Privacy and the Access of Information in a Smart House Environment

Simon Moncrieff
Curtin University of Technology
GPO Box U1987 Perth 6845
W. Australia
S.Moncrieff@curtin.edu.au

Svetha Venkatesh
Curtin University of Technology
GPO Box U1987 Perth 6845
W. Australia
S.Venkatesh@curtin.edu.au

Geoff West
Curtin University of Technology
GPO Box U1987 Perth 6845
W. Australia
G.West@curtin.edu.au

ABSTRACT

In this paper we present a framework for addressing privacy issues raised by the monitoring of assisted living smart house environments. In home environments, the conflict between the goals of the surveillance, and the private nature of the home, raises the issue of occupant privacy. This issue needs to be addressed if applications are to be accepted by the occupant. We identify four key properties required for the design of privacy sensitive ubiquitous computing applications. Subsequently, we develop a *dynamic* and *flexible* method for implementing privacy measures through controlling access to data, and an interface to provide *feedback* to the occupant, enabling them to *control* the implemented privacy measures. We form a generic framework for implementing privacy sensitive ubiquitous computing applications based on previous applications within the field. This framework was then extended and used to develop a specific framework for a privacy sensitive smart house. The approach proposed in the framework dynamically applies privacy measures to multi-modal data according to the situation, or context, of the environment. We further test an implementation of the privacy measures, and detail methods to implement feedback and control. The approach aims to decrease the invasiveness of the surveillance, while retaining the purpose of the assisted living environment.

Categories and Subject Descriptors

J.0 [**Computer Applications**]: General

General Terms

Design, Human Factors

1. INTRODUCTION

Assisted living environments, a form of smart house, seek to enhance the way of life for the aged and invalid population by enabling them to remain in their homes for longer. This is achieved through the use of sensor technology to monitor the occupant of the environment to ensure their safety. Advances in complex sensor technology have extended the scope of such monitoring, allowing the active surveillance of the environment in order to ensure the occupant's safety. However, surveillance raises the issue of privacy. Due to the conflicting goals of surveillance and private environments (i.e. the home), privacy issues need to be addressed if the applications are to be accepted by the occupant [16].

Reaching a single, all encompassing definition of privacy is difficult, a point highlighted in [10]. However, there is a large corpus of work proposing design strategies and policies for addressing privacy in ubiquitous computing [10, 17, 9, 2, 15]. Consequently, rather than defining privacy, we identify key properties required for a privacy sensitive smart house. Four such properties are identified: the implementation of the privacy system should be *dynamic* and *flexible*, and mechanisms to provide *feedback* on, and *control* over the implemented privacy measures should be included. The latter two properties are important for the acceptance of such systems by the occupant [16, 9, 2, 15].

Previous approaches to privacy sensitive applications in ubiquitous computing typically account for what is happening within the environment (*context*), and who is using the application (e.g. the observer or occupant). In certain applications, privacy is implemented by default [18, 7, 3]. However, other applications assess the *context* in order to determine whether or not privacy measures should be implemented [20, 15]. Who is using the system is then used to determine what privacy measures should be enacted, using a simple rule set, accounting for the user, and the user's static, pre-defined preference. For example, privacy measures can be set for an observer with a given authorisation level [18], or given a user's requested privacy level [20]. The limitation of such an approach is that the context has a binary influence on what data an observer can access. That is, for a given user, if privacy measures are in place, what is happening in the environment does not influence what they are able to view. If privacy measures are not in place, the observer can access all data. This amounts to a single privacy policy for a given observer. Consequently, such an approach is not suitable for an actively monitored smart house environment. Such environments consist of multiple and changing situations that require different privacy policies, and require a trade off between ensuring the safety of the occupant, and limiting the invasion of their privacy. That is, a single privacy policy would be either too invasive for the occupant, or

MM'07, September 23–28, 2007, Augsburg, Bavaria, Germany.

too restrictive for those monitoring the environment, e.g. a carer attempting to verify an occupant's health may not be able to do so if given insufficient access to data. Consider the example of the bathroom, which is associated with sensitive, private activities, but is also a hazardous environment that requires monitoring. Hence, smart house environments require a more dynamic approach.

In this paper we propose and validate a framework for implementing privacy in a smart house environment that addresses the four key properties. The framework determines what privacy measure to implement accounting for both the situation within the environment, the context, and the observer of the environment, e.g. a carer observer. The occupant is then informed of, and given limited control over, the privacy measures.

We detail a method for dynamically determining what data access an observer can be given based on *context*, with access in the worst case scenario, and a *normal* situation, differing. Thus, the framework enables the applied privacy measures to be dynamically adjusted according to the *context*. To determine context, we use the concept of the *context space*, which identifies and quantifies multiple aspects of the environmental context to determine multi-modal contextual data that are relevant to ensuring an occupant's safety and privacy. For example, the spatial location and activities of the occupant. The context space was first introduced in [13] to determine the feasibility of influencing privacy using the situation in the environment.

A point in the context space is then mapped to an appropriate privacy policy, or privacy measure. The mapping is achieved by accounting for both the observer type, e.g. carer observer, and the context. However, due to the potential complexity of the context space, a simple rule (i.e. binary) is insufficient to perform the mapping. Consequently, we propose a method to generate a complex rule set for a given observer. By incorporating the context in the determination of the privacy policy, the framework does not rely on a single static privacy policy. This is an approach that is necessary in the monitoring of a private environment.

The privacy policy is implemented using multi-resolution data hiding techniques, designed to preserve privacy where possible, while still allowing an observer access to relevant information. The privacy measures, termed *data access levels*, are then presented to the observer. We combine the data hiding techniques into a multi-dimensional sensor space, the axes of which are formed from the sensor modalities present in the monitored environment. Thus, each point in the space represents a privacy policy governing access to the sensor data captured within the environment. This approach, which we term the *privacy space*, enables flexibility within the proposed framework. Different contexts are mapped to different privacy polices, and different types of observer are accommodated (e.g. family members, carers) as the same context can map to different points in the privacy space, as determined by the observer's purpose and associated level of trust.

