**INTRODUCTION**

Traditional recommender systems that learn user’s preference from only user-item interaction data often suffer from data sparsity and cold start problem, which worsens the recommendation performance . To overcome them, social recommendation utilizes the user’s social relations as auxiliary information to help estimate users’ preferences better. Over the past recent years, extensive researches have been working on how to utilize social information to improve recommendation performance . There is a commonly accepted so-called social-trust assumption among those researches: users’ preference is similar or influenced by their social-connected friends. With this assumption, existing approaches set similarity constraints to users and their friends when estimating interests, and achieve success in improving recommendation performance. Specifically, from the perspective of representation learning, users’ preferences and interests are embedded as dense vectors in the latent space, and items’ features are the same. When the interaction function, dot product in most models, is fixed, users with close user embeddings in latent space means similar preferences towards items. Based on this, these approaches set a constraint on the distance of each

**LITERATURE SURVEY**

# Title: Location recommendation for location-based social networks,

**Author: S.berger**

**Abstract:**  we address the problem of protecting cloud infrastructures and customer workloads via smart auditing and logging, satisfying regulatory and compliance requirements. We observe that traditional approaches of logging and auditing events in cloud-scale infrastructures will not be effective without taking into account other controls. We introduce the concept of Cloud Security Intelligence (CSI), a new systematic approach for collecting, aggregating, correlating, and analyzing data from management, control, and data planes of cloud infrastructures, using a closed-loop architecture. Our approach cross-correlates control and data plane events, automatically deriving rules for monitoring and audits. Specifically, it sets dynamic rules concerning what and how to audit, adapting the logging accordingly, while comparing the data access patterns and configurations with the desired privileges and specifications. We have implemented CSI on two OpenStack ® -based systems: a closed loop network protection scheme and a cloud storage audit and risk analysis scheme for monitoring data access. In order to make cloud security approaches effective and scalable, we suggest that it is essential to use an intelligent approach such as correlating cloud logic from multiple cloud layers and components-e.g., IaaS (Infrastructure as a Service) or PaaS (Platform as a Service)-providing workload context that is maintained by cloud management systems, and using analytics on historical logs.

# Title: A recommendation system for spots in location-based online social network

# Author: D.richard yuf

# Abstract: Attribute-based access control (ABAC) is a flexible approach that can implement AC policies limited only by the computational language and the richness of the available attributes, making it ideal for many distributed or rapidly changing environments.

# Title: Exploiting geographical influence for collaborative point-of-interest recommendation

# Author: Don buneh

**Abstract:** We describe two new public key broadcast encryption systems for stateless receivers. Both systems are fully secure against any number of colluders. In our first construction both ciphertexts and private keys are of constant size (only two group elements), for any subset of receivers. The public key size in this system is linear in the total number of receivers. Our second system is a generalization of the first that provides a tradeoff between ciphertext size and public key size. For example, we achieve a collusion resistant broadcast system for *n* users where both ciphertexts and public keys are of size  for any subset of receivers. We discuss several applications of these systems

# Title: socially-aware personalized markov chains for sparse sequential recommandation

# Author: vincet.c

**Abstract:** Attribute-based access control (ABAC) is a flexible approach that can implement AC policies limited only by the computational language and the richness of the available attributes, making it ideal for many distributed or rapidly changing environments.