**Title:**

**Privacy and Security in Ubiquitous Personalized Applications**

**What is the research problem?**

Ubiquitous computing is a concept in software engineering and computer science where computing is made to appear anytime and everywhere. In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format. Personalization in such environment can be achieved based on user preferences. However, storing and exchanging potentially personal information raises user privacy concerns. The idea behind this paper is to explore a general framework to providing privacy-aware personalization in ubiquitous computing environments.

**Overview/main points of the proposed approach/architecture**

* Ubiquitous computing is the concept of using internet connected and inexpensive computers to help with everyday functions. This proliferation of computing into the physical world suggests new paradigms of human computing interaction inspired by constant access and increase in information and computational capabilities.
* Personalization is an important aspects of this new paradigm which can be achieved by user characteristics and preferences.
* These preferences are usually stored on the user devices and released in exchange for personalized services. This benefits both the user as well as the service providers as they could provide improved and differentiated services, such as, targeted advertising and loyalty reward programs. The user in turn will benefit by getting services customized to their preferences
* However maintaining such user preferences/user model and releasing them to the service provider’s raises privacy and security concerns relating to the storage, access and processing of the information contained within the model.
* Users may wish to limit and control the amount of information released to the service provider. Protecting user identity would require providing mechanisms to allow anonymous/pseudonymous interaction with personalized services.
* Mechanisms are thus required for defining relevant subsets of the user model, allowing users to control their release, and authenticating and protecting the integrity and confidentiality of the user information released to the service provider

**Related Work**

* There has been some work on adapting P3P to provide privacy in ubiquitous computing environments. User agents on user mobile devices can release contextual information based on a comparison between the privacy declaration and user preferences.
* Most of the related work has focused on providing anonymity, hiding user identity and keeping personal information secret. Participation in the social world requires disclosure of information, users need to provide information about them in order to personalize information and services. Thus, privacy needs to be seen in terms of a negotiated controlled disclosure of information.
* This paper addresses a wider notion of privacy that focuses on providing users with notice of data collection, choice regarding collection and informed consent

**Framework Design**

* The Secure Persona Exchange (SPE) framework is based on P3P with an underlying notice-choice privacy model. Personas are used to represent user information and provide personalization. The framework also contains provisions to allow access to services with varying degrees of anonymity.
* End User Requirement:
  + Purpose specification: allows users to view what benefits are offered by the personalized service and what personal information is needed to offer those benefits.
  + Openness: users should be aware of any data collection that takes place
  + Simple and appropriate controls: users want simple control over the information disclosed and the entity to which this information is released
  + Limited data retention: can be used to discover the length of the period for which service providers would store user data and preferences
  + Pseudonymous interaction: users may prefer to interact with personalized services under assumed identities
  + Decentralized control: follows a distributed architecture with user data stored on their mobile devices and thus under their control
* A persona thus captures the information regarding the user and their preferences that is needed for personalizing a particular service. Client-side personalization through personas addresses user concerns relating to the storage of personal data on systems outside their control.
* A major challenge for client-side personalization is ensuring the authenticity and integrity of user information. This is realized in the SPE framework through an Authorizing Entity responsible for creating user personas and releasing them to users. The Authorizing Entity is thus the trusted third party in the exchange and plays a role similar to the Certification Authority in PKI.

**Pseudonymous Interaction**

* The SPE framework can be combined with a network-level anonymizer to provide pseudonymous access to personalized services.
* Also the SPE framework supports pseudonymity through the concept of personas

**Security Requirements**

* From Security prospective following key attributes were considered in the SPE framework authentication, confidentiality, integrity and nonrepudiation.

**Conclusion**

* The SPE framework provides privacy-aware personalization in ubiquitous computing environments. The paper discusses in detail about the user requirements, requirements for personalization, privacy and security. In turn it describes an framework SPE which addresses these requirements