The framework includes feedback and control mechanisms to provide a link between the occupant and the privacy system. For assisted living environments, such mechanisms should be integrated into the environment, where possible, as the purpose is to augment the environment, rather than create a new one. In providing feedback, the level of privacy present in the environment is shown, allowing the occupant to take action if required. Unobtrusive feedback is supplied to the occupant by taking advantage of the properties of the privacy space. We introduce a possible method for providing feedback using ambient displays placed in the environment, which provide a summary of the level of monitoring present in the environment. A further method allows the occupant to receive more detailed information if actively requested. This approach allows the occupant to quickly assess the level of monitoring in the environment, and then request further detail if required. Due to the purpose of the assisted living environment, giving the occupant complete control over monitoring is not possible. Properties of the context space are used to allow the occupant to control aspects of the privacy.

The novelty of this work lies in combining the context and the observer type to dynamically alter the privacy measures applied to the environment. Further, we introduce methods of providing the occupant with feedback on and control of the implemented privacy measure using properties of the privacy space and the context space respectively. In combining these aspects, we account for the four key properties required for developing privacy sensitive smart environments. Approximately five hours of data, captured in a smart house environment simulated in a lab, was used to examine the properties of the privacy implementation.

The significance of this work lies in the introduction of a method for addressing privacy issues in an assisted living smart home. As the need for assisted living environments grows [8], in conjunction with the ability to implement such environments due to advances in ubiquitous technologies, privacy is becoming an increasingly salient issue. As the home environment under observation is private in nature [15], privacy management is an important aspect of assisted living that needs to be addressed if the technologies are to be accepted by the intended beneficiaries [16]. This work seeks to limit the intrusion of the technology into the lives of the occupants, while still facilitating the active monitoring of the environment to ensure an occupant's safety.

2. BACKGROUND

2.1 Privacy in Ubiquitous Computing

In this section we identify the key properties required to design a privacy sensitive smart house. To do so, we explore privacy issues related to the design and implementation of privacy applications in ubiquitous computing. The work of social psychologist Altman [1] is relevant to smart house environments, as Altman examined the effect of the environment on privacy. The exploration of privacy with respect to personal space is of particular relevance. Altman developed process regulation theory, proposing that privacy consists of two component processes, a dialectic process, and a dynamic process. That is, privacy is a process that is influenced by both our own perceptions, and the perceptions of others, and is a process that is dependent on circumstances. Palen and Dourish [17] extend privacy regulation theory to the consideration of the design and analysis of information technology. Similarly, Boyer *et al.* [3] argued that a single privacy model cannot be applied across applications, Dourish and Grinter [6] link the definition of security with the dynamic aspect of the privacy process, and Hong and Landay [9], state "the point is that, rather than being a single monolithic concept, privacy is a fluid and malleable notion

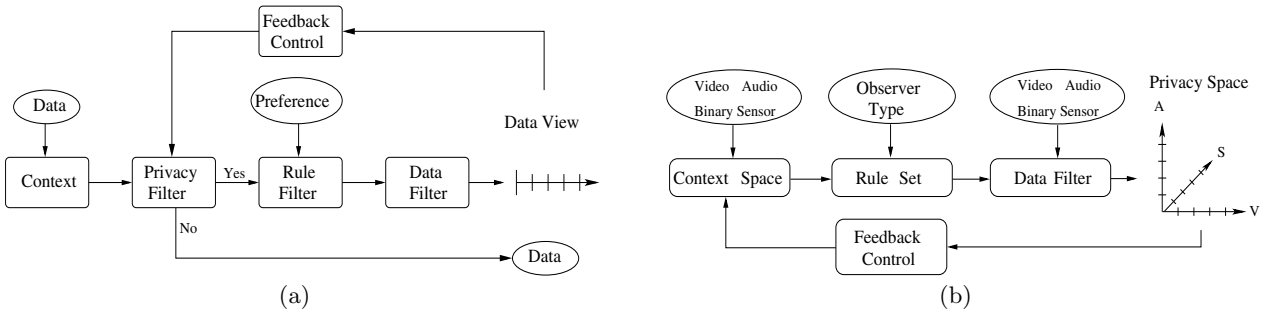

Figure 1: (a) A generic framework for privacy sensitive applications, and (b) Privacy sensitive smart house environment framework.

with a range of trust levels and needs (pg. 92)." In considering privacy as a process, rather than define privacy, we identify the integral parts of the process and incorporate them into the design of a system for implementing a privacy sensitive smart house. Thus, from privacy regulation theory, two properties are identified. First, flexibility, the dialectic process; a flexible system enables the privacy measures to accommodate different perceptions, that is, the occupant's preferences, and the observer's purpose. Second, the dynamic aspect, the policy needs to change with respect to the situation within the environment.

The dynamic and flexible aspect relate to the implementation of the privacy measures within the system. The occupant's acceptance of the privacy system is a further important aspect as a private area is under surveillance. The two properties that have been identified as important to the acceptance of the such systems [9, 15] are *feedback*, which is required to communicate the implemented privacy measure to the occupant, and control, allowing users to *control* aspects of the privacy measures, if necessary.

Thus, these four properties: a dynamic approach, flexibility, feedback, and control, are considered central to developing a privacy sensitive smart house.

2.2 Privacy Sensitive Smart Home Applications

Initially, we examine previous approaches for addressing privacy issues in smart house environments. A method has been proposed for monitoring an assisted living environment by learning the typical activity patterns associated with an occupant, using an intelligent agent and a network of sensors [5]. Privacy issues were addressed by restricting the monitoring to the sensors. A second technique involves restricting the type of sensor used. Wilson [21] used simple binary sensors to perform simultaneous tracking and activity recognition in an assisted living environment. Binary sensors were employed due to, amongst other factors, the decrease in privacy issues associated with the anonymous nature of the sensors. Similarly, Chen *et al.* [4] used audio classification to monitor activities in a bathroom environment, proposing that audio exhibits fewer privacy concerns compared to video data, and supplies more detailed information than binary sensors. Such approaches do not actively address privacy, but attempt to limit the intrusiveness of the systems. However, using the approach proposed in this paper, multi-resolution data hiding, the audio and video data can be reduced to binary sensors, while allowing access to richer data when required.

