Survey on Privacy Preservation in contextaware web services

R. Vengadeswari

Research Scholar
Department of Computer Science
St. Joseph's College, Tiruchirappalli, India.

P. Joseph Charles

Assistant Professor
Department of Information Technology
St. Joseph's College, Tiruchirappalli, India.

Dr.S. Britto Ramesh Kumar

Assistant Professor
Department of Computer Science
St. Joseph's College, Tiruchirappalli, India.

Abstract*:*

Context awareness is a property of mobile devices that is defined complementarily to location awareness where as location may determine how certain processes in a device operates, context may be applied more flexibly with mobile users, especially with users of smart phones. survey of the research literature, here its intended to derive an overview of the actual dynamism of context awareness in healthcare and to identify strengths and weakness in this field of health care. A number of opportunities remain for this evolving field of research .Yet there is no consensus as to the most appropriate models or attributes to include in context awareness. Here conclude that greater understanding of which aspects of context are important in healthcare setting is required the inherent social technical nature of context aware application healthcare, and the need to draw on a number of disciplines to conduct this research.

Keywords: Context-awareness, Healthcare, Privacy

1. INTRODUCTION

Context awareness is a concept that has been described for sometimes, but technologies are now available to support the development of application. Healthcare systems could integrate context awareness computing not only to explore new tools but to propose useful and acceptable systems. A number of researches have underlined this context of work as particularly relevant to the evaluation of complex tools assisting the cooperation between workers. The critical issue with medical data management is the protection of private information of patients from being revealed to third parties. As the globe is interconnected, it is now possible that a patient from one location may consult a physician at a different location over the internet. The records of the patients are digitized and maintained as electronic medical records. Electronic medical records are often more useful that both patients and physicians can refer medical information wherever they are. Transmission of electronic medical records has raised new issues on privacy as it is more prone for the attackers to hack patients' information for performing malfunctions. Information 'leakage' is seen as having the potential to discourage to both patient and physician from participating in the system. The use of encryption, secure logins and passwords are certain security measures for privacy. Healthcare will evolve as new technologies are adopted.

2. REVIEW OF LITERATURE

Kamakshi et al [1] proposed a framework that allowed a systemic transformation of original data using randomized data perturbation technique and the modified data was then submitted as result of client's query through cryptographic approach. Using this approach they could achieve confidentiality at client as well as data owner sites. This model gave valid data mining results for analysis purpose but the actual or true data was not revealed.

Vasudevan et al [2] proposed a new solution by integrating the advantages of both privacy preserving data using role based access and cryptographic techniques with the view of minimizing information loss and privacy loss. By making use of cryptographic techniques to store sensitive data and providing access to the stored data based on an individual's role, and ensured that the data was safe from privacy breaches.

Heurix et al [3] proposed an overview of actual privacy threats and presented a pseudonymization approach that preserved the patient's privacy and data confidentiality. It allowed (direct care) primary use of

medical records by authorized health care providers and privacy preserving (non-direct care) secondary use by researchers. The solution also addressed the identifying nature of genetic data by extending the basic pseudonymization approach with query able encryption.

Kiran et al [4] proposed a framework that performed two major tasks of secure transmission and privacy of confidential information during mining. Secure transmission was handled by using elliptic curve cryptography and data distortion for privacy preservation was ensuring by highly secure environment. The authors had used data distortion mechanism for Privacy Preserving Data Mining (PPDM) to analyze how these methods could be used in the above medical data.

Adam et al [5] proposed an approach for integration and querying of health care data from multiple sources in a secure and privacy preserving manner. The basic idea of their approach was to use commutative encryption to encrypt all data items in each party's data set. Commutative encryption ensured that the encrypted keys from different data sets would be equal if and only if their original values were equal. The encryption prevented any source or querying party from extracting the individually identifiable or sensitive information from the joined data set. A similar commutative decryption ensured that only the querying party could extract the final result set.

Rui et al [6] examine the privacy perceptions of both patients and clinicians/practitioners. They examine how access to the data in an EHR system should be managed and controlled. For example, a patient should be able to restrict access to her EHR if she does not want to reveal such information to family members or healthcare providers and, at the same time, the authenticity of EHR with respect to content authentication and source verifiability should be addressed. On the other hand, clinicians should apply mechanisms to obtain patients' information from multiple EHR repositories accurately, securely, and timely. Furthermore, access to historical medical records should be, in general, granted to a practitioner if both the patient's consent and authorization from the respective Care Delivery Organization (CDO) are granted.

Giannetsos et al [7] distinguish privacy, integrity, and policy issues. They describe privacy requirements in the form of questions: who is asking for the data (Identity), how much does the data reveal about me (Granularity), how long will the data be retained (Time). Regarding integrity, they point out that the adversary can be both an outsider and an insider. As the personal nature of information significantly increases the interest in launching an attack such sensitive data should be delivered with the assurance that no intermediate users have tampered with them. Regarding policy, synergy between policies and technologies entails all of the challenges of interdisciplinary cooperation, the included parties should determine which issues are best addressed by policy or technology, while policy language can be used in order to express users preferences in a readable format, in case of a complex environment.

