ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

A Review on Privacy Control Techniques in Context-aware Web Services

[I]R. Stephen, [II]P. Joseph Charles, [III]Dr. S. Britto Ramesh Kumar
[I]M.Phil Scholar, Dept. of Computer Science, St.Joseph's college, Trichy Tamilnadu, India
[II]Assistant Professor, Dept. of Information Technology, St.Joseph's college, Trichy Tamilnadu, India.
[III]Research Advisor, Dept. of Computer Science, St.Joseph's college, Trichy Tamilnadu, India.

Abstract
A system is context-aware if it uses context to provide relevant information or services to the user, where relevancy depends on the user's task. Context-awareness is offering services to users with react of proactively to user environment and service conditions. In the internet world web services as building blocks in such context-aware web services. The main goal of context-aware system is to track and identify the users. The mobility feature and personal assistant devices are the most computing have made context of user and it is an important aspects of context-aware system. The rise of information and communication technologies along with context-aware web services and the whole internet platform has inclined towards pervasiveness. This paper mainly addresses key performance issues, challenges and techniques for privacy control in context-aware web services. It also focuses on key issues related to these existing privacy control techniques and summarizes them.

Keywords
Context-aware web services, Privacy, Privacy preferences, Privacy protection system

I. Introduction

A context is being termed as "some information which can be utilized to identify the present condition of any entity" [1]. In a real time scenario, numerous examples related to the context are given such as location, time, temperature, noise, the bandwidth of communication, connectivity of network etc. "A system is considered to be context aware if it utilizes the context in an effort to provide the appropriate information or service to the user where appropriate and significant information depends upon the requirement and need of the user". As context-aware web services are becoming more and more popular for supporting various applications, there are also increasing demands for web services privacy technologies in the industry and research community [2]. The information exchange in such a web services-based environment must be protected by
privacy-enhancing technologies. The implicit and transparent collection of data offers more privacy concerns rather then those initiated by the user itself. The objective of a privacy-preserving in location based services is to protect the privacy of a user's location while maintaining a high level of location based services accuracy.

Phones, especially smart phones, are increasingly the most common gateway for people to access the information and services available on the web [3]. Smart phones are programmable devices that come with variety of embedded sensors such as general packet service, accelerometers, microphones, cameras and others. These sensors can be used to collect information about users and their surroundings in terms of location, motion and temperature. Location awareness is one important aspect of context-aware system. However, context encompasses the user's location, because other things of interest are also mobile and changing. The improvements in mobile technology, smart phones and sensor networks present a unique opportunity for context-aware systems to access the networking systems. A very important issue in such applications is that of privacy. While context-aware systems and applications face security threats similar to other distributed and mobile applications, privacy and security aspects are more prominent due do the sensitive nature of context information. So, we can observe that along with user privacy protection by hiding users' identity or location, we require to protect data privacy.

The rest of the paper is organized as follows: section II presents issues and related works in context-aware web services. Section III discusses various privacy control techniques in context-aware web services proposed by researchers. Section IV presents conclusion and discussion on privacy control techniques.

II. Literature review and related works

Saad et al [1] proposed a review on the security and privacy issues related with context-aware systems. It is a survey paper about security requirements, the author discussed various security requirements for context-aware systems, especially privacy and confidentiality security requirements are basically related to protect the use of some highly sensitive information or data. The author proposes various frameworks for implementing efficient and effective security on user's information in the context-aware system. The author described an inter relationship between frameworks and security models. The privacy security models relationship with Cerberus and Kerberos frameworks and it is used for achieving the purpose of fulfilling and implementing various security requirements in the context-aware systems. These frameworks aimed at the identity of the user who is requesting access to services of context-aware systems.

Nirmal et al [2] developed architecture for context-aware web services based on privacy preferences. This paper aims at contributing privacy management layer to the context-aware web service architecture. The purpose of privacy management layer is to encourage the concept of privacy awareness in this class of services. The author described architecture for privacy in context targeting the user privacy preferences to discover the most secure and flexible web services. The author used the information category chart about user's information for privacy policy and also used sensitive level of the information category according to user convenience. In this paper, with the increase in adoption of context-aware web services developing privacy policies become more and more important as it simplifies the possibility of applying

user's privacy preferences.