2.3 Privacy Sensitive Ubiquitous Computing Applications

To examine applications that actively address privacy issues, we turn to the wider field of ubiquitous computing, investigating privacy sensitive applications for both private and public environments. As a result, we have developed a generic framework, shown in Figure 1(a), that unifies previous approaches for designing such applications. The framework represents a generalisation of the combined aspects of the previous approaches, designed with a view to addressing the issues identified in Section 2.1. While the previous approaches do not contain all aspects of the generic framework, they can be considered to be encapsulated by, or subsets of, the framework.

The first component of the framework consists of determining the context, which is generally associated with a property of the environment. For example, the combination of motion sensors, used to detect the presence of a person, and a RFID tag, used to identify the person, can be used to determine if a person is authorised to access a particular area [20], or determine the presence of multiple people within a home office media space [15]. The second component, the privacy filter, interprets the context in a binary fashion in order to determine if privacy measures are required, or not. For example, privacy measures are required if a person has authorisation to enter an area [20], or if unknown people enter a home office media space [15]. If privacy measures are required the data is filtered to obscure privacy sensitive information, otherwise, the observer is given access to all data. In this framework, the context and privacy filter components are used for systems in which continuous privacy may not be suitable.

The rule component uses a rule based approach, and predetermined preferences, to determine the level of privacy required, e.g. using an observers authorisation level [18], an observed person's preferences for a given observer [3], a user's pre-defined preferences [7], or a users requested privacy level [20].

The privacy level is then passed to the data filter component, which uses data hiding techniques to filter, or obscure, the observed data in order to implement the required data access level. For example, the data can be filtered at two levels, e.g. video on and video off [15], or filtered at multiple resolutions, e.g. masking an occupants identity by obscuring the video data at different levels, such as replacing the image of the occupant with a bounding box [20]. The output from the data filter is then presented to the observer as

the *data view*. Finally, feedback is provided to the person being observed, which allows them to control the privacy filter, e.g. by turning the cameras off [15].

There are a number of advantages to this framework, the context introduces a dynamic aspect, while the use of preferences and multi-resolution filtering introduces flexibility. However, the dynamic aspect is limited to a binary interpretation of the context, determining if privacy is implemented or not, while static, pre-defined preferences are used to determine the data access level. This limits the scalability of the context in regard to handling multiple situations, and dynamically determining the data access level.

3. FRAMEWORK FOR A PRIVACY SENSITIVE SMART HOUSE

A specific framework for the design and implementation of a privacy sensitive smart house environment, shown in Figure 1(b), was developed using the generic framework described in Section 2.3. To overcome the limitations of the dynamic aspect associated with the generic framework, we introduce two key ideas to expand the framework, the context space, and the privacy space.

3.1 Context Space

Contextual data is data that can be semantically linked to a situation. In contrast with previous approaches, we use context to influence the *level* of privacy filtering. In order to dynamically adjust the privacy (data access level) according to the situation, we use the context space. The context space is a single, multi-dimensional construct that encapsulates multiple aspects of the situation within an environment (*context*). Each aspect, or context type, is represented as an axis of the context space, with the context types combining to form the context space. Combining multiple context types enables the context space to account for numerous situations within the environment. Each context type within the space can be either discrete, or continuous, with both possible within the same space. For privacy in an assisted living environment, the relevant context relates to ensuring the occupant's safety, and to reducing the invasion into the occupant's privacy.

3.2 Rule Set

The rule set is used to map a point in the context space to a point in the privacy space by determining the appropriate data access level given the context. The data access level is then passed to the data filter that then generates a view in the privacy space by filtering each data source type as specified by the data access level. Thus, the privacy level is dynamically updated as the context within the environment changes. The rule component represents a method for translating the situation in the environment to an appropriate data access level for an observer. Thus, the context to privacy space mapping equates to a mapping between semantic concepts.

The rule set introduces a flexible component to the framework, allowing the incorporation of preferences. In this case the preferences are associated with occupant preferences and the observer types, accounting for the purpose and trust level associated with the observer. The same context can be mapped to different data access levels depending upon the observer's purpose, e.g. doctors, family members, and carers will have differing data access levels for the same context.

Due to the potentially complex nature of the context space, a complex rule set is required to perform the mapping. One proposed method for generating the rule set is a decision tree, trained using data captured from the smart house environment. Given the training data, the context can be calculated and labelled with an appropriate data access level. The context and associated labels can then be used to generate a decision tree, from which the rules can be extracted. Other possible methods for generating rules include clustering and dimensionality reduction.

The determination of the appropriate data access level is open to interpretation due to the dialectic aspect of the privacy process, i.e. the data access levels associated with certain contexts can be influenced by an individual's perspective. However, a uniform privacy measure should apply across similar contexts, or scenarios. To determine appropriate privacy measures for an observer type, the purpose and associated level of trust should be taken into account. Furthermore, a risk analysis approach can be adopted, balancing two types of risk. First, the risk associated with an inappropriate access to privacy sensitive data, which could lead to the embarrassment of the occupant, as their privacy was unduly compromised, and to the rejection of the system. The second risk lies in not giving the observer a sufficient data access level to determine the occupant's safety.

3.3 Data Filter and Privacy Space

The data filter implements the appropriate data access level by applying data hiding techniques defined by a point in the privacy space. The privacy space is a method for describing the multi-resolution data hiding techniques used to filter multi-modal data. Thus, the privacy space is a multi-dimensional representation of the data access levels for the data source types, or sensor modalities (e.g. video and audio), present in the smart house. Each axis corresponds to the data access level for a source type, with points on the axis corresponding to different privacy filtering methods, with the origin representing the highest level of privacy, i.e. lowest data access level, with increasing data access levels when moving away from the origin. Each axis can be discrete or continuous. For example, a continuous axis for video data could be implemented by blurring the image to different degrees depending upon the appropriate access level. Alternatively, levels for the discrete filtering of the video could consist of showing: 1) no data, 2) the position of the occupant marked on the plan of the room, 3) removing the image of the occupant and replacing it with a shadow image [20], and 4) all video footage.

