International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-09

INVESTIGATIVE STUDY FOR ENHANCING SECURITY, PRIVACY USING AMBIENT INTELLIGENCE IN CONTEXT SENSITIVE SYSTEMS

Vijayakranthi Chinthala[1], Manas Kumar Yogi[2]

[1]M.Tech Scholar
Department of Computer Science and Engineering Dept.,
Indur Institute of Engineering and Technology
Siddipet, India

[2]Sr. Assistant Professor
Computer Science and Engineering Department
Elenki Engineering College
Siddipet, India

Abstract

This paper presents the conceptual mechanism in Ambient intelligence where the context sensitive behavior of the system helps user to improve their expressiveness and thereby increasing the overall productivity. This technology challenges the existing ones in present security systems where the trust levels can be compromised by malicious means. Biometric template protection mechanisms are strengthened by approaches like cancelable biometrics, Fuzzy vault scheme. We present the technology overview of RFID and discuss its limitations too. RFID privacy mechanisms highlight the design assumptions on which the RFID technology works. Finally we conclude the paper with future scope of Ambient Intelligence.

Keywords-Ambient, Context- Aware, Persuasion, Privacy, RFID, Security

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-09

1. Introduction

Ambient intelligence (AmI) is a unique concept for embedded computing that establishes on the large-scale integration of electronic devices into people's surroundings and the continuous availability of digital information to the users of such environments. Ambient intelligence implies efficient means of control that support the natural and intelligent use of such smart environments, emphasizing predominantly social aspects. Recent technological advances have enabled the minimization of embedded hardware thus helping the large-scale integration of electronic devices into people's backgrounds. In accession, efficient interaction concepts have been developed that support the natural and intelligent use of such systems, emphasizing the social aspects of the technology embedding. The resulting computing paradigm, which is called ambient intelligence (AmI), provides users with novel means to increment their productivity, increase their well-being, or enhance their expressiveness .In addition to the physical benefits provided by hardware embedding, AmI environments shows a number of characteristics that rely on adequate social embedding such as context awareness, personalization, adaptation, and anticipatory behavior. However, as the familiar box-like form factors of devices will disappear to be replaced by pointers to their functional properties embedded in the environment, new interaction concepts will be developed that differ substantially from the traditional box-related user interfaces. The classical concepts and definitions of trust and security will be challenged by the resulting AmI applications, and they need to be readdressed to meet the needs and requirements imposed by the use of obscure technologies. Although many technologies in the area of copyright protection, data encryption, digital signatures and firewalls can increase the security of AmI environments, there is a indigence to convince the end user to trust such secured AmI environments. This raises the question of persuasiveness in relation to ambient intelligence. The concept of ambient persuasion is portrayed as the extent to which AmI technology supports convincingly natural interaction with smart environments. In this section the concept and derivation of a framework for the discussion of the resulting challenges and issues are elaborated.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-09

2. Ambient Intelligence

Ambient intelligence aspire to take the integration onset of embedded devices one step further by recognizing environments that are sensitive and responsive to the presence of people. The focus of ambient intelligence is on the user and his experience from a consumer electronics perspective, which introduces several new basic problems related to natural user interaction and context-aware architectures supporting communication, entertainment, human-centered information, and service.

2.1. A Definition of Ambient Intelligence

5 key elements of ambient intelligence:

1. Embedded: many networked devices that are unified into the environment
2. Context aware: it can recognize persons and their situational requirements
3. Personalized: it can be customized towards their needs
4. Adaptive: it can change in response to actions, and
5. Anticipatory: it anticipates people's desires without conscious mediation.

2.2. Canonic Concept Involved:

The major novel thing in ambient intelligence is the involvement of the user. Most of the earlier computing paradigms such as personal, mobile, and ubiquitous computing were aimed in the first place at facilitating and improving productivity in business environments, but it goes without saying that these developments have played a major role in the development of ambient intelligence. The next step, however, is to bring connectivity, interaction, interoperability, and personalization to people and into people's homes. This is not merely a matter of introducing productivity concepts to consumer environments. It is far more than that, because a totally new interaction paradigm is needed to make ambient intelligence work. Contemporary concepts of productivity are to a large extent still based on the graphical user interface known as the desktop metaphor that was developed in the 1970s, and which has become a world standard in the mean

time. The new metaphor is needed with the same impact as the desktop metaphor but which enables natural and social interaction within AmI environments, and this is a tremendous challenge. Over the years it has become obvious from the studies conducted by researchers that the impact of efficient AmI ware is not only determined by its functionality, but also to a large extent by its persuasiveness.

