REVIEW ON THE SECURITY RELATED ISSUES IN CONTEXT AWARE SYSTEM

Saad Almutairi[1], Hamza Aldabbas[1] and Ala Abu-Samaha[2]

[1]De Montfort University, Software Technology Research Laboratory (STRL)
Leicester, United Kingdom
{Almutairi,hamza}@dmu.ac.uk
[2] Middle East University, Amman, Jordon
asamaha@meu.edu.jo

ABSTRACT

A context aware system is recognized as a "system which uses any context information previous to, or in the duration of, service stipulations", whereas the main goal of this system is to track and identify the users. The mobility feature of most computing and personal assistance devices have made the 'context of the user' an important aspect of the system, affecting its development process in terms of end-user requirements and system behaviour. Context Aware Systems are different from traditional systems as they provide unique features such as heterogeneity, high complexity and artificial intelligence. Since the parameters that constitute a context aware system, such as location and time of the day are rapidly changing. The use and importance of this system is increasing and therefore becoming a major part in prospective wireless systems. However, beside the numerous advantages, context-aware systems have also come up with the numerous issues and challenges related to privacy and security of the user's information in these systems. Therefore, this paper is mainly aimed at a review of the security and privacy issues related with context-aware systems. It also gives a brief introduction regarding the preferred and suitable frameworks required to implement the security requirements. It further focuses on the main question for most researchers about the frameworks used for context-aware systems.

KEYWORDS

Context, context-aware systems, security requirements, frameworks in context-aware systems.

1. INTRODUCTION

"The most profound technologies are those that disappear. They weave them selves into the fabric of everyday life until they are indistinguishable from it" [30]. This statement is quoted from Mark Weiser's visionary article `The Computer for the Twenty-First Century'. This article was published in 1991 and it was considered as a head of its time, Mark Weiser's vision has given birth to a new field in computing namely pervasive computing (aka ubiquitous computing) which is also guided to explore the vital concept of context awareness. Context awareness is the initial element of pervasive computing. Since the first introduced by Schilit and Theimer [31], the term 'context aware system' attracted many researches, for example, Dey and Abowd [1] defined Context as any information which is used in characterising the current condition of any object or entity. 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 [2]. In a much broader perspective, a context is being termed as "some information which can be utilized to identify the present condition of any entity". Moreover, Dey and Abowd have further talked about the definition on the basis on which a

DOI : 10.5121/ijwmn.2012.4313

system can be considered as a context aware system. According to the definition, "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" [1]. Sitou and Spenfelner pointed out that context aware application "seem to be particularly prone to problems related toa discrepancy between user expectation and system behaviour" [25]. In almost the same manner, a context aware system is recognized as a "system which uses any context information previous to, or in the duration of, service stipulations, whereas the main goal of this system is to track and identify the users" [3].

Context Aware Systems are different from traditional systems as they provide unique features such as heterogeneity, high complexity and artificial intelligence. Since the parameters that constitute a context aware system, such as location and time of the day are rapidly changing [32]. Thus the use and importance of context aware system is increasing and therefore becoming a major part in prospective wireless systems. It is being highlighted as important and quite useful due to several reasons such as context can reduce the input cost, it can provide an exciting user experiences without much effort on the user`s part and also users can benefit through context sharing [4,34].

This paper is organized into five sections. In section 2, we will have some discussion about background history along with some related works which have been done in the past by various researchers. Section 3 will review the security issues which related to context aware systems. Section 4 will present some frameworks which have been proposed in the literature review, and finally Section 5 will summarize our conclusion.

2. BACKGROUND AND CONTEXT AWARE APPLICATIONS

Various researchers have highlighted and discussed the basic concept of context and context aware systems in their own way. Most of them are not quite in favour of the most basic concept and have tried to come forward with their own definition in a more precise manner. For instance, Schilit *et al.* [5] have mentioned three points which are required to be considered when discussing a context. Firstly, at what location you are, with whom you are roaming around and what kind of various resources you are utilizing. Furthermore, Chen *et al.*[6] has termed context as a collective combination of environmental states and settings that judges the behaviour of an application or which are important from the user's perspective. Moreover, Dey*et al.*[7] has defined context as information that is used to determine the situation of any entity such as a person, place. These entities are further considered to be very useful for establishing an efficient interaction between the users and any application.

