average Customer Review 4/5



Description - Written by soccer great and championship Stanford coach Bobby Clark, this book tells you how, starting at point zero, an uninitiated coach can meld kids into a team and help them enjoy one of the most rewarding experiences of their youth.

Category - books \ sports \ coaching \ soccer

Average Customer Review 4.5/5

Description - You've made it! Your baby has turned one! Now the real fun begins. From temper tantrums to toilet training, raising a toddler brings its own set of challenges and questions — and Toddler 411 has the answers.

Category - books \ parenting & families \ parenting

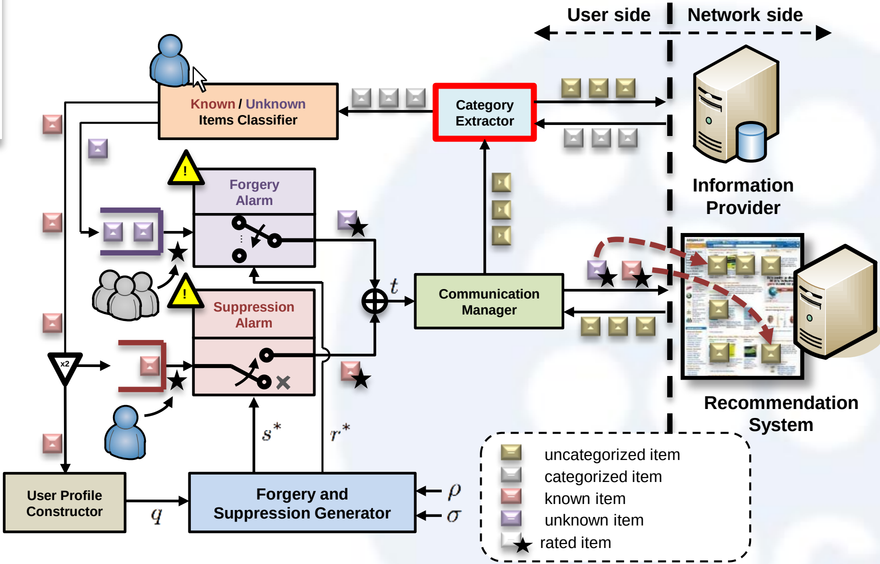
Average Customer Review 3/5

on

Architecture

Block Functionality

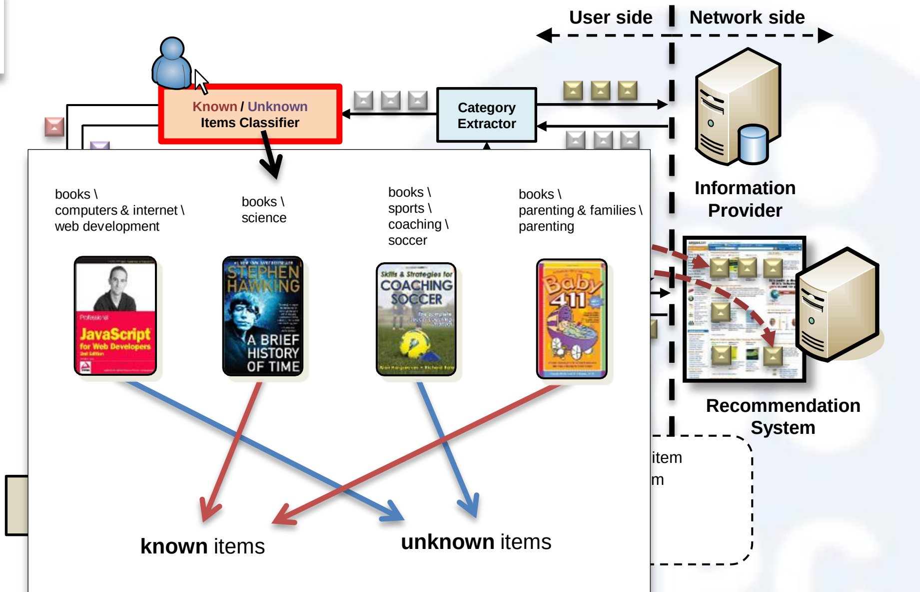
- Obtain categories associated with the items downloaded by the Communication Manager



