Towards Privacy Protection in Pervasive Healthcare

Sheikh I Ahamed[1], Nilothpal Talukder[1], and Achilles D. Kameas[2]
[1]Dept. of Mathematics, Statistics and Computer Science
Marquette University, Milwaukee, Wisconsin, USA
{iq, ntalukde}@mscs.mu.edu
[2]School of Sciences and Technology,
Hellenic Open University, Patras, Hellas
kameas@eap.gr

Abstract

Proliferation of small handheld devices and wireless technologies has kindled the phenomenon of pervasive computing. Healthcare, being a prime concern for every society, has been considered as an ideal setting for deployment of this technology. Pervasive healthcare aims to improve patient independent living and quality of life and pay special attention to issues of security, privacy, transparency and ease of use. From its very nature of being open and dynamic, the pervasive environment has been challenged with security and privacy related issues with regards to collaborative information sharing. In this paper, we present some of the privacy challenges that arise when designing pervasive healthcare environments and discuss addressing some of these issues in a home based patient monitoring system. Specifically, we cover privacy violation through individual healthcare information availability and information leakage through context-aware services.

Keywords-Privacy violation; Information leakage; Healthcare; Pervasive Computing

1 INTRODUCTION

Pervasive Computing has come a long way from its inception to have widespread prevalence in our day to day life. The term pervasive health care is used to describe the integration of pervasive computing technology in healthcare services. The need for pervasive healthcare systems basically stems from the facts that (a) healthcare professionals experience a high level of mobility and they need to share resources and information with the staff, faculty and colleagues in real time and (b) there is an increasing trend in favor of treating chronic disease or recovering patients at home. In all these cases, there is a pressing need for ubiquitous access to resources and data for treatment, diagnosis, research, emergency situation etc [3].

The recent proliferation of Ambient Intelligence infrastructure, which supports precise measurement and data acquisition through groups of devices and sensors, communication through wireless channels, data mining, data fusion, decision making based on inference, and automatic planning and timely response has made possible the deployment of early pervasive healthcare systems. However, making such a huge amount of personal information available through networks raises serious privacy concerns for pervasive healthcare environments.

From the first days that novel technologies became interwoven into our lives, privacy concerns are blended with them. Though privacy needs more analytical treatment to be completely defined and regulated from the technological perspective, computer scientists' effort to define regulation boundaries helps viewing a clearer picture of privacy protection. Privacy management is continual management of these boundaries [31]. The simplest notion of privacy would be how much disclosure of information is allowed by the person. In healthcare scenario, it is customary to ask whether a patient should comply with the needs of disclosing the information of his health records. If yes, then when, how often, to what extent and to whom? Display and maintenance of identities also raise privacy concerns, whereas complete anonymity can't be achieved or is not even a solution for every situation. Practical anonymity requires complete inability to identify or infer the subject based on the location data. Example of such privacy protection efforts in location services could be Mist Router [32] which allows messages to traverse in a semi trusted heretically arranged proxy network. Cryptography schemes like mix routing [33] and Onion routing [34] offer anonymity in protocols for email and IP communications. But for healthcare scenario, rather than adopting anonymity, it needs more to defend against inference attack. And again with the pervasive healthcare applications with small handheld devices the energy and memory constraint has always been a primary concern. So, the simplest model contributes to the longer life of the applications. The regulation of privacy also needs to be flexible in a way that suits the needs of the specific task. The privacy requirements and policies need to be very dynamic according to time, need and severity.

In this paper, we describe two possible privacy violations: attack on healthcare records of individual patients and context-based information leakage. The first one deals of issues such as when and how to preserve the information, who are the owners of that information and then provides suggestions on the deployment of privacy protection measures. The second one describes the possible privacy violation through

access to context-based services and information in the home based system.