Pramod et al [3] discussed in this paper, the mobile devices such as smart phones as the primary access point to networked information. The author aimed at existing system focus mostly on location, including user's location and surroundings. A key element of this paper work is the use of collaborative information sharing where devices share and integrate knowledge about their context. The author introduces the need for privacy and security mechanism. The author presents a framework to provide users with appropriate levels of privacy to protect the personal information based on user's devices. As a future work the author plans to carry out user studies to evaluate utility of the propose privacy control mechanism.

Georgia described in [4] any person can right to protect their information or services to user environment and service conditions. Context-awareness offers user's services; in this paper the reflection of user privacy preferences in the provision of context-aware web services is addressed. The author introduces consumer privacy language is proposed with an adaptation mechanism for SOAP messages. The author used consumer privacy preferences for comparing personal context with environment context and used privacy enforcer architecture to developed privacy preferences in context-aware web services.

Aniket et al [5] designed a context-aware privacy protection system for location based services. In this paper design of privacy-preserving techniques is principled in terms of time and space complexities. The aim of this paper is protection for data privacy and communication anonymity. The author has implemented context-aware privacy protection system with Google maps, a popular location based system. The author introduced various-size-grid Hilbert curve mapping for developing protection of user location privacy. The author's existing schemes on preserving location privacy in LBS can be generally classified into two categories, one is trusted third party based and another one is user based schemes. Most research on trusted third-party based schemes adopts a k-anonymity based framework.

Supriyo et al [6] developed a framework for context-aware privacy of sensor data on mobile system. In this system privacy is needed when a user shares personal sensor data with applications on a Smartphone. This paper focused on the more general problem of choosing what data to share, in such a way that certain kinds of inferences. The author proposed ipshield as a privacy-aware framework which uses current user context together with a model of user behavior. The author proposed conceptualizes ipShield, the inference privacy framework and describe the implementation on an Android-based mobile platform and prior work on privacy frameworks rely on static privacy policies, or use information flow techniques to detect potential leakage from applications and apply binary policies of complete access or no access to data at all. In this paper with the comparison of ipShield, it makes two main contributions. First, it implements context-aware privacy policies. Second, ipShield, uses a graphical model to capture initial adversarial knowledge and its subsequent increase with each disclosure.

Arijit described [7] the context protecting privacy preservation in ubiquitous computing, because context-awareness is an important issue in ubiquitous computing domain. In this paper, the author proposed a scheme which provides two layer privacy protection of user's or application's context data. The objective of this paper is to protecting spatial and temporal contextual information. The author proposed scheme based on cluster-based private data aggregation and it performs privacy-preserving data aggregation in low communication overhead with high computational. In cluster-based private data, each cluster leverages the additive property of polynomials to calculate the desired aggregate value. The author proposed the context protecting privacy preservation scheme depends upon cluster based. This scheme has two layers, in first layer the contextual information derived from spatial and temporal domain and identity of the user is protected. In second layer, the actual contextual data privacy protection is made using the concept of privacy-preserving data aggregation.

Po-Wah et al [8] described privacy in a context-aware according to social networking based on recommendation system for enterprise. This paper outlines hierarchical privacy architecture, because users are willing to share private information. So, the protection of private information is needed. The author aimed at developing instant knowledge privacy architecture to provide privacy services to both enterprise and its users. In this paper the author used IK model that is instant knowledge model to developing privacy in context-aware system. Although privacy is a social construction, modern technology has changed the landscape of how privacy needs to be controlled. Thus, there is a duality between technical solutions and the social structures in which those solutions operate, with the help of model of the IK system a proposed technical privacy requirements for the model and the social implications motivating these requirements.

Yonnim et al [9] developed a method of forecasting the privacy concern based on an index model of privacy concern and also an approach method of triggering the privacy preserving service. This paper is aimed at recognizing user regarding privacy concern and then the service provider to supply a service which has a proper level of privacy preservation. The author developed a prototype web-based system to show the availability of a triggering method in privacy preserving service. The author aimed to easily forecast privacy concern degree of users before a service offer as a form of indexing, but it was not easy to acquire and express user's feelings about privacy concern. So before service offer an improvement of service quality is needed.