2.3. Persuasion

The traditional solutions for rendering security will fail in AmI environments since these techniques focus on the communication channel and assume that the environments connected by this channel is secure. Similarly, for trust there needs to be more emphasis on the environment than on the communication channel. Since it is fundamentally different to create trust in an environment than in a communication channel, there is a need to involve different strategies for creating end-user trust in AmI environments.

These strategies impart forward a paradigm shift in user–system interaction concepts characterized by the following two alterations:

1. The role of applications and services will change from traditional access and control means towards lifestyle assistants.
2. The emphasis on perceived user value will change from usability towards creating user experiences such as presence, connectness, and immersion.

This paradigm shift in user-system interaction implies that it becomes increasingly important to obtain penetration into the human factors that influence human behavior. When considering behavioral change, three concepts appear: persuasion, motivation, and learning; see Fig.1.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-09

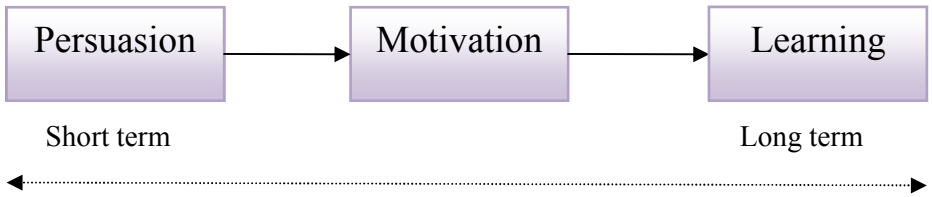

Fig.1. The relation between persuasion, motivation and learning.

Persuasion is an effort to change attitudes and/or the behavior of persons without using force or deception. A motive is a need or desire that causes a person to act. Learning is the modification of a behavioral tendency by experience that is not merely attributed to the process of growth. While persuasion reflects a momentary effect, learning implies a more long term change of behavior. How human behavior is driven or motivated and how it can be modified has been one of the most important research topics in psychology for many decades. In fact, motivation as a cause for behavior plays an important role in learning. Although motivation does not always imply learning, learning trusts on motivation to happen. Learning is defined as the modification of a behavioral tendency by experience that is not simply attributed to the process of growth.

Influencing people to change their behavior is not a new area of research. In fact, human sciences have been investigating for a long time how an individual's behavior can be changed by external factors. Whereas sociology studies the human as a member of a social structure, psychology studies the human as an individual. From a sociological point of view, an individual's behavior is determined by the societal structures of which this individual is a part. In psychology much attention has been attributed to processes of learning and behavioral change.

Technology can be persuasive due to the following actions.

- Making things easier, reducing complexity
- Supervising users through a step-by-step process

- Personalizing to the user and context
- Suggesting things to the user at the right time
- Monitoring the user so that the user can learn from himself
- Monitoring others so that the user can learn from others
- Conditioning the user

2.4. Ambient Persuasion

The term ambient persuasion is referred to use of AmI ware in a context-aware and networked infrastructure to enable context-sensitive system behavior and deliver persuasive content that is tailored to the user at the right time and at the right place. Potentially, ambient persuasion combines all the key elements of ambient intelligence, presented in the previous sections, in order to apply persuasive strategies. The following persuasive strategies as relevant are identified below.

1. Reduction supercedes a complex task by a simpler one by virtue of the introduction of automation and computation, but also by virtue of anticipation of a defining characteristic of ambient intelligence.