We have organized the paper as follows: Section 2 presents some scenarios which illustrate privacy violation issues from various aspects in pervasive healthcare environment. Section 3 provides the overview of the privacy challenges we have addressed. Sections 4 and 5 discuss in detail these privacy challenges, namely health information disclosure and information leakage. The sections explain the challenges in terms of healthcare scenarios, mention some of the existing approaches to address those challenges and finally recommend some realistic measures to achieve completeness of the solutions. Section 6 highlights some related works on pervasive healthcare area. Section 7 provides the future directions of the research.

2 MOTIVATION

We illustrate a scenario from pervasive healthcare setting where privacy violation and information leak is a concern.

2.1 *Scenario 1*

Andrew is suffering from high blood pressure. Recently he has experienced a mild stroke, too. Still, he feels uncomfortable and always prefers to be at home after he was released from the hospital. The doctors who treat him think he is not out of danger yet and he needs to be at rest and under their supervision for some time, while he is gradually getting back to his normal life. Thanks to pervasive computing, Andrew has installed an advanced monitoring system in the central server of his house. The system monitors his Activities of Daily Living (ADL), his Instrumental Activities of Daily Living (IADL) and his physiological parameters. With the system's support, Andrew enjoys his home life and at the same time he is under the care of the physician, nurse and psychiatrist. The pervasive healthcare system has the ability to gather data about Andrew's behavior and condition and to interpret this data in order to draw conclusions about his condition. This data is logged locally, together with his past Patient Record (which includes his medical history with blood pressures, other diseases, measured readings, mental health records, the findings of the physicians, past and present medications and even his personal information like health insurance policies) and can be sent to Andrew's physicians and nurse. When the system deduces that Andrew is suffering a problem, it will issue an alarm and notify Andrew's doctors and relatives.

Andrew is the owner of the information in his PR and has the right to provide access to it to others. He does not have the right to modify this information; this right rests with the Pervasive Healthcare system and the treating doctors. Andrew's privacy can be attacked either by unauthorized access to his PR information or by drawing inferences or correlations based on authorized pieces of this information. Although pervasive healthcare has contributed to the radical change to the healthcare facilities, it has also raised concerns of possible privacy violations, as sensitive medical information is gathered to specific storage points (the patient's home server or network, the hospital DB) and can be subject to single point of failure attacks. Moreover, since this information is in digital form, it can be copied and transmitted in practically zero cost. Finally, the individual has no direct perception of the usage of this information, although it directly related to him.

2.2 *Scenario 2*

Andrew owns the past information in his PR, but his treating physicians own his recent medical data. Andrew does not want to share his medical information with other people and he is concerned about the capability of his home visitors to access his PR. His pervasive home system allows new devices to be integrated in the environment. So, anyone entering his house with a pervasive device on hand could possibly gain access to Andrew's sensitive information if it is not properly secured. Andrew wants the system to enforce authentication and access control policies and ask for approval before granting access to content and services in his home.

The pervasive environment has made the security of such information more vulnerable. It is now harder to protect sensitive medical information, as it is not clear who owns this information and who has the right to grant access or other types of rights to it.

2.3 *Scenario 3*

Dr. Smith is Andrew's physician and he is the owner of the pressure measurements and prediction information. He doesn't want Andrew to access the information and thus want to protect the privacy of the information. Although the information belongs to the patient, here the doctor holds the right to keep it secret for treatment reasons. So, is there any violation revealing the information and how can it be protected?

2.4 *Scenario 4*

Laura is appointed as a nurse to take care of Andrew. She needs to access medical history information of Andrew, but she has not yet been granted access to view that information. Current access mechanism requires that Dr. Smith is present in the house for granting her access to that information. But Dr. Smith also doesn't want to reveal the information that he is in Andrew's house.

This is a slightly different scenario, which is related to the use of context services to draw inferences. Laura, by gaining access to Andrew's PR information, reveals the presence of Dr. Smith, as he is the only one who has

the right to grant her this access. This constitutes a violation of Dr. Smith's privacy through context information. How can the leakage be prevented?

