An architecture of privacy sensitive ubiquitous computing

Technology, Artificial Intelligence

Abstract

A ubiquitous computing is term resulted from IoT (Internet of Things), Artificial Intelligence and many modern technologies where many gadgets and devices allows us to access information from anywhere and anytime. In that case, primary concern is privacy due to involvement and exchanging of information among nodes like computer, mobile, laptop, printer etc. Any malicious node could steal information. It is claimed of perfect protection of things by developers but legally information is never hundred percentage protected because government have all data. Hence, It could be built where user can choose their privacy.

Introduction

Ubiquitous computing (or ubicomp) envisions a computational environment integrated into the physical world, featuring a multitude of heterogeneous computing devices interacting seamlessly to provide information when and where required. Personalization in ubiquitous computing environments would depend on detecting user characteristics and preferences and providing services based on these. 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. Service providers would benefit from being able to provide improved and differentiated services, such as, targeted advertising and loyalty reward programs. Users would benefit from receiving information and services customized to their preferences.

Security Challenges in Ubiquitous Computing

Vulnerabilities:

- The most addressed vulnerability is related to network dynamics. As mobile devices may join or leave the network at any given time, it is important for a network to self-configure.
- The second most commonly addressed challenge results from the large number of nodes that engage in network communications. Since some nodes may act selfishly (refuse to forward packets to other nodes), maliciously (seek to damage network operations) or show signs of a dynamic personality (behave strategically in a way that best benefits them, challenges occur in trust computation and management, as well as in the detection of ill-behaved nodes, which, if not handled carefully, may lead to a collapse of a whole network.
- In ubiquitous computing, it is challenging to ensure the availability of services and design security mechanisms that rely on complex computations due to the devices' resource constraints.

Defense:

- Cryptographic protocols the protocols in ubiquitous computing mostly rely on three types of cryptographic algorithms, 30% on symmetric and 29% asymmetric, while a majority of studies proposes a combination of both (hybrid approaches are proposed in 36. 5% studies).
- Authentication and access control While analyzing the studies for our SLR, we have identified a number of requirements that need to be

ensured while designing authentication and access control mechanisms for ubiquitous computing environments.

- With a rising number of devices participating in a ubiquitous computing environment, it is important that Number of trust-based solutions and cryptographic algorithms proposed over the last decade.
- Privacy protection mechanisms (10%) Negotiation approach This approach aims to find proper information to be exposed by allowing users to negotiate with the services on submitting data elements according to their privacy preferences.

One Solution for Ubiquiotous Computing Call ‘ CONFAB SYSTEM’:

- Application Developer Requirements
- Support for optimistic, pessimistic, and mixed-initiative applications
- Tagging of personal information
- Mechanisms to control the access, flow, and retention of personal information (quantity)
- Mechanisms to control the precision of personal information disclosed (quality)
- Given the choice between a simpler solution and a more powerful but complex one, we usually opted for the simpler one, to make it easier for end-users to understand what data the system knew about them and where that data was flowing, and to facilitate adoption by application developers.
- In designing and developing Confab, we had two requirements in addition to the ones listed in the previous section: making the

architecture and applications easy to understand by end-users, and easy to use by programmers.

Operators and Methods:

- The privacy tag specifies a notification address, a maximum time to live, the maximum number of past values that should be retained, and an additional request to delete the data if the requestor is not in the specified location.
- Tuples contain metadata describing the tuple (e. g., data format and datatype), one or more values, one or more sources describing the history of the data and how it was transformed, and an optional privacy tag that describes an end-user’s privacy preferences.
- Intrinsic context data represents information about that entity itself, whereas extrinsic context data represents information about an entity in relationship to another entity.
- In-methods affect what data is stored within Intrinsic Extrinsic Static Name, age, email address A room is part of a building Dynamic Activity, temperature A person is in a specific room.

Conclusion

There are many solutions been coming across through all research papers:

- Cryptographic solutions: Cryptography is somewhere considered as a interest of civil rights and because of this it is banned in some countries like Kazakistan, Pakistan, Mongolia etc.

- There are also other restrictions due to, export controls, National Security Agency involvement makes it difficult to imply.
- Authentication and access control policy has lack of internet and network standards which could be very difficult to implement due to poor (AAA-authentication, authorization and accounting) in Our current policy of Internet of things.
- Hence, Confab could be prior solution to avoid privacy in ubiquitous computing for reasons given below:
    - Ubiquitous Computing is based on programming language, so during development if application of In, Out and on operators then it will be reliable.
    - The requirements of Confab Architecture more of Agile iterative model which is depend on feedback structure.
    - From an end-user perspective, Confab facilitates the creation of three basic interaction patterns for privacy-sensitive applications: optimistic, applications where the default is to share personal information and detect abuses; pessimistic, applications where it is more important to prevent abuses; and mixed-initiative, where decisions to share information are made interactively by end-users.