There are many applications which can be considered as context aware or having greater context aware applications to be used. These applications were used in the recent past and many examples can be quoted from the current scenario. According to various researches, many context aware applications were lab based and provided the designers with the facility to work in a proper laboratory environment. A typical example of the most initial kind of context aware application is the Active Badge introduced in the early 90's [8]. Regarding its working, it made use of badges in order to transfer infrared signals to various sensors located in numerous buildings. This case helped to track the user's location and therefore automatically redirect the user's call to that exact tracked location. Another example of context aware application is ParcTab which also serves and provides the user with the same kind of functionality as provided by Active Badge. However this application performs this procedure by making use of much simpler badges [9]. Furthermore, it was also implemented in a form of a PDA (Personal Digital Assistant) in order to introduce much richer context aware applications.

There are many others quite efficient and effective context aware applications which are mobile based and therefore provide some potential facilities and functionalities for the users. These mobile applications come up with various user friendly services such as displaying the relevant information to the user, automatically performing any functionality or providing a service to the user, etc [10].As mentioned above, tourist information systems are a kind of application which makes some major use of context aware softwares nowadays. The major example in this regard is Cyber Guide, a mobile based context aware system used by visitors. It provides the users with information on various places and locations which could be of interest to users by making efficient use of the history of the places visited by users and the direction of movement, etc [11]. Another example in this regard is a GUIDE system which serves as a tour guiding system for the visitors in a city of Lancaster [12]. Moreover, Mobile Location-Aware Handheld Event is another tour guiding system which acts as an event planner and therefore serves as a tour guiding system for the visitor by making GPS location acquisition [13]. Furthermore, Access Sights also acts as a tour guide system and therefore serves people with special needs, like blind users or weak sighted users, with a tour guiding facility [14].

3. REQUIREMENTS & DESIGN CONSIDERATIONS

Before embarking into the discussion especially on some potential security issues regarding the context aware applications, a brief insight will be thrown on to the basic categories of context as a whole. Most of the studies have come forward with various categories of context. However, the majority have agreed collectively upon three - four as the major ones. For instance, in research conducted by Chen and Kotz [14], four basic categories of context have been mentioned. These are: *Computing Context, User Context, Physical Context and Time Context.* A brief description about the information and areas covered by each is given below [37]:

- **Computing context:** covers areas and information related to system connectivity, inter networking, other computing related assets like printers and workstations, CPU, Memory resources etc [14]. Another important aspect and characteristic of context aware applications in terms of computing context is that users sometimes use multiple devices. Therefore they prefer the devices which provide the facility of performing multiple functionalities at the same time [15]. These kinds of devices cover mobile applications and PDAs etc.

- **User context**: contains information related to the user's application usage which includes the user's personal information, preferences, current location, and potential activity, etc [14]. The choice of users can be characterised by the details related to the kind of preferences they have [16]. For instance, some users are willing to go to any specified location by taxi or hiring private transport whereas some other users are willing to travel walking distance only [16]. Therefore, for this reason, a component or facility for storage and efficiently using preference related information is required.

- **Physical context**: covers areas and provides information regarding Location, Time, Destinations, lighting, Physical and environmental conditions, etc [14]. For instance, in most cases the users require access to information such as weather forecasts, route directions, ongoing traffic situations and temperature related updates, etc [16]. Therefore the requirement is always kind of useful information which is going to be updated on a regular basis and should always be made available to the users.

- **Time context**: provides information and access about the time and calendar related information on a daily, weekly or monthly basis [14].