For all of the above questions we have the answers in the next section. We consider all of these questions as separate challenges in terms of privacy prevention in home based healthcare monitoring system.

3 CHALLENGES IN PARVASIVE HEALTHCARE: PRIVACY VIOLATION

The privacy challenges are sometimes ignored in the pervasive models for healthcare and various other applications for the sake of simplicity. But privacy violation will be the prominent problem in the pervasive environment which is caused by huge amount of information being readily available. We summarize the two privacy challenges addressed here as the following:

i) Unwanted Health Information Disclosure:

Here, we refer to the privacy of healthcare information of the patient. We discuss US federal enactments on this issue and draw conclusion on how to protect it and when. We show a recent healthcare model by researchers addressing privacy concern of this primary information.

ii) Prevention of Information Leakage through Context:

We move away from the primary healthcare information and emphasize on the context information like location of the owners that could be used as constraints on primary information. It addresses the issue of information leak through accessing constraint information and eventually violating the privacy of the individual.

The next two sections will highlight in detail of each of these challenges with some related terminologies and discuss their impact on pervasive healthcare environment. And at the end of each section we suggest some of the guidelines and adaptations necessary for the approaches to meet the challenges towards preserving privacy on pervasive healthcare environment.

4 UNWANTED HEALTH INFORMATION DISCLOSURE

The change of trend in keeping medical records from paper to electronic media has increased the easy access to important and sensitive information of individuals. Nevertheless, the protection of individual privacy has to be ensured by the health-care providers and public health practitioners everywhere.

4.1 *Federal Privacy Act*

In the United States, Federal Health and Human Services (HSS) issued patient privacy protections as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The importance of the privacy preservation led to statutory enforcement. The new methods of electronic transactions require new safeguards to protect the security and confidentiality of health information. In sum, the act requires compliance with privacy rules stated with respect to Health plans, health care clearinghouses, and health care providers conducting financial and administrative transactions like enrollment, billing and eligibility verification electronically [7].

4.2 *Scenarios revisited*

The second scenario described in the previous section requires the patient to authorize access to his/her health information, but only on a need-to-know basis, i.e. the patient (or the owner of medical information, depending on the case) must decide the type of access rights he/she will grant, as well as to whom, for how long and for which purpose these rights will be granted. For example, special authorization may be required to make health related information available to the public services, except perhaps in cases of emergency or danger.

The third scenario depicts a situation where the physician conceals the treatment prediction information from the patient. The doctor or the healthcare service providers hold the right to restrict access to the prediction information, which may be kept secret for the sake of analysis by the physician and can only be revealed to the patient, upon request, after the end of treatment

4.3 *What belongs to whom*

From the point of view of ownership and subject some terms could be very useful to consider:

Primary Information: This is the information content. Healthcare records can be an example of primary information.

Subject of the information: It is always assumed that the subject of the information is the patient.

Owner of the information: The owner of the information is the one who has the complete right to access and modify the information. The owner of the information is not necessarily its subject. Scenarios 2 and 3 provide a clear distinction between different types of information owners. The same information can also be shared by multiple owners as depicted in scenario 2.

4.4 *An agent based approach towards healthcare privacy preservation*

In an attempt to preserve the privacy of the information the home based patient monitoring system Xhas to take special care. There are some frameworks

addressed the issue with privacy violation to provide transparency in pervasive healthcare environment. For example, the Autonomous agent framework in Baja University [3] adapts the SALSA framework for Negotiation based access control in pervasive healthcare. The system defines QoP (Quality of Privacy) as the probability of Pervasive Environment meeting the privacy contracts with similarity to QoS (Quality of Service) for network bandwidth. It mandates that the agents in the pervasive systems must be able to enforce privacy before they start communicating their information to the environment and before it grants access. No sensitive information is provided to anonymous agents.