3.4 Feedback and Control

3.4.1 Feedback

Continual active feedback of the monitoring would be onerous to the occupant due to the dynamic characteristics of the proposed privacy system, and due to the monitoring of a home environment. Consequently, we propose the use of both ambient and active feedback methods, with the latter being made available upon the request for further information from the occupant. The ambient orb[1] is used to derive one type of ambient display. The ambient orb is a wireless

[1]http://www.ambientdevices.com/cat/orb/orborder.html - *accessed January 2007*

device that changes colour according to a dynamic information source. We link the colour of the orb to the current data access level of the environment. The Euclidean properties associated with the axes of the privacy space are used to map a point in the privacy space to a colour, with blue representing the origin of the privacy space, and red representing the highest data access level (i.e. farthest point from the origin). A more detailed ambient display consists of monitors (e.g. LCD screens) showing the data access levels for each data source in the form of a bar chart. Numerous ambient displays would be placed throughout the environment. Multiple observers are accommodated by showing the current highest data access level. The ambient displays provide an easily accessed method for determining the data access level that minimises the intrusion of the smart house system on the environment. However, the level of detail supplied by such displays is limited. The *active feedback display* is required to provide more detailed feedback using an existing monitor, such as a television. This display allows the occupant to access detailed information on the people observing the environment, and the associated data access levels. Additionally, logs are provided that detail information regarding past observers, highlighting high data access levels.

3.4.2 Control

It is not possible to give the occupant direct control over the monitoring of the smart house environment, due to both the nature and purpose of the environment, i.e. to ensure the safety of the occupant, they should not be able to turn the monitoring off. Instead, we propose to give the occupant control over aspects of the context used to determine the occupant's safety. For example, if a context indicates a potential danger to the occupant's safety, causing an increase in data access level, the occupant can indicate a normal situation, i.e. the occupant is safe, resetting the appropriate context to *normal*, which in turn resets the data access level. Similarly, if an occupant is deemed capable, they can indicate an *abnormal* context, resulting in an increased data access level.

4. IMPLEMENTATION AND EXPERIMENTATION

An implementation of the proposed framework was developed and subsequently tested using data captured from a smart house environment simulated in a lab. This enabled the examination of the properties of the context and privacy spaces, and the determination of the efficacy of the proposed method for mapping a context point to a privacy point.

4.1 Experimental Process

A number of scenarios were captured during three data recording sessions within the simulated smart house environment. The simulated smart house contains two rooms, a bedroom (*private space*), and a kitchen/lounge area (*living space*). In order to simulate the real world functionality of each room, devices, such as a stove and fridge, were placed in the environment and augmented with binary sensors, such as reed switches. Pressure mats were used to detect proximity to doorways, interaction with furniture, and placed in front of certain devices to detect device interaction. Additionally, visual sensors, video cameras, were placed in the corners and centre of each room, capturing video footage at a resolution of 320x240 pixels and a frame rate of 25 frames per second. An omnidirectional microphone was placed in each room to capture the audio associated with the environment. The audio signals were captured at $44.1Khz$, 16bit, in wave format. The ten video streams, sensor logs for all binary sensors, and the two audio streams were captured and stored for off-line synchronisation and processing.

Table 1: Testing and training data set details.

Data Set	Sequence Name	Duration (min)
Training	Training Set 1	95.2
	Training Set 2	104.0
Testing	Testing Set 1	95.3

The captured data was split into two sets; the training data set, consisting of two data capture sequences, and a test data set, consisting of a single data capture sequence. Details of the two data sets are shown in Table 1; approximately five hours of data was captured in total. The training data set was used to generate the rule set required for mapping between the context and privacy spaces. Subsequently, both the testing and training data were used to validate the performance of the mapping, and the privacy framework. Each data sequence consisted of numerous scenario types consisting of multiple interleaved activities. The scenarios encompassed multiple environmental contexts, including the extremes of the context types that form the context space. Further, combinations of different scenarios were present. The continuous capture of data resulted in a large range of context within the data sequences, comprising both scenarios and the transitional context between scenarios. The scenarios were developed to simulate a smart home with a single occupant. Section 4.2.1 describes the scenarios present in the data in more detail.

4.2 Implementation

In this section we detail an implementation of the context space, the rule set, and the data filtering and privacy space components of the proposed framework.

4.2.1 Context Space

To define the context space, we identified four properties of the environment that are relevant to reducing the invasion of the occupant's privacy, and ensuring the occupant's safety. We then implement methods to quantify the context types using multi-modal analysis, consisting of the analysis of audio and simple binary sensor data (e.g. reed switches). The four context types used were *spatial context* (*where*), *social context* (*who*), *hazard context* (*how* and *what*), and the *activity context* (*what*). In this section we briefly outline the context types. For a more detailed description of the derivation and determination of the context, refer to [13].

The spatial context divides the home into *living spaces* and *private spaces*, and is derived from the location of the occupant within the environment. Living spaces encompass areas such as the kitchen and living room and are associated with social interactions. Conversely, private spaces, such as the bathroom and bedroom, are more associated with privacy sensitive activities. The purpose of the social context is to determine an appropriate privacy policy given the properties of the two identified spaces. For example, due

to the potential presence of a privacy sensitive activity in a private space, a higher level of privacy is appropriate. The social context can be combined with the other context types to identify potential risks. For example, if an environment consists of a single occupant, a social interaction within a private space would not generally be expected. The spatial context is assigned a value of 0 for private space, 1 for a public space, and -1 when the occupant is outside the environment.

The social context indicates the presence of a social interaction in the form of a conversation between two or more people within the environment[2]. Conversation is detected through detecting segments of speech within the environment [11, 13]. The social context is used to identify sections of speech in order to allow or deny access to the content of the conversation, depending upon the observer. For example, a carer observer should not generally be given access to the content of the conversation. Further, the social context can be used to influence the level of monitoring. If multiple people are present, this suggests that the occupant is already being monitored, which reduces the need for high level monitoring. However, the presence of others introduces a potential risk, thus requiring a degree of monitoring. The social context has a value of 1 if a social interaction is present, and 0 otherwise.