3.1. PRIVACY ISSUES IN CONTEXT AWARE

Privacy concern which related to current context aware systems is a very challenging issue, and is being considered as quite an important and a hot topic to be discussed. However, it has been discussed and mentioned by the researchers that there are many factors which play quite a major role in raising some considerable privacy concerns and potential security issues in the mind of the user who is utilising and accessing the context aware based applications. These factors can be further classified into two categories; small scale and large scale. Small scale factors directly affect the personal, private and sensitive information of the users and therefore users are directly affected by these factors. On the other hand, large factors are the total opposite of the small ones and therefore make much less impact directly to the private or sensitive data of a user.

Furthermore, a brief highlight will be thrown onto some various potential factors that raise some potential privacy concerns among the users of context aware system applications [17].

- *Information Receiver reliability:* One of the factors which raises some privacy concerns among the users of context aware system applications is the reliability and authenticity of the receiver who receives the user's information. Users sometimes have an ambiguity or doubt on the credibility of the person who receives and uses their information. Therefore, the only option left for the user is to show some trust and confidence on the credibility and authenticity of the receiver's information.
- *Possible usage of user's information:* Another factor mentioned by some researchers which raises privacy concerns among the user is the kind of usage which is going to be made related to their private and sensitive data at the receiver's end.The concerns arise when the users think or become doubtful about the proper or positive usage of their sensitive information.
- *Level of sensitivity in terms of users data:* According to studies, some times the level or extent of sensitivity and privacy of user's data also raises a concern in the user's mind whether to share or transmit this kind of data or not . The user thinks twice whether it will be secure and good enough to make the private and sensitive data available and accessible to a third party or not.
- *Environment in which user's information is shared or its privacy is being disclosed:* This is a factor which raises concern in the user's mind whether they should be sharing and giving access to their information in various contexts and environments. The users are sometimes reluctant to share their information in any context or environment due to the concerns about the reliability and authenticity of the context. Moreover, a change or any update in the context also triggers some serious privacy concerns among the users and therefore prevents them further in sharing their sensitive and highly secure information in that very context.

3.2. SECURITY REQUIREMENTS FOR CONTEXT AWARE SYSTEMS

Many researchers have come up with, and collectively agreed upon, some common steps to be undertaken in an effort to implement the most efficient and effective level of computer security and applications working in a context aware system environment. The main purpose is to ensure that the level of risk is also going to be reduced by implementing these security steps. These requirements will be discussed to consider the security steps required to be undertaken in order to provide reliable security to context aware systems and applications. The following are the security requirements which been specified briefly below by International Telecommunications Union (ITU-T) represented in their recommendation X.805 and X.800 [17, 18, 25, 26, 27, 28, 29].

- **Authentication:** Authentication is basically a process of verifying the identity of the entity which is accessing the facilities of context based systems and applications. Authentication is essential to verify the identity of every node in the system and its eligibility to access the network. This means that, nodes in the Context aware systems are required to verify the identities of the communicated entities in the network, to make sure that these nodes are communicating with the correct entity, in order to make sure that the user who is trying to access the context aware system is reliable or eligible to access the system. This will help to validate the user's identity and will assist in ensuring that only the authorized user can access the system. A need of mutual authentication is justified in the case of security infrastructure to validate the user's identity. Furthermore, it has been said that in order to validate and run the authentication process, it is not always required that the user or device should be connected to the application identity. This could be done by authentication of users in terms of their context e.g., nicknames in IRC chat rooms.

- **Access Control:** This step in the security requirement is defined as a process of giving permission or access to the authentic and real users to utilise the system facilities. At the same time, its other purpose is to restrict access to the system utilities against fake or unauthorized users. In addition, users should be capable of restricting each other from accessing their private information. There are many techniques that can be used for access control such as Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC) [25].This requirement is actually executed to verify or to validate the related privileges with each user. If the verified or reliable user matches and fulfills the required privileges then the access or authority to use the system resources will be granted to the user. Otherwise the request for accessing the resources will be rejected due to the failure of providing the relevant permission information [33, 36].