Daniele et al [10] introduced context-aware retrieval points of interest, it's a popular location- based services. The access to points of interest services is prone to potentially serious privacy issues. Since requests for points of interest often include sensitive information like user's location and personal interests. In this paper SpaceTwist and AnonTwist algorithms are used, the purpose of these algorithms to enforce location privacy. According to SpaceTwist algorithm a fake user's location communicated. The author proposed a novel technique to protect the privacy of users accessing to mobile services for POIs retrieval. However, the access to such services is prone to potentially serious privacy issues, since requests include sensitive information and handled by untrusted parties. Different privacy threats may arise, depending on the external knowledge available to an adversary, and on the kind of information that is considered sensitive by a user.

Pandit et al [11] described in this paper surveys current state of research and analyses the effect of threat on the privacy of context aware system users. The author proposed a novel framework to tackle the privacy preservation issue comprehensively, from user perspective as well as service provider perspective. According to applications like finding the restaurants or movies playing in an area do not require the exact location and context of the user. When a user's movement in public spaces is tracked and systematically recorded along with the context of user's actions and user contextual

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

privacy is under threat. In recent times, most people carry a smart internet enabled mobile device and perform transactions or use various features provided by the smart phones. Location of the device and the user, user's context and consequently the details of user that is stored in the phone. Currently, the services that are being provided largely are location dependent services.

Jalal et al [12] proposed a flexible, privacy-preserving authentication framework for ubiquitous computing. The proliferation of smart gadgets, appliances, mobile devices, PDAs and sensors has enabled the construction of ubiquitous computing environments. The objective of this paper is proposing an authentication framework that addresses this problem through the use of different wearable and embedded devices. These devices authenticate entities with varied levels of confidence, in a transparent, convenient, and private manner, allowing the framework to blend nicely into ubiquitous computing environments. However, the real life deployment of active information spaces is hindered by poor and inadequate security measures, particularly, authentication and access control techniques.

Stefanie et al [13] aimed at to develop context-aware and location-based services to next generation networks. That's the migration from legacy networks to next generation networks requires network-spanning service enablers to offer network features to value-added services. This paper introduced a location service enabler for legacy and future networks. The enabler supplies location information to value-added services taking into account privacy issues. Value-added services are for example context-aware and location-based mobile applications as well as emergency services.

Emin described [14] privacy in context-aware mobile business applications, particularly users require full privacy control over their context data like identity, time schedule, profiles, location, etc. Particularly platform for privacy preferences proposed a privacy solution for internet users. The aim of this paper is to extend platform for privacy preferences to support user-centric privacy aspects in both pull and push services regarding context-aware mobile business applications. As a preliminary work, a privacy context data model from the privacy perspective will be formally described. Afterwards, Platform for privacy preferences extension for the privacy architecture and policies will be designed. In future work the author proposed the required security protocols and cryptographic methods will be developed to enforce privacy with platform for privacy preferences policies and platform for privacy preferences extension will be integrated within the applications of an existing mobile business framework.

Xiaodong et al [15] proposed modeling privacy control in context-aware system, this paper aimed at to describe a theoretical model for privacy control in context-aware systems based on a core abstraction of information spaces. The author mainly focused on deriving socially based privacy objectives in pervasive computing environments. The author aimed at to use information spaces to construct a model for privacy control that supports users socially based privacy objectives and also discussed how to introduce decentralization, a desirable property for many pervasive computing systems, into user's information space model, using unified privacy tagging.

III. Comparison of privacy control techniques

Table 1: Comparison of privacy control techniques

Author	Tool used	Technique	Future work
Saad. A [1]	Cerberus, Kerberos	Security requirements Framework	Design secure architecture
Nirmal. G [2]	Matrix formula	Match making process	Design privacy preferences layer
Pramod. J [3]	Collaborative information sharing	Design framework	Utility of the propose privacy control
Georgia. M [4]	Consumer privacy language	Adaptation mechanism	Propose privacy enforcer architecture
Aniket. P [5]	Hilbert curve	Privacy preserving	Adopts k-anonymity based framework
Supriyo. C [6]	Ipshield framework	Privacy policy	Define white listed inferences
Arijit. U [7]	Cluster based	Spatial, data layers	Complexity analysis
Po-who. Y [8]	IK model	Privacy architecture	Adopt technical requirements
Yonnim. L [9]	Privacy index model	Method of triggering	Quality of service
Daniele. R [10]	POIs retrieval	Space twist, anonymity	Experimental evaluation
Pandit. A [11]	User perspective	Novel framework	Design secure location based services
Jalal. A [12]	Kerberos	Access control	Gaia research project
Stefanie. R [13]	Service enabler	User's context	Novel architecture
Emin. I [14]	Context data model	Usability tests	Cryptography methods
Xiaodong. J [15]	Core abstraction	Decentrali-zation	Trust modeling