2. Customization and tailoring adjusts messages and content to the beliefs and needs of the person. Personalization is an essential aspect of ambient intelligence; in this case it covers not the superficial aspects of the system behavior but addressing the specific needs, problem and situation of the individual. This requires very rich, privacy-sensitive models of users that go beyond simple habits and preferences, and include aspects of their personality, their health status, the social network and context, etc. It requires embedding ambient intelligence in the social context of a person, a notion that extends the definition of ambient intelligence to cover also aspects of social intelligence.

3. Suggestion reminds people to perform certain behaviors at opportune moments. Prompting of behaviors then needs to be sensitive to context, a central aspect of ambient intelligence.

4. Self-monitoring allows people to monitor themselves and to inform themselves about how they could modify their behaviors. Self-monitoring can be very tedious; it will be argued below that ambient intelligence opens up the opportunity to facilitate this process and thus achieve persuasion.

2.4.1 Authentication measures in Ambient Intelligence:

In an ambient world, systems will anticipate and react to people's behavior in a personalized way. Clearly this requires that these systems have access to reference information linked uniquely to the individuals using the system. Consequently, in an ambient world personal information will be stored in a large number of locations and, if this personal information is not properly protected, a huge privacy problem may arise. Biometrics (i.e., fingerprints, face, iris, voice . . .) are examples of such information that is linked uniquely to an individual and is becoming increasingly popular for person identification. This is mainly due to the fact that they are very convenient to use: they cannot be lost or forgotten and therefore they are much preferred over passwords and tokens. In order to use biometrics for identification or authentication, reference information has to be measured using an enrollment device during the so called enrollment phase. This phase is carried out at a trusted authority who stores the reference information in the biometric system (e.g., a database).

During authentication a person first claims her identity. Then, the biometric of that person is measured using an authentication device and compared with the reference data corresponding to the claimed identity. When the authentication measurement and the reference measurement are sufficiently close, it is concluded that the authentication measurement originates from the person with the claimed identity and authentication is successful. In the other case, it is concluded that this person does not have the claimed identity.

There is no doubt that, when the system described above is implemented without any additional precautions, privacy problems arise. Since biometrics is unique characteristics of human beings,

they contain privacy-sensitive information. Moreover, a compromised biometric identifier is compromised forever and cannot be reissued (people have merely two eyes, ten fingers).

This stands in sharp contrast with passwords and tokens that can easily be reissued. Also, when the biometric reference information is not stored with adequate protection in a database, it can be used to accomplish cross-matching between databases and track people's behavior. A malicious employee of a bank can for instance find out that some biometric identifiers in his database also appear in the database of a night club. It is further well known that, based on the reference information in a database, pseudo biometric identifiers can be made that pass the identification test. Finally, in many countries legislation obliges institutions to properly protect the stored personal information. The threats mentioned above become less severe if the database owner is assumed (or verifier) can be trusted.

3. Requirements for Template Protection

In this section the two approaches are consider that might be considered to achieve biometric template protection. From the drawbacks of these approaches the security requirements for template protection are derived.

3.1 Naive Approaches

One might retrieve that encryption of biometric templates solves the troubles. It is to shown here that a straightforward application of encryption does not solve the privacy problem with respect to the verifier.

Assuming that symmetric key encryption scheme is used (the system works similarly for a public key scheme). All sensors get a secret key K which equalizes the secret key of the verifier. During enrollment a biometric X of a person is measured, X is encrypted with the key K and $E_K(X)$ is stored in the reference database. During authentication the measurement of the same biometric results in the value Y (close to X due to noise). The sensor encrypts the value Y with the key K

and sends $E_K(Y)$ to the verifier. The verifier is faced with the problem of comparing $E_K(X)$ with $E_K(Y)$.

However, encryption functions have the property that $E_K(X)$ and $E_K(Y)$ are very different even when X and Y are very close (but not equal). Hence, given only the values $E_K(X)$ and $E_K(Y)$ the verifier cannot decide whether X and Y originate from the same person. This implies that the verifier must decrypt $E_K(X)$ and $E_K(Y)$ to obtain X and Y and find out whether they are sufficiently standardized. But in that case the verifier knows X and hence the system does not provide privacy with respect to the verifier. It only prevents an eavesdropper from obtaining X or Y.