Oladimeji et al [8] privacy is achieved when the involved applications confer the ownership and control over disclosure to the principal of that information Thus, the interchange of the EHR over ad-hoc and pervasive communication channels is susceptible to data harvesting by malicious (passive attacker), while data can be distorted by spurious signals from a malicious (active) attacker.

It is equally important to outline which challenges a patient faces regarding health identity and anonymity.

Ahamed et al [9] provide two indicative scenarios regarding privacy violation and information leakage in a healthcare context from which they induce the following challenges: patient authorization is needed to access her EHR, but only on a need-to-know basis, while doctors/healthcare service providers hold the right to restrict access to prediction information, which may be kept secret for the sake of analysis and can only be revealed to the patient, upon request, after the end of treatment.

Comparative Analysis

Author	Proposed work	Advantages	Drawbacks/Limitation	External device
Kamakshi et al	Actual privacy threats and presented a pseudonymization approach that preserved the patient's privacy and data confidentiality.	Confidentiality at client as well as data owner sites.	The actual or true data was not revealed.	No
Vasudevan et al	view of minimizing information loss and privacy loss	cryptographic techniques to store sensitive data	information loss and privacy loss	No
Heurix et al	patient's privacy and data confidentiality of secure.	Data privacy	Secondary used data	NO
Kiran et al	Transmission and privacy of confidential information during mining.	highly secure environment.	authors had used data distortion mechanism	No
Adam et al	Integration and querying of health care data from multiple sources	secure and privacy preserving manner.	sensitive information from the joined data set	No
Rui et al	Security models and requirements for healthcare application clouds.	Development of the proposed EHR security.	Such credentials, while still making an assertion about some property, status, or right of their owner, do not reveal the owner's identity.	No
Giannetsos et al	To attain an understanding of the types of issues and challenges that has been emerging over the past five years.	Communication Security.	Security and Communication Networks not clear.	No
Oladimeji et al	Goal-centric and policy-driven framework for deriving security and privacy risk mitigation strategies in ubiquitous health information interchange.	improve the quality of healthcare delivery	Fully systematically	No
Ahamed et al	Privacy challenges that arise when designing pervasive healthcare environments and discuss addressing some of these issues in a home based patient monitoring system.	improve patient independent living and quality of life and pay special attention to issues of security, privacy, transparency	Information leakage through context-aware services.	No

3. CONCLUSION

This all the papers proposes a security model for health information networks and a minimum set of security mechanisms needed to address security requirements of the model. These are shown to counter the security threats in a public network. The preservation of user private medical data through a role based access control system. The users of the system are identified as doctor, nurse and patient. The information flow of the system is controlled with the hierarchy of the role. The system is designed to reveal user's medical data only to those who are involved in the treatment process of the concern patient. Others could not view the information of one's personal data. Initially the users of the system are expected to register themselves before they participate in health consultation. Users role are designated as doctor, nurse and patient. The prefix of the login id is itself designed to depict the role of the user. The minimum set of security controls providers a simple a convenient framework for health information networks to design and implement their security architecture.

References

[1] Kamakshi, P. and Dr. Vinaya Babu, A. "Preserving Privacy and sharing the data in Distributed Environment using Cryptographic Technique on perturbed data", Journal of computing, volume 2, issues 4, April 2010, ISSN 2151-9617.

[2] Lalanthika vasudevan, S. E. Deepa sukanya, N. and Aarthi. "Privacy Preserving Data Mining using Cryptographic Role Based Access Control Approach". Proceeding of the International Multi conference of engineers and computer scientists 2008, IMECS 2008, 19-21 March 2008, Hong kong.

[3] Johannes Heurix and Thomas Neubauer, "Privacy Preserving Storage and Access of Medical Data through Pseudonymization and Encryption", Springer – Verlag Berlin Heidelberg 2011.

[4] Kiran, P. Sathish kumar, S. Dr. Kavya, N. P. "A Novel Framework using Elliptic Curve Cryptography for Extremely Secure Transmission in Distributed Privacy Preserving Data Mining", Advanced Computing: an International Journal (ACIJ), vol3, No.2, March 2012.

[5] Nabil Adam, Ph.D, Tom white M. D, Basit Shafig Ph.D, Jaideep Vaidya Ph.D, and Xiaoyun. "Privacy preserving Integration of Healthcare Data", AMIA Annu symp proc. 2007, 2007 1-5.

[6] Rui, Z. and Liu, L. "Security models and requirements for health care application clouds", Paper presented at the 33rd International Conference on Cloud Computing, USA, and July 2010.

[7] Giannetsos, T. Dimitriou, T. and Prasad, N.R. "People-centric sensing in assistive healthcare: Privacy challenges and directions", Security and Communication Networks 4.11:1295–1307.

[8] Oladimeji, E. A. Chung, L. Jung, H. T. and Kim, J. "Managing security and privacy in ubiquitous e-Health information interchange", Paper presented at the 5th International Conference on Ubiquitous Information Management and Communication, ACM, Korea, February 2011.

[9] Ahamed, S. I. Talukder, N. and Kameas A. D. "Towards Privacy Protection in Pervasive Healthcare", Paper presented at the 3rd International Conference on Intelligent Environments, Ulm, Germany, and September 2007.