The hazard context is used to increase awareness when the occupant of the environment is interacting with a hazardous device. We define a hazardous device to be a device that has to be attended to while active, or on. Examples of such devices include taps, stoves, fridges, and so on. There are two components to the hazard context. The first component indicates the presence of an active hazardous device within the environment, and is determined by a binary sensor associated with the device (*Hazard 1*). Consequently, this component is discrete, and is assigned a value of 0 or 1. The second component of the hazard context is termed the *anxiety* [14] (*Hazard 2*). The anxiety determines abnormal interactions with an active hazardous device by learning typical temporal patterns of interaction between the occupant and the hazardous device, and associated devices within the environment. The value of the anxiety ranges from 0 to 1. As the occupant interacts with the hazardous device the anxiety reduces to 0. Between interactions with hazardous device, the anxiety increases the greater the deviation from a normal interaction pattern. Once a set threshold is reached, the occupant is queried as to their current status, a positive response resets the anxiety to 0, while, in the absence of a response, the anxiety increases. An anxiety value of 1 represents an abnormal interaction, indicating that the occupant may be injured (preventing interaction with the device), or has forgotten that the device is active (resulting in a potential danger, e.g. a stove can become a fire hazard if left on). Consequently, as the anxiety increases a higher level of monitoring of the environment is required.

The final context type is the activity context, which is used to increase awareness when the occupant becomes abnormally inactive. The activity context is determined using the probabilistic framework used to determine anxiety [14], in this case typical patterns of interaction between the occupant and the environment are learned, and used as an indication of the level of typical activity. Binary sensors and audio sensors [14] are used to determine interaction with the environment. As with anxiety, a lower value indicates the occupant is active, and requires less monitoring. A high value of the activity context indicates an expectation should become active again due to an unusual lack of activity. The cause of this lack of activity could be a passive activity, such as reading or sleeping, or an injury to the occupant. In such cases, an observer should be given access to sufficient information to distinguish between the two cases. Like the anxiety hazard context, the activity context ranges from 0 to 1.

The context types combine to form a $5D$ context space. Thus, the audio and binary sensor data is processed, resulting in a feature vector representing situation within the environment of the form (*Hazard2 (Anxiety), Hazard1, Social, Activity, Spatial*). The feature vector was calculated at a resolution of $1s$ for each data sequence.

The scenarios present in the test data consisted of everyday scenarios, along with scenarios designed to include the extremes of the context space. For example, anxiety values ranging from 0 to 1 were present, simulating an occupant forgetting to turn off the stove while cooking. Further, multidimensional aspect of the context space was tested by performing multiple scenarios simultaneously. For example, the presence of a social interaction while cooking, or a change in spatial location, either while cooking, or during a social interaction. Multiple social interactions were present in the the scenarios, comprising a number of different speakers, occurring in both spatial locations. Consequently, the types of activities present in the data sequences consisted of social interactions, cooking, to simulate an interaction with a hazardous device, and activities ranging from active to passive, e.g. reading.

4.2.2 Rule Set

A decision tree was used to generate the complex rule set for mapping between the context space and the privacy space. The rule set was extracted from the decision tree trained using the context calculated from the two training data sequences, train set 1, and train set 2. The class data used for classification was generated as follows:

- Each data sequence was divided into sections according to the context within each section, i.e. each section encapsulated a uniform environmental context.
- For each section, an appropriate data access level, or privacy space point was identified, and assigned to the section.
- Each second of data in each section was then assigned the data access level of the ground truth privacy point.

Thus, to train the decision tree, we treat each point in the privacy space as a class. This process was performed for each data sequence, both training data sets, and the test set. Fourteen privacy space classes were identified in the data sequences. Consequently, the decision tree was trained using the context data as the attribute values, and the privacy space points as the corresponding class values. The decision tree classifier used was an implementation of the $C4.5$ decision tree algorithm, $J48$ [22]. This method proved successful in mapping between context and privacy points. When tested on unseen data (testing set 1), an accuracy of

[2]Social context excludes telephone conversations.

Table 2: The influence of the context on the privacy ground truth (data access levels).

Context	Privacy	Reasoning
Spatial		
Living	-	Normal privacy measures are applied.
Private	↑	Potential presence of privacy sensitive activities.
Social		
None	-	Normal privacy measures are applied.
Present	↓	Occupant already being monitored (i.e. decrease in privacy within the environment). Capped to preserve identity of people present and the content of the conversation
Hazard1		
1	↓	A hazardous device is active in the environment.
Anxiety		
Low	-	Normal interaction with the hazardous device.
High	↓	Abnormal interactions, indicating a potential danger to the occupant.
Activity		
Low	-	Occupant is active within the environment.
High	↓	Absence of an interaction could indicate a potential danger to the occupant.

Table 3: The data access levels for each sensor type present in the environment.

Sensor Type	Access Level	Description
Video	0	All data blocked.
	1	(x, y) co-ordinates show on a plan of the smart house.
	2	The image of the occupant is replaced with a bounding box.
	3	The image of the occupant is replaced by a shadow image [20].
	4	All data is presented to the observer.
Audio	0	All data blocked.
	1	Background and foreground audio as labels [12], indicating audio activity.
	2	Background audio signal, with labels representing environmental foreground audio and speech.
	3	Background and foreground environmental audio, with a speech labelled.
	4	All data is presented to the observer.
Binary	0	All data blocked.
	1	Room occupied by occupant, and active hazardous devices.
	2	Device last interacted with, and active hazardous devices.
	3	Device interacted with, and the form of the interactions, and active hazardous devices.
	4	All data is presented to the observer.

91.90% was obtained. To determine the presence of ambiguous data, the decision tree was tested with the training data, resulting in a 95.3% accuracy for training set 1, and 95.4% for training set 2. Such errors represent ambiguities between the context determined when generating the ground truth and the context determined by algorithmic data analysis.