4.5 *Ease of Requirements at Critical Hours*

There will be special cases when access to information must be made available very easily. This need of high availability stems from the unprecedented critical moments. Home healthcare systems must be criticality aware and respond according to the situation with flexibility in privacy policies. When potentially negative trend is identified the monitoring system the alerts are triggered which doesn't need to meet privacy requirements. The alert with sufficient amount of data about the status should be readily available in the environment for faster detection and treatment. The home healthcare system deploys audio or visual feedback alert systems that use health variables and threshold values for generating pre-alarm or post alarms. Interaction scenarios with the user is integrated into the system's operation either as part of medical data acquisition schedule or as an automatically created system response. Privacy requirements are blurred and vary from systems and diseases at the critical moment of time.

4.6 *Recommendations*

Finally, the owner of the information has to be more aware than before as long as the high availability and easy access of sensitive information are concerned. Even social engineering plays a key role for violation as such. Most of the approaches use probabilistic models [3] to avoid privacy violations in healthcare. To protect privacy in pervasive healthcare the probabilistic models doesn't fit in very well. For such an environment with lots of interactions with devices, a trust model with dynamic updates depending on punish and rewards with interactions is the best suited solution [24].

5 PREVENTION OF INFORMATION LEAKAGE TRHOUGH CONTEXTS

Until now we have not assumed anything about the context awareness of the pervasive healthcare applications, although it is an implicit component. The scenarios for information leakage are sometimes complex from the point of view of the service requester and their origin is from the context-sensitivity of the information requested from a pervasive device. It happens when access to some primary information like some medical records are constrained through some other context information. The unabated access to this context information is the reason for the violation of individual privacy.

5.1 *When Contexts are Constraints*

We consider scenario 4 to highlight information leak issue. The information leak is due to constraint information satisfaction of the doctor's presence in the vicinity for information access. Gaining or Failing to access the information reveals the location of the doctor whether he is in the house or not. But it violates the privacy of the doctor. Even the situation could be like the doctor is not the owner of the information and his privacy is violated through access to the constraint information. For clarification of explanation some of the terms are introduced here for convenience.

Primary service: It is the service that offers the *primary information* or access to the resources requested by the client. For example access to some medical history records is a service provided by an entity in the pervasive environment.

Constraint information: The *primary information* access can be constrained by some information that is needed to be satisfied before ensuring access to the resources. Like access to the medical history records, it is dependent on the location of the service provider. He only allows access if he is in the vicinity. So, the *primary service* is dependant on the *constraint information* of the service provider's location.

5.2 *Exploring Categorical Constraints*

There could be variants of such constraints to access primary information. The categorization of the constraint makes the privacy challenge even more challenging. We identify the categories of constraint information as the following: *Satisfy Any*, *Satisfy All* and *Hierarchical* from the perspective of satisfaction of constraint information within the context.

5.2.1 Satisfy Any:

Let's consider a scenario where C requested a healthcare information from A and it needs to satisfy a constraint of A (being in a fixed location) to provide access to the resources. If A fails to meet the constraint, it can ask B which also has the equal right for providing access upon satisfying his constraint (being in a fixed location). The dotted lines show optional interactions among A and B for constraint satisfaction.

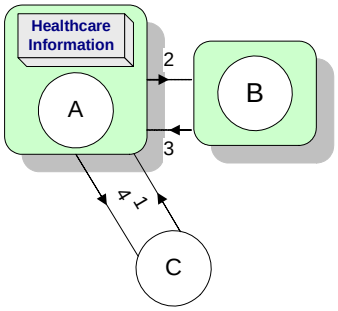

Figure 1. Privacy violation scenario on constraint satisfaction: Satisfy Any

Upon satisfaction the access to resource has been provided to C provided C has the access to the healthcare information. So, it needs satisfaction of any nodes' constraint and they are not dependent on one another. Thus C is passively getting access to constraint information. But if C is a malicious node denied access only for constraint dissatisfaction can infer absence of both A and B.