Architecture

Block Functionality

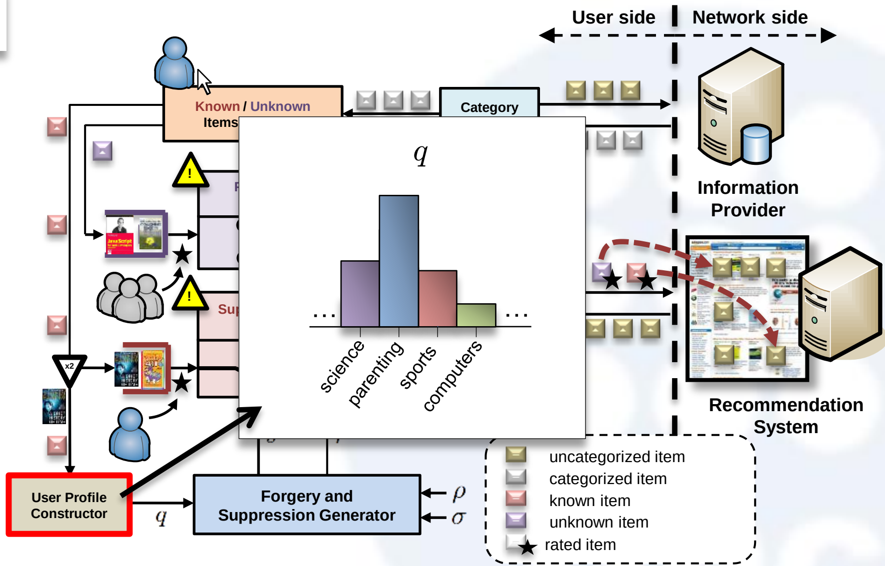
- The user classifies the items as known or unknown



Architecture

Block Functionality

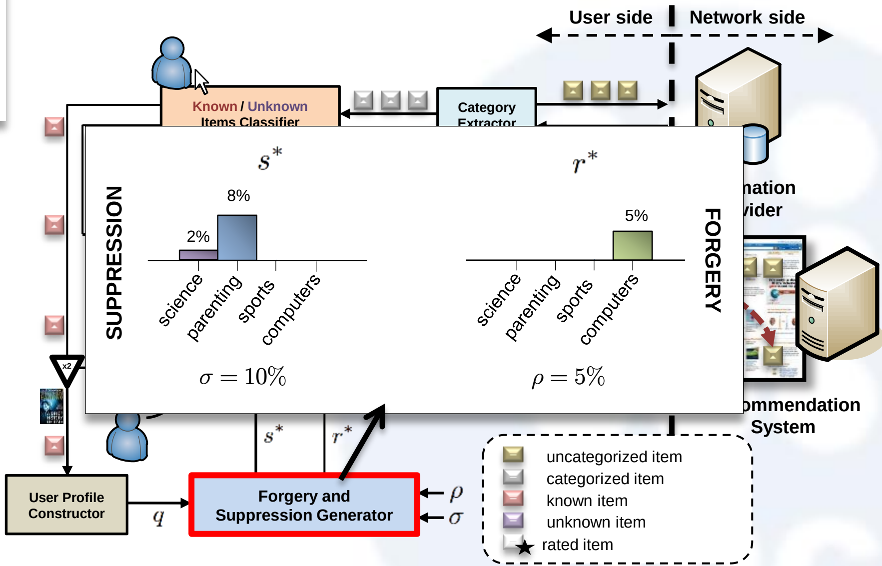
- Computes the actual user profile



Architecture

Block Functionality

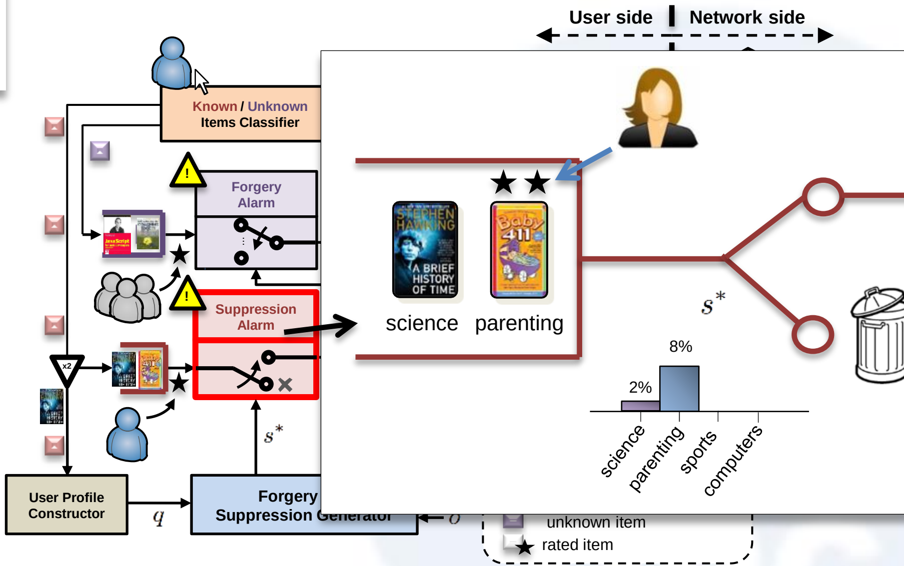
- Centerpiece of the architecture
- The user specifies a forgery rate ρ and a suppression rate σ