IV. Conclusion and discussion

Context-aware web services are to provide a services or information depends on user's requirements and need of the user. Each and every task of services behind the web services with service provider. Most of the people used smart phones, personal assistant devices to access the services through the internet. So need to protect the user's personal information while user gives their details to access the services and also protect the user's privacy preferences. Many frameworks have been proposed and discussed about privacy in context-aware web services. So in this paper the problem of privacy control with its different techniques in context-aware web services has been considered. The ultimate

goal of context-aware web services is to provide the quality of services to the end-user, who can profit from web services offering both context and privacy-awareness.

References

[1]. *S. Almutairi, H. Aldabbas, A. Abu-Samaha. "Review on the security related issues in context aware system". De montfort university, software technology research laboratory (STRL) Leicester, united kingdom. In proceedings of the International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 3, June 2012.*

[2]. *N. Gaud, A. Deen, S. Silakari. "Architecture for discovery of context-aware web services based on privacy preferences". Computer science & Engineering, U.I.T, R.G.P.V. Bhopal, Madhya Pradesh, India. In proceedings of the Fourth International Conference on Computational Intelligence and Communication Networks 2012.*

[3]. *P. Jagtap, A. Joshi, T. Finin, L. Zavala. "Preserving Privacy in Context-Aware Systems" Computer Science and Electrical Engineering, University of Maryland, Baltimore County, Baltimore, MD 21250 USA.*

[4]. *G. M. Kapitsaki. "Reflecting user privacy preferences in context-aware Web Services". Department of Computer Science University of Cyprus Nicosia, Cyprus. In proceedings of the IEEE 20th International Conference on Web Services 2013.*

[5]. *A.Pingley. "CAP: A Context-Aware Privacy Protection System for Location-Based Services". George Washington University.*

[6]. *S. Chakraborty, K. R. Raghavan, M. P. Johnson, M. B. Srivastava. "A Framework for Context-Aware Privacy of Sensor Data on Mobile Systems". University of California, Los Angeles. ACM HotMobile'13, February 26–27, 2013.*

[7]. *A.Ukil. "Context Protecting Privacy Preservation in Ubiquitous Computing". Innovation Labs, Tata Consultancy Services, Kolkata, India. In proceedings of the IEEE CISIM 2010, Krakow, Poland.*

[8]. *P. Yau, A. Tomlinson. "Towards privacy in a context-aware social network based recommendation system". Information Security Group, Royal Holloway, University of London Egham, Surrey, TW20 0EX, UK.*

[9]. *Y. Lee, O. Kwon. "An index-based privacy preserving service trigger in context-aware computing environments", School of International Management, Kyunghee University, Seochun, Ghiheung, Yongin, Kyunggi-do, South Korea. Expert Systems with Applications 37 (2010) 5192–5200.*

[10]. *D.Riboni, L. Pareschi, C. Bettini. "Integrating Identity, Location, and Absence Privacy in Context-aware Retrieval of Points of Interest". University, degli Studi di Milano, D.I.Co., EveryWare Lab.*

[11]. *A.A. Pandit, Dr. A. Kumar, " Conceptual Framework and a Critical Review for Privacy Preservation in Context Aware Systems", in proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, IEEE 2012, pp.435-442.*

[12]. *J. Al-Muhtadi, A. Ranganathan, R. Campbell, M. D. Mickunas, "A Flexible, Privacy Preserving Authentication Framework for Ubiquitous Computing Environments", Proceedings of the 22 nd International Conference on Distributed Computing Systems Workshops (ICDCSW'02), IEEE 2002.*

[13]. *S. Richter, A. Bohm, "A location and privacy service enabler for context-aware and location-based services in NGN", T-Systems Enterprise Services GmbH, Germany.*

[14]. *E. I. Tatli, "privacy in context-aware mobile business applications", Department of Computer Science, University of Mannheim, Germany.*

[15]. *X. Jiang, J. A. Landay, "Modeling privacy control in context-aware system", University of California, Berkeley. 1536-1268/02/$17.00 © 2002 IEEE*