5.2.2 Satisfy All:

Another scenario may require satisfying all the constraints involved in the primary healthcare information or resource access. From the figure above we can see that D has requested access to healthcare information from A. But to gain access to this resource, the constraints of A, B and C all need to be satisfied.

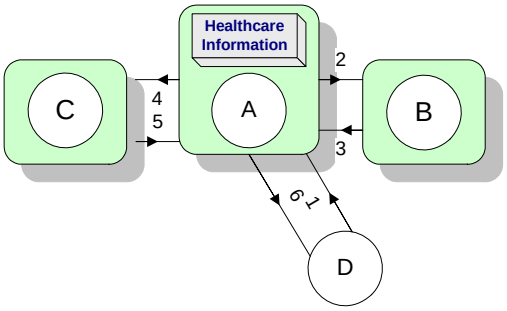

Figure 2. Privacy violation scenario on constraint satisfaction: Satisfy All

Here both the constraints must be satisfied. But to differentiate between *Satisfy All* and *Hierarchical constraints* we introduced one more node. In this scenario if access is granted or denied, the locations of all the nodes involved in constraint satisfaction are leaked and eventually the privacy is compromised.

5.2.3 Hierarchical constraints:

Hierarchical constraints are the ones which are dependant on other constraints in a chain fashion. If we arrange the constraint satisfaction graph in a hierarchical structure the root will be the primary information and the leaves will be the constraints that are independent. We compare it with the access rights graph described in [1]. Actually, because of their structure, hierarchical constraints cause the least damage during the denial of access, but still threaten the privacy of the leaf nodes. This is because the service requester has no way to know which constraint has not been satisfied all the way through the hierarchy of constraints.

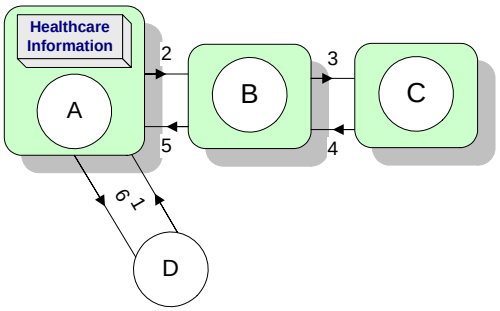

Figure 3. Privacy violation scenario on constraint satisfaction: Hierarchical Constraints

5.3 *Addressing the Information Leakage Issue*

The researchers in [1, 2] have proposed a new access control model to avoid information leak. To implement it, the constraint information also needs to be constrained. That brings out the hierarchical constraint satisfaction requirement. The model illustrates three scenarios of privacy violation and proposes an access rights based approach to handle the situations. The clients wanting to gain access to the primary service have to show proof or assurance to access constraint information. But proof of access requires digital certificate or encryption keys for all the contexts and information which enforces the individuals to maintain separate information. The constraint information is hierarchically constrained to avoid collision for both primary and constraint service provider. The approach in [2] for hierarchical representation for such constraint information saves space for the devices. The granularity of the information from coarse to fine is a good adaptation for search space shortening in such situations. Although the privacy violation issues are handled in these scenarios, the model is heavyweight in a truly pervasive environment.

A dynamic trust model with separate constraint trust could be a better alternative in terms of storage and computation. The privacy aware trust model depicted in [26] can be adapted to healthcare aide solution (as in [25]) to help preventing the information leak through constraint information access. The dynamic trust value for constraint access can be determined from the recommended value from the trustee parties and dynamically updated through each interaction.

6 RELATED WORKS ON HEALTHCARE

The pervasive healthcare projects everywhere in the world address the issues with the lack of staffing, high mobility, cost utilization etc. But issues with privacy have been repeatedly overlooked in the design and implementation of these systems. Now we move on to highlighting some of the pervasive healthcare projects [8-21] that are in full swing at different universities and institutions with the objective of providing more and more assistance to the elderly and ill people.