A detailed discussion of the risk analysis method used to determine the appropriate ground truth label for a given context is beyond the scope of the paper. However Table 2 presents a general overview of the effects of the context on the privacy for the current mapping, which was determined for a carer observer, for a house with a single occupant. In addition to the risk analysis, two factors were considered when determining the appropriate privacy policy, or data access level. The first relates to the observer's purpose, or task, in monitoring the occupant, which determines what information the observer needs to access. In this case, the primary purpose of the carer is to ensure the occupant's immediate safety. The second factor relates to how each sensor type can be used to accomplish this task, and how this changes with changing context.

The mapping policy used represents one possible approach of many to determine an appropriate context to privacy correspondence. This is due to the dialectic nature of the privacy, which results in many such mappings that would be acceptable depending upon different perceptions, providing that the observer is able to perform their purpose. The advantage of the flexible mapping process, facilitated by the privacy space, is that the mapping can be influenced by environmental factors, and different perceptions of privacy.

4.2.3 Data Filtering and Privacy Space

The rule set defines the data access level, a point in the privacy space, given the context. The data filter component then implements the appropriate data access level for each information source using the data hiding technique corresponding to the access level. For the experimental environment detailed in this paper, the privacy space is discrete and consists of three axes, one for each modality present; audio, video, and binary sensors. The data hiding levels are described in Table 3. The co-ordinates of each axis represent different data hiding techniques, with five levels of filtering present on each axis. While the filtering method used for each axis differs, the level of detail for corresponding co-ordinates is equivalent. Access to past data, filtered at the corresponding level, is introduced at level 3. This provides information on events leading up to the current state of the environment. The data hiding techniques are designed to give an observer access to relevant information, while preserving aspects of the privacy. For example, the (x, y) co-ordinates of the occupant reveals position, the bounding box (video, level 2) reveals position and limited pose information, and the shadow image conceals the image of the occupant, but allows the observer to determine the detailed pose and position information.

4.3 Experimental Results

In this section we examine the properties of the context and privacy spaces, and the mapping between the spaces.

4.3.1 Context Space

Figure 2 displays each element, or dimension, of the context space, plotted against time, calculated for training data set 1. Figure 2(c) shows the combined plots for the presence of a hazard, and the anxiety contexts. Figure 2(a) shows the speech context, Figure 2(d) shows the activity context, and Figure 2(b) shows the spatial context. The figures provide contextual detail of the activities present within the environment for the first training data set. Two social interactions

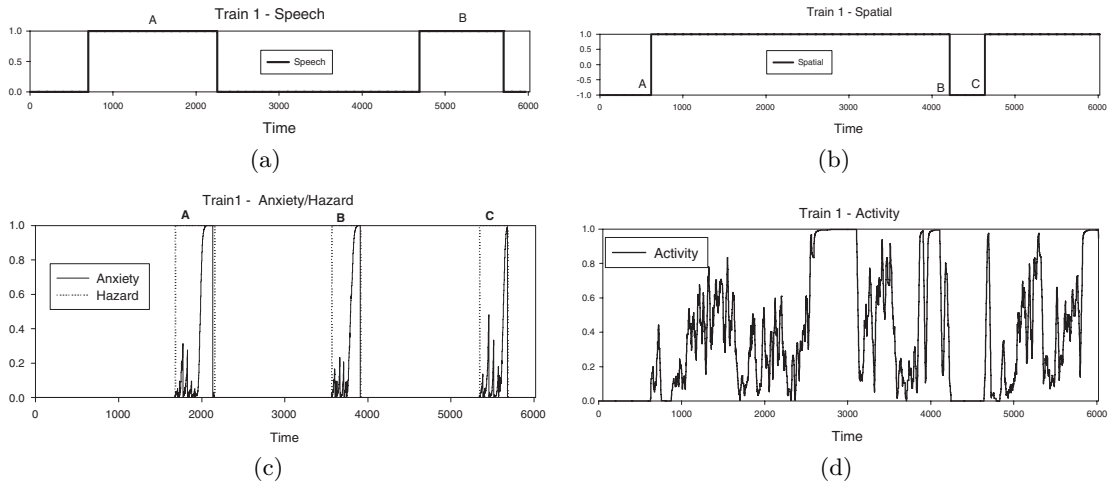

Figure 2: Each element of the context space for training data set 1, plotted against time.

are present, Figure 2(a), at times A, and B. Changes in the spatial context are present when the occupant enters and leaves the environment. The occupant entered the living environment, corresponding to a spatial context value of 1, at point A, Figure 2(b). The occupant then left at point B, and re-entered at point C. Figure 2(d) details the level of activity in the environment, which includes three sections when the occupant was inactive for a prolonged period of time. Three hazardous sequences are present, with the first and third occurring during a social interaction, Figure 2(c) points A and C. The second hazardous sequence, Figure 2(c) point B, occurred when there was no social interaction present in the environment.

4.3.2 Privacy Space

Figure 3 shows the ground truth, and classified (*Classed*), data access levels for the audio and video for testing set 1, for the video of training set 1, and for the sensor axis of training set 2, plotted against time. The *Classed* plots are generated from the data access levels obtained from applying the decision tree, trained on both training data sets, to determine the mapping between the context and the privacy space, i.e. the classified context data. The *Classed* plots are superimposed on the ground truth plots. Thus, the visible sections of the *Classed* plot represent sections of deviation between the classification and the ground truth data access levels. The figure shows the varying data access levels applied throughout each captured data sequence, demonstrating the dynamic nature of the data filtering, and hence privacy. Further, figures 3(a) and 3(b) demonstrate the different access levels present for different sensor types. From observing the sections of deviation between the ground truth and *Classed* plots, it is noted that the majority of deviation is either in the form of short pulses, or brief periods of misalignment between the ground truth and the context data, i.e. the boundaries between access levels; this is attributed to smoothing. The short pulses can be removed by introducing a lag and smoothing the access levels over time.

4.3.3 Mapping from Context to Privacy

Figure 4 depicts the context and corresponding data access levels for a segment of training data set 1 that contains a cooking scenario in which the stove was left unattended, resulting in a high level of *anxiety*. The segment depicts activities before, during, and after the cooking scenario, including a period of inactivity after cooking (e.g. reading). The activities take place within the living space (a spatial context of 1), and no social interaction was present (a social context of 0). The context plots (top) show the remaining contextual data; the hazard, anxiety, and activity contexts. The lower plots depict the corresponding data access levels for the video and audio.