The problem of storing reference information also exists with password attestation. In order to protect passwords adjacent the owner of the database and eavesdropping, the ensuing measures are appropriated. During enrollment a cryptographic hash function H is applied to a chosen password pwd and the hash of the password H(pwd) together with the username or identity ID is stored in the (public) database for authentication. For example, in the UNIX system this database can be found in the directory: /etc/passwd. During authentication the identity ID and the password pwd' are entered and $(ID,H(pwd'))$ is sent to the verifier. The verifier then compares $H(pwd')$ with H(pwd) and when $H(pwd) = H(pwd')$ access is granted to the computer, otherwise access is denied. The security of this system follows from the fact that H is a one-way function: given H(pwd) it is very hard to compute pwd. Hence, for the owner of the database as well as for the eavesdropper it is infeasible to retrieve pwd from H(pwd).

Ideally, one would like to mimic the password authentication scheme in the case of biometrics. The problem is, however, that biometrics is inherently noisy and that H is a one-way function. These functions are very good for security purposes but have no continuity properties. Applying the password authentication scheme implies that H(X) is stored in the reference database.

During authentication the value Y is obtained, which is typically close to X when X and Y originate from the same person, but in general they are not equal due to noise. Therefore, due to the one-way property of H, even when X and Y are very close, H(X) and H(Y) will be very different. This means that other approaches for template protection must be considered and it is an overview of the most important existing. Before that some security assumptions and requirements for template protection systems are granted.

3.2 Requirements Security Assumptions

The scenarios in the previous section illustrate that an encryption approach to template protection does not work because the verifier must be trusted. Hashing biometric templates is not feasible because biometric measurements are intrinsically noisy. In order to come up with a template protection system, the following security assumptions are made.

- Enrollment is performed at a trusted authority (TA). The TA enrolls all users by capturing their biometrics, performing additional processing and adding a protected form of the user data to a database.
- The storage is vulnerable to attacks the pair from the outside and from the inside (malicious verifier).
- During the attestation phase an attacker is able to present artificial biometrics at the sensor.
- All capturing and processing during authentication is tamper resistant, e.g., no information about biometrics can be obtained from the sensor. The sensor is assumed to be trusted; it does not distribute measured information.
- The communication channel between the sensor and the authentication authority is public, i.e., the line can be eavesdropped by an attacker.

3.2.1 Requirements

The imperatives for an architecture that does not suffer from the threats mentioned in the introduction are:

- The information that is reserved in the database does not give sufficient information to make successful impersonation possible.
- The information in the database contributes the least possible information about the original biometrics; in particular it reveals no sensitive information about the persons whose biometrics are stored.
- When a biometric measurement of the clone person is contaminated with noise, authentication (or identification) should still be successful if the noise is not too large.

Note that an architecture that conflicts those requirements, guarantees that the biometric cannot be compromised and can handle noisy biometric measurements.

3.3 Approaches to Template Protection

Recently the template protection problem was recognized by several authors and techniques were proposed that can be used to solve the problem. In this section it is an overview of the most important techniques.

3.3.1 Cancelable Biometrics

It introduces an approach known as cancelable biometrics. During enrollment, the image of a biometric is obtained, for example, the image of a fingerprint, a face, and iris. In order to protect its privacy, the biometric image is distorted using a parameterized one-way geometric distortion function before storing it in a biometric system. The function is made such that from the distorted image it is difficult to retrieve the original image and matching can be done using the distorted images. Furthermore, using a different parameter for the distortion function, it is possible to derive several distorted images from a single biometric image (template). This allows for storing different (distorted) biometric reference information in different biometric applications (versatility) and to reissue biometric templates (renewability). Although cancelable biometrics satisfies most requirements of a biometric template protection system, its major drawback is that it is difficult to build a mathematical foundation for this approach that allows an assessment of the security properties of the system.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-09