IST VIVAGO® [8] system is comprised of a wearable wrist unit, a base station and a specially developed software named 'Vista' which is actually responsible for managing the alarms and accessing data remotely. The wrist unit can be used to generate both manual and automatic alerts in critical moments. The alarms will be sent to the base station which incorporates several protocols to forward the alarm to several predefined recipients. But the requirement of privacy of the data has not been a concern. The 'Terva' [10] monitoring system works with the principle of scheduling collection of data related to health condition like blood pressure, temperature, sleep conditions, weight, etc., over quite a long time. The default frequency has been set four times a day -- morning, noon, evening and night -- and saved in the form a TOD (time-of-day) matrix for later analysis. The whole system has been housed in a suitcase that includes a laptop, blood pressure monitor and several other monitoring devices. This approach doesn't quite fall in the domain of pervasive healthcare for it lost its mobility in this way.

Among the others, Center for Future Health [12], a five-room house has been deployed with several infrared sensors, monitoring devices and biosensors. The ultimate goal of the project is to provide a unified solution for the seniors in the home, enabling them to closely participate in disease detection and health management by themselves. A similar healthcare project named 'AHRI' (Aware Home Research Initiative) [13] is being undertaken at GeorgiaTech University. CAST (Center for Aging Services Technologies) [14] is organizing multiple projects including: a. A safe home for debilitated elderly by tracking their activities. b. A sensor-based bed to track the sleep and weight, and detecting diseases. MobiHealth project [15, 16, 17] focuses building a system for collecting vital body signals and manipulating those in distant health care institutes. Monitoring critical health signals have been possible by Body Area Network (BAN) has been used in signal monitoring and GPRS, UMTS has been used for transmitting signal on the fly. The project Citizen Health System (CHS) [27, 28, 29, 30] has been undertaken with the goal of developing a generic contact center that can provide better health care services to home bound patients. Modularity is considered in their generic design and Wireless Application Protocol (WAP) has been used for providing wireless communication. But all of the systems working with huge amount of real time sensor and prediction analysis data lack in focusing in privacy protection issues. The aim of our paper is to identify the privacy issues that matters most in the pervasive healthcare environment and future recommendations for prevention.

A feedback-based self monitoring system for managing obesity named 'Wireless Wellness Monitor' [15, 16] has been devised using Bluetooth and Jini network technology that supports Java dynamic networking. The system consists of measuring devices, a home server as the base station, mobile terminals (e.g. PDA or smart phone) and databases which are connected through the internet. The measuring devices collect data and place that in the home server. In [17] researchers have depicted several required characteristics of wearable health care system along with the design, implementation and communication issues of a plug-and-play system.

It is apparent that all the healthcare and self monitoring systems described above emphasizes mostly on automated patient caring, several alert notification systems, efficient usage of wireless technology for readily available information everywhere. But their drawbacks on addressing the privacy protection have stalled them from achieving the completeness as a whole.

7 CONCLUSION AND FUTURE WORKS

In this paper, we have summarized some of the privacy concerns in the form of health information disclosure and information leakage through context information. We have depicted how the challenges threaten the privacy in pervasive healthcare environment and discussed some existing and futuristic approaches to avoid that. Our future aim is to build an automated robust healthcare framework that will provide medical data acquisition through collections of diverse collaborating distributed devices and artifacts. The critically aware automated healthcare system will be based on intelligent inference and decision making algorithms along robust against the security and privacy. We are streamlining the privacy requirements

on the framework towards a robust and transparent pervasive healthcare application. A prototype of the healthcare system is described in [25].

In the future, we plan to design and evaluate a generalized inference model for pervasive healthcare, which will encompass the issues and concepts described in this paper.

8 REFERENCES

[1] U. Hengartner, P. Steenkiste, "Avoiding Privacy Violations by Context-Sensitive Services," in Fourth Annual IEEE International Conference on Pervasive Computing and Communications (Percom), 2006.