Points $1-11$ on figures 4(a) and 4(b) mark changes in the data access levels for the video and audio due to changes in the environmental context. Corresponding points on the audio and video data access level plots are labelled. Points 1 and 2 correspond to brief periods of inactivity within the environment. The change in the data access level at these points represent a deviation from the ground truth due to misclassification of the context point space. This is attributed to the brevity of the period of inactivity ($1s$), which did not correspond to an inactive period in the ground truth. The region between points 3 and 7 contain the cooking sequence (hazardous activity). At this stage, the data access level is determined predominantly by the anxiety context, with the access level rising from point 3 to 7 in conjunction with the rise in the anxiety. Of note, the data access level for audio increase more rapidly that the access level for the video due to the use of the audio in the determination of the anxiety. Point 7 marks the end of the cooking sequence, at which time the stove was turned off and the anxiety level reduced to 0, this is reflected in the data access levels. Points 7 to 11 contain a period of transitional context, from the occupant being active, to the occupant being inactive. The data access level for the video and audio increases as the absence of activity becomes more unusual, both attaining an access level of 3. This demonstrates the trade off between maintaining the occupant's privacy, and ensuring their safety. As there is no immediate danger present in the environment (i.e. hazard), a data access level of 4 would be inappropriate. However, a data access level of 3 is sufficient for an observer to ascertain the state of the environment, particularly due to the access to past data made available at level 3. For example, the observer can review the mask image of the

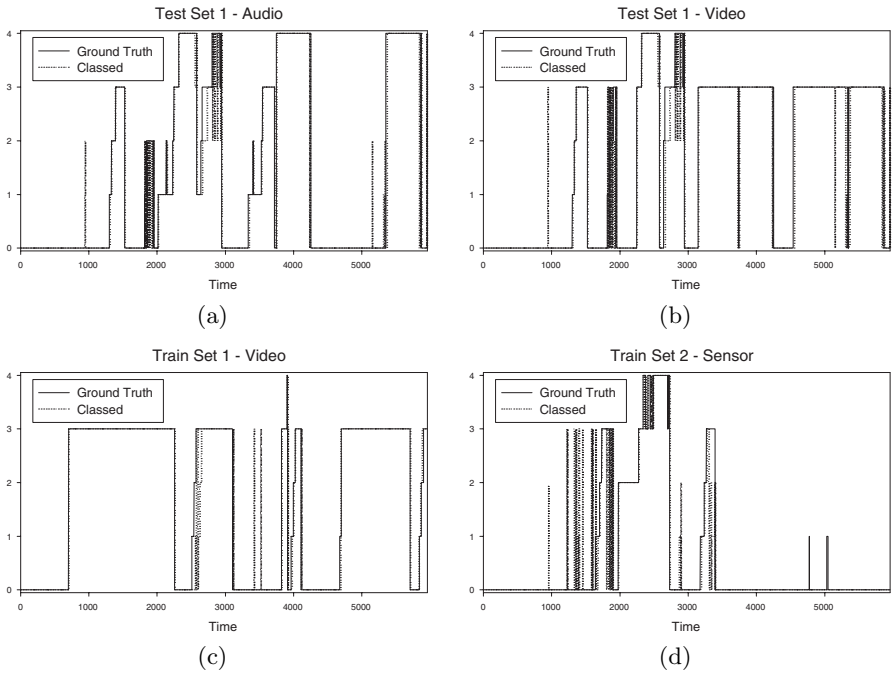

Figure 3: The plots of the ground truth and classification results (*Classed*) of the privacy space plotted against time. Classification results were obtained using the decision tree generated with the training data set. Figure (a) depicts the audio axis of the testing set 1, (b) the video axis of testing set 1 (c) the video axis of training set 1 and (d) the sensor axis of training set 2.

occupant in order to distinguish if the occupant is injured, or engaged in a passive activity, e.g. sitting and reading.

5. CONCLUSION

In meeting the growing requirement for assisted living applications [8], there are a number of factors that need to be overcome if the technology is to be accepted [21]. One such factor is privacy. Consequently, privacy management is an important aspect of assisted living environments that needs to be addressed [16]. The importance of privacy management arises due to the private nature of the home environment under observation [15].

In this paper we propose a framework for applying privacy measures to a smart house environment. The method is dynamic with respect to the context of the environment, and includes sufficient flexibility to accommodate different occupant preferences and observer types. An interface between the applied privacy measures and the occupant is proposed by showing privacy levels on displays placed throughout the environment. The occupant is then given a degree of control over the monitoring by enabling them to influence contexts that are used as an indication of occupant safety. We then detail an implementation of the privacy system, including a novel representation of the context of the environment, the context space, and a method for applying multi-modal and multi-dimensional data hiding techniques to data captured in a smart house environment, the privacy space. We then investigated the properties of the privacy and context space on data captured within a simulated smart house environment.

The proposed approach is scalable beyond the modalities suggested, and can similarly be applied to develop a privacy space consisting of a single dimension. Furthermore, the implementation of the context is flexible, and can be determined using resources available in an assisted living environment, such as binary sensors used to determined activities in the environment [5], or to determine abnormal interactions with hazardous devices [19]. Future work includes the development of methods for presenting the relevant information to an observer, including mechanisms for visualisation and data access. Further future work involves the extension of the context space. This can be achieved in two ways; 1) the inclusion of further modalities such as video, and 2) increasing the complexity of existing context types, particularly, extending the spatial and social contexts beyond binary values.

6. ACKNOWLEDGMENT

ARC Discovery Grant: Homes that Sense and Support (DP 0449437)

7. REFERENCES

[1] I. Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. Brooks/Cole Pub. Co., Inc., Monterey, CA, 1975.

[2] V. Bellotti and A. Sellen. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93)*, pages 77–92. Kluwer, 1993.

[3] J. P. Boyer, K. Tan, and C. A. Gunter. Privacy sensitive location information systems in smart buildings. In *3rd International Conference for Security in Pervasive Computing*, April 2006.