3.3.2 The Fuzzy Vault Scheme

The fuzzy vault method is introduced for a general cryptographic construction allowing the storage of a secret S in a vault that can be locked using an unordered set X. The secret S can only be retrieved from the vault using a set Y if the sets X and Y have sufficient overlap. The authors mention biometric template protection as a possible application where X is the biometric template obtained during enrollment. During authentication, the rightful owner of the secret can unlock the vault using a measurement of his biometric Y that is sufficiently similar but not necessarily identical to the measurement X used to lock the vault. This method also has the required properties of versatility and renewability. The special property of the fuzzy vault scheme is that it can be (un)locked using unordered fuzzy sets. This makes this method well suited for biometric templates that are represented by such sets. In most cases, however, biometric templates are best represented as ordered data structures such as feature vectors. The most important exception is where fingerprints are characterized using the locations of minutiae. These locations are most naturally represented as unordered fuzzy sets and an initial attempt to use the fuzzy vault scheme in the setting of fingerprints. Little work is reported yet in using the fuzzy vault scheme for other modalities than minutiae-based fingerprints.

3.3.3 Extracting Keys from Noisy Data

The approach for extracting cryptographic keys from noisy data refers to a collection of method is developed that refer to the situation where two parties communicate over a public channel and want to derive a secret cryptographic key. The underlying mathematical principles for these methods are well understood and security proofs are available.

It was recognized that the above methods for key extraction also apply in a biometric template protection setting and work most naturally with biometric modalities that can be represented as feature vectors in a high-dimensional space. Since most biometric modalities can be represented as feature vectors, the methods for key extraction can be used to protect the templates of a wide range of modalities.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-09

Conclusion : As far as dissemination of information on personal presence is out of control, Ambient Intelligence vision is subject of criticism .Any immersive, personalized, context-aware and anticipatory characteristics brings up societal, political and cultural issues about the loss of privacy, as soon as any third party gets control over the respective information and status data. However, any disabled person may welcome the implicit information presentation and access to improve support and individual assistance. Hence there must be a distinction between solutions for personal improvement and any other purpose. Several research groups and communities are investigating the socioeconomic, political and cultural aspects of ambient intelligence. New thinking on Ambient Intelligence distances itself therefore from some of the original characteristics such as adaptive and anticipatory behavior and emphasizes empowerment and participation to place control in the hands of people instead of organizations. As long as there is no legal obligation to open one's individual status data to any access by third party, the degree of freedom, still is to stay away of any such solutions and all services with inherited methods of that type.

References

[1]. E. Aarts and J. Encarnaçao (eds.) (2006), True Visions: The Emergence of Ambient Intelligence, Springer, Berlin.

[2].E. Aarts and S. Marzano (eds.) (2003), The New Everyday: Visions of Ambient Intelligence, 010 Publishing, Rotterdam.

[3].E. Aarts and B. Eggen (eds.) (2002), Ambient Intelligence Research in HomeLab, Neroc Publishers, Eindhoven.

[4]. N.K. Ratha, J.H. Connell, R. Bolle (2002) Enhancing Security and Privacy of Biometric-based Authentication Systems IBM Systems Journal, Vol. 40, No. 3,2002.

[5].A. Juels, M. Sudan (2002) A Fuzzy Vault Scheme Proc. Intl Symp. Inf. Theory, A Lapidoth, E.Teletar, Eds., pp.408, 2002.

[6].U. Uludag, S. Pankanti, A.K. Jain (2005) Fuzzy Vault for Fingerprints, Proc. 5th Int. Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA 2005), Springer LNCS 3546, pp.310-319, 2005.

[7]. P. Tuyls, J. Goseling (2004) Capacity and Examples of Template Protecting Biometric Authentication Systems, Biometric Authentication Workshop (BioAW, Prague, 2004), LNCS 3087, pp.158-170, 2004.

[8].Y. Dodis, L. Reyzin, A. Smith (2004) Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, Proceedings of Eurocrypt 2004, LNCS 3027, pp.523-540, Springer-Verlag, 2004.

[9].S. Garfinkel and B. Rosenberg, editors. RFID: Applications, Security, and Privacy. Addison-Wesley, July 2005.

[10]. K. Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Wiley, 2003.

[11]. B. Fabian, O. G¨unther, and S. Spieker mann, Security analysis of the object name service for RFID, In Proceedings of the 1st International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, July 2005.