[2] U. Hengartner, P. Steenkiste, "Exploiting Hierarchical Identity-Based Encryption for Access Control to Pervasive Computing Information," in First Annual IEEE International Conference on Security and Privacy in emerging areas in communication networks (Securecomm), 2005, pp. 384- 396.

[3] M. Tentori, R. Favela, M. D. Rodriguez, "Privacy-aware Autonomous Agents for Pervasive Healthcare," in IEEE Intelligent Systems, Nov-Dec 2006, pp. 55-62.

[4] M. Ahmed, D. Quercia, S. Hailes, "A Statistical Matching Approach to Detect Privacy Violation for Trust-Based Collaborations," in the Sixth IEEE International Symposium on World of Wireless Mobiles and Multimedia Networks (WoWMoM), 2005, pp. 598-602.

[5] S. K. S. Gupta, T. Mukherjee, K. Venkatasubramanian, "Criticality Aware Access Control Model for Pervasive Applications", in Fourth Annual IEEE International Conference on Pervasive Computing and Communications (Percom), 2006.

[6] T. Heiber, P. J. Marron, "Exploring the Relationship between Context and Privacy," Privacy, Security and Trust within the context of Pervasive Computing, pp. 35-48

[7] HIPAA http://www.hhs.gov/ocr/hipaa/

[8] S. I. Korhonen, J. Lötjönen, M. Sola, and M. Myllymäki, "IST Vivago—an intelligent social and remote wellness monitoring system for the elderly," *in Proc. 4th Annu. IEEE EMBS Special Topic Conf. Information Technology* Applications in Biomedicine (ITAB 2003) Birmingham, U.K., Apr. 24–26, 2003, pp. 362-365.

[9] J. Parkka, M. Van Gils, T. Tuomisto, R. Lappalainen, I. Korhonen, "A wireless wellness monitor for personal weight management",*Information Technology Applications in Biomedicine, 2000.* Proceedings. 2000 IEEE EMBS International Conference on 9-10 Nov. 2000 Page(s):83 - 88

[10] **I.** Korhonen, R. Lappalainen, T. Tuomisto, T. Koobi, V. Pentikainen, M. Tuomisto, V. Turjanmaa, "TERVA: wellness monitoring system"**,** *Engineering in Medicine and Biology Society, 1998. Proceedings of the 20th Annual International Conference of the IEEE* Volume 4, 29 Oct.-1 Nov. 1998 Page(s):1988 - 1991 vol.4

[11] N. Saranummi, I. Korhonen , M. van Gils and S. Kivisaari, "Barriers limiting the diffusion of ICT for proactive and pervasive health care," in *Proc. of the IX MEDICON*, Pula, Croatia, 2001.

[12] www.centerforfuturehealth.org

[13] www.cc.gatech.edu/fce/ahri/

[14] http://ledger.southofboston.com/articles/2004/03/29/life/life02.txt

[15] A. van Halteren, D. Konstantas, R. Bults, K. Wac, N. Dokovsky, G. Koprinkov,V. Jones, I. Widya., "MobiHealth: ambulant patient monitoring over next generation public wireless networks.", *Stud Health Technol Inform*. 2004;106:107-22.

[16] D. Konstantas, A. van Halteren, R. Bults, K. Wac, I. Widya, N. Dokovsky, G. Koprinkov, V. Jones, R. Herzog, "Mobile patient monitoring: the MobiHealth system.", *In Stud Health Technol Inform*. 2004;103:307-14.

[17] A. van Halteren, R. Bults, K. Wac, N. Dokovsky, G. Koprinkov, I. Widya, D. Konstantas, V. Jones, R. Herzog, "Wireless body area networks for healthcare: the MobiHealth project.", *In Stud Health Technol Inform.* 2004;108:181-93. Review.

[18] N. Maglaveras, "Contact centers, pervasive computing and telemedicine: a quality health care triangle.", *Stud Health Technol Inform*. 2004;108:149-54.