[4] J. Chen, A. H. Kam, J. Zhang, N. Liu, and L. Shue. Bathroom activity monitoring based on sound. In *Pervasive Computing*, pages 47–61, Munich, Germany, May 2005.

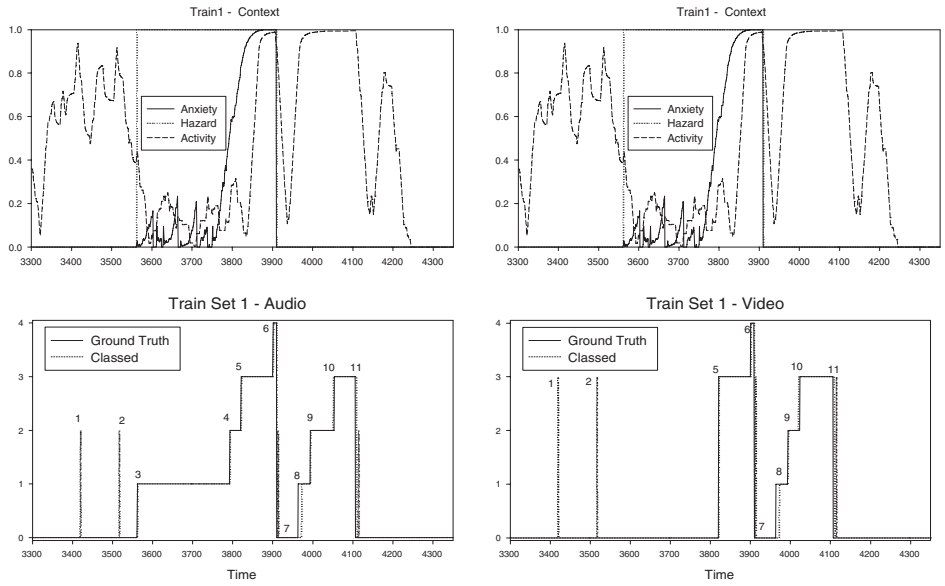

Figure 4: A segment of the Training data set 1 depicting a cooking scenario (hazardous event), displaying the corresponding context space elements, and data access levels for a) audio and b) video.

[5] S. Das and D. J. Cook. Health monitoring in an agent-based smart home. In *Proceedings of the International Conference on Smart Homes and Health Telematics (ICOST)*, Singapore, September 2004.

[6] P. Dourish, R. E. Grinter, J. Delgado de la Flor, and M. Joseph. Security in the wild: User stategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, November 2004.

[7] D. A. Fidaleo, H. Nguyen, and M. Trivedi. The networked sensor tapestry (nest): a privacy enhanced software architecture for interactive analysis of data in video-sensor networks. In *ACM 2nd international Workshop on Video Surveillance and Sensor Networks, VSSN '04*, pages 46–53. ACM Press, New York, NY, October 2004.

[8] S. Helal, B. Winkler, C. Lee, L. Kaddoura, Y. Ran, C. Giraldo, S. Kuchibhotla, and W. Mann. Enabling location-aware pervasive computing applications for the elderly. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003. (PerCom 2003)*, pages 531– 536, March 2003.

[9] J. I. Hong and J. A. Landay. An architecture for privacy-sensitive ubiquitous computing. In *2nd international Conference on Mobile Systems, Applications, and Services, MobiSys '04*, pages 177–189, Boston, MA, USA, June 2004. ACM Press, New York, NY.

[10] S. Lederer, I. Hong, K. Dey, and A. Landay. Personal privacy through understanding and action: five pitfalls for designers. *Personal Ubiquitous Comput.*, 8(6):440–454, 2004.

[11] S. Moncrieff and S. Venkatesh. Narrative structure detection through audio pace. In *IEEE Multimedia Modeling 2006*, pages 20–27, Beijing, China, 4–6 Jan 2006.

[12] S. Moncrieff, S. Venkatesh and G. West. Persistent audio modelling for background determination. In *IEEE International Conference on Multimedia and Expo (ICME 2005)*, Amsterdam, Netherlands, 2005.

[13] S. Moncrieff, S. Venkatesh and G. West. Dynamic privacy in a smart house environment. In *IEEE International Conference on Multimedia and Expo (ICME 2007)*, Beijing, China, July 2007.

[14] S. Moncrieff, S. Venkatesh, G. West, and S. Greenhill. Incorporating contextual audio for an actively anxious smart house. In *Int'l Conf. Intelligent Sensors, Sensor Networks and Information Processing*, pages 373–378, Melbourne, Australia, December 2005.

[15] C. Neustaedter and S. Greenberg. The design of a context-aware home media space for balancing privacy and awareness. In *5th International Conference on Ubiquitous Computing*, pages 297–314, 2003.

[16] P. A. Nixon, W. Wagealla, C. English, and S. Terzis. *Smart Environments: Technology, Protocols, and Applications*, chapter Security, Privacy and Trust Issues in Smart Environments, pages 249–270. Wiley, 2004.

[17] L. Palen and P. Dourish. Unpacking "privacy" for a networked world. In *SIGCHI Conference on Human Factors in Computing Systems (CHI03)*, pages 129–136, Ft. Lauderdale, Florida, USA, April 2003.

[18] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, and A. Ekin. Enabling video privacy through computer vision. *IEEE Security and Privacy*, 3(3):50–57, 2005.

[19] G. West, S. Greenhill, and S. Venkatesh. A probabilistic approach to the anxious home. In *The 29th Annual International Computer Software and Applications Conference - COMPSAC 2005, Edinburgh, Scotland, July*, 2005.

[20] J. Wickramasuriya, M. Alhazzazi, M. Datt, S. Mehrotra, and N. Venkatasubramanian. Privacy-protecting data collection in media spaces. In *ACM International Conference on Multimedia (ACM Multimedia 2004)*, New York, NY, October 2004.

[21] D. H. Wilson. *Assistive Intelligent Environments for Automatic Health Monitoring*. PhD thesis, Robotics Institute, Carnegie Mellon University, September 2005.

[22] I. H. Witten and E. Frank. *Data Mining: Practical machine learning tools with Java implementations*. Morgan Kaufmann, 2000.