- **Privacy and confidentiality:** This requirement is basically related to protect or restrict the use of some highly sensitive, private or secure information or data from being shared or being made available to anyone else without your permission or willingness to do so. Each node in the context aware system has to secure both the information that is exchanged between each other; and secure the location information and the data stored on these nodes. Privacy means preventing the identity and the location of the nodes from being disclosed to any other entities. While confidentiality means keeping the secrecy of the exchanged data from being revealed to those who have not permission to access it. According to some previous research, it is considered as being someone's capability to protect or restrict your information from going public to others or keeping the sensitive data quite confidential and not disclosing it to unwanted entities in some way. However, implementing this concept in context-aware is considered a very challenging task. Most of the studies have claimed that, it is highly possible that the users who want to access and use the functionalities and facilities of context-aware systems quite increasingly would get somehow drawn in sharing the contextual information. In order to make sure such users would not be sharing or providing access to their private information to other entities, there should be a need to apply some methods to make the information confidential from unwanted users.

- **Data Integrity:** The data transmitted between users in the context aware systems should be received to the intended entities without been tampered with or changed by unauthorized modification. This requirement is essential especially in military, banking and aircraft control systems, where data modification would cause potential damage. Previous studies have showed that the integrity of the user's data can be acquired by providing assurance that the data is not going to be accessed and therefore altered or modified by the fake, illegal or invalid users. The integrity requirement in context-aware systems is defined as a concept in which the access to the user's resources is not allocated or assigned to any illegal or incorrect user. Moreover, this will create a serious problem in tracking the illegal and unauthorized users accessing and modifying the user's context in an illegal manner.

- **Availability and survivability:** The services and applications in the system should be accessible, when needed, even in the presence of faults or malicious attack such as denial-of service attack (DoS). While survivability means the capability of the network to restore its normal services under such these conditions. These two requirements should be supported in any context aware system. Availability in this kind of systems is related with the concept of making sure that the services, facilities and functionalities required by the users are made available or accessible to them. This requirement is considered as important in the case of wireless systems where there is a total lack or unavailability of required services and functionalities by the user. This availability issue could be quite serious in many other critical applications as well.

4. RELATED FRAMWORKS IN CONTEXT AWARE SYSTEMS

Previous studies have proposed various frameworks for implementing efficient and effective security on user's information in the context and the context-aware system as a whole. The main purpose of implementing these frameworks is to gain and acquire various security related requirements and models which mentioned before. However, each framework has come up with its own purpose of implementing and serving with a unique kind of security requirements and models. For this reason, each separate framework has got its own importance and is therefore definitely required to be implemented and fulfilled. The following are brief details about various frameworks which been used to implement various security requirements along with the kind of unique purpose they fulfil and which are therefore being used in the context-aware systems.

- **Confab Framework:** As discussed before, users should be able to apply some privacy, confidentiality and therefore protect their private or personal information from the illegal access of unauthorized users. Therefore, in an effort to fulfil this security requirement. Jason *et al.* [19] came forward with an architecture called Confab in order to provide privacy to the users for the protection of their sensitive information. Talking specifically regarding its purpose and workings, Confab framework is basically designed for providing protection and reliable security to the information relevant to the user's location in ubiquitous systems. Moreover, its working hierarchy is based on some specific analysis related to basis privacy requirements of end-users and the application developers [20]. The private information of the user is acquired, stored and therefore processed on the user's device instead of taking and storing it on some other device for security purposes.

- **Uniform Access Control (UAC):** Covington *et al.* [21] came up with a uniform access control framework specifically for serving the purpose of environmental roles. Moreover, it has been declared and claimed as a further extension to the Role-Based Access Control (RBAC) model. Regarding the RBAC model, specific privileges or access rights to the users towards the system services are linked with the environmental roles. Talking specifically about the concept behind the roles, a role can be a developer or a manager in a top level domain. Moreover, it is responsible for analysing and determining the security aspects related to Context-aware systems and applications in ubiquitous environments [22, 36].

- **General Role Based Access Control (GRBAC):** Furthermore, these environment roles are based on another framework called the General Role Based Access Control. Ahamad *et al.*[22] have highlighted a main difference between RBAC and GRBAC models. Generally RBAC framework is a basic model which only covers and relates towards subject