[19] N. Maglaveras, I. Chouvarda, V. G. Koutkias, G. Gogou, I. Lekka, D. Goulis, A. Avramidis, C. Karvounis, G. Louridas, E. A. Balas, "The citizen health system (CHS): a Modular medical contact center providing quality telemedicine services**",** *IEEE Transactions on Information Technology in Biomedicine,* Volume 9, Issue 3, Sept. 2005 Page(s):353 - 362

[20] N. Maglaveras, "Citizen Health System: telehealth homecare.", *Stud Health Technol Inform*. 2003;92:117-25.

[21] N. Maglaveras, V. Koutkias, I. Chouvarda, D. G. Goulis, A. Avramides, D. Adamidis, G. Louridas, E. A. Balas, "Home care delivery through the mobile telecommunications platform: the Citizen Health System (CHS) perspective.", *Int J Med Inform*. 2002 Dec 18;68(1-3):99-111.

[22] N. Saranummi, I. Korhonen , M. van Gils and S. Kivisaari, "Barriers limiting the diffusion of ICT for proactive and pervasive health care," in *Proc. of the IX MEDICON*, Pula, Croatia, 2001.

[23] J. Yao, R. Schmitz, S. Warren, "A wearable point-of-care system for home use that incorporates plug-and-play and wireless standard.", *In IEEE Trans Inf Technol Biomed*. 2005 Sep;9(3):363-71.

[24] S. I. Ahamed, M. M. Haque, "An Omnipresent Formal Trust Model for Pervasive Computing Environment," COMPSAC 2007.

[25] M. Sharmin, S. Ahmed, S. I. Ahamed, M. Haque, and A. J Khan, "Healthcare Aide: Towards a Virtual Assistant for Doctors Using Pervasive Middleware, 1st Workshop on Ubiquitous and Pervasive Health Care (UbiCare 2006) in conjunction with Fourth Annual IEEE International Conference on Pervasive Computer and Communications (PerCom 2006), Pisa – Italy, Mar 2006, pp. 490-495.

[26] N. Talukder, S. I. Ahamed, M. M. Haque, "Context-Aware and Privacy-Preserving Access Control Framework for Pervasive Environment," to be appeared in the proceedings of SPEUCS-First workshop on Securiy and Privacy of emerging Ubiquitous Systems 2007, Aug 2007.

[27] N. J. Hopper and M. Blum. Secure Human Identification Protocols. In *Advances in Cryptology - ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 52–66, 2001.

[28] S. A. Weis, "Security parallels between people and pervasive devices," Pervasive Computing and Communications Workshops, 2005. Third IEEE International Conference ,2005 Page(s):105 – 109

[29] MARKS: a middleware for pervasive computing of Ubicomp Research Lab. (www.mscs.mu.edu/~ubicomp).

[30] M. Sharmin, S. Ahmed, and S. I. Ahamed, "MARKS (Middleware Adaptability for Resource Discovery, Knowledge Usability and Self-healing) in Pervasive Computing Environments", *Proceedings of the Third International Conference on Information Technology : New Generations (ITNG 2006),* April, 2006, Las Vegas, Nevada, USA, 306-313.

[31] L. Palen, P.Dourish, "Unpacking Privacy for a Networked World", *Proceedings of the ACM Conference on Human*

Factors in Computing Systems CHI 2003 (Fort Lauderdale, FL), 129-136. New York: ACM.

[32] J. Al-Muhtadi, R. Campbell, A. Kapadia, M. Dennis Mickunas, and S. Yi. "Routing through the mist: Privacy preserving communication in ubiquitous computing environments", In *Proceedigns of IEEE International Conference of Distributed Computing Systems (ICDCS)*, Vienna, Austria, Jul 2002.

[33] L. D. Chaum, "Untraceable electronic mail, return addresses,and digital pseudonyms", *Communications of the ACM*, 24(2):84–90, 1981.

[34] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing", *Communications of the ACM*, 42(2):39–41, 1999.