Architecture

Block Functionality

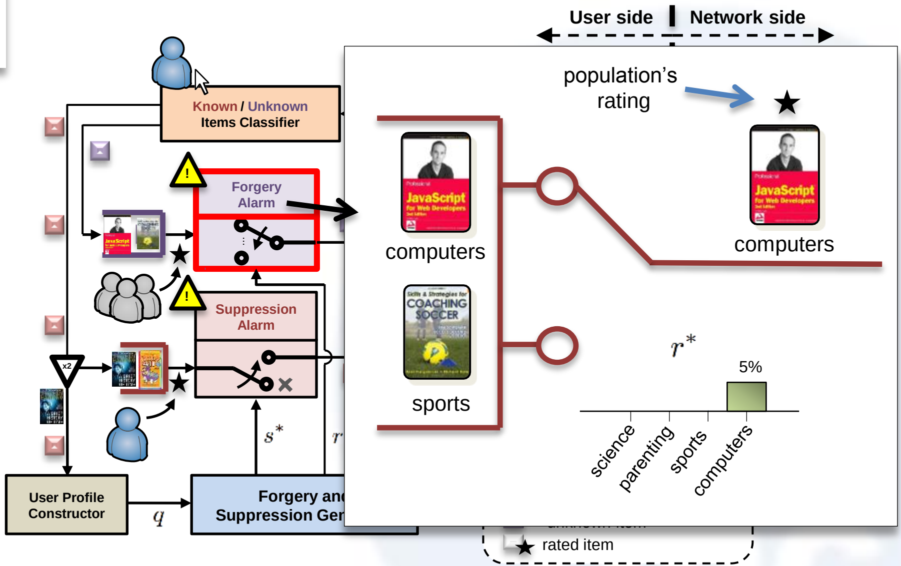
- Generate an alarm when an item should be suppressed



Architecture

Block Functionality

- Generate an alarm when an item should be forged



Formulation of the Optimal Trade-Off between Privacy and Utility

Trade-Off between Privacy and Utility

- The degradation in the accuracy of predictions is measured as σ and ρ
- We model items as r.v.'s taking on values in a common finite alphabet of n categories
- We define
  - q as the actual user profile
  - $\rho \in [0,1)$ as the forgery rate
  - $\sigma \in [0,1)$ as the suppression rate
- Accordingly, the user's apparent profile is defined as

$$\frac{q+r-s}{1+\rho-\sigma}$$

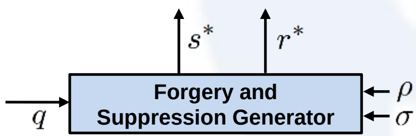
  - $r=(r_1,\ldots,r_n), r_i \geqslant 0, \sum r_i = \rho$
  - $s=(s_1,\ldots,s_n), q_i \geqslant s_i \geqslant 0, \sum s_i = \sigma$

Trade-Off between Privacy and Utility

- Privacy is measured as the Shannon entropy of the user's apparent profile
- The privacy-forgery-suppression function

$$\mathcal{P}(\rho, \sigma) = \max_{\substack{r,s \\ r_i \geqslant 0,\, \sum r_i = \rho \\ q_i \geqslant s_i \geqslant 0,\, \sum s_i = \sigma}} \mathrm{H}\left(\frac{q + r - s}{1 + \rho - \sigma}\right)$$

  - This formulation specifies the key functional block of our architecture, namely the 'Forgery and Suppression Generator'



Conclusions

Conclusions

- The forgery and suppression of ratings arise as two simple mechanisms in terms of infrastructure,
  - but it comes at the cost of a loss in utility, namely the degradation in the accuracy of the predictions
- We propose an architecture that implements these two mechanisms in those CF-based recommendation systems that profile users exclusively from their ratings
  - The centerpiece of our approach is a module responsible for computing the tuples of forgery r and suppression s
  - This information is used to warn the user when their privacy is being compromised
  - It is up to the user to decide whether to forge or eliminate a rating
- We present a formulation of the optimal trade-off among privacy, forgery rate and suppression rate

A Privacy-Protecting Architecture for Collaborative Filtering via Forgery and Suppression of Ratings

Javier Parra-Arnau,

David Rebollo-Monedero and Jordi Forné

http://sites.google.com/site/javierparraarnau/

Department of Telematics Engineering
Technical University of Catalonia (**UPC**)
Barcelona, Spain

Leuven, Belgium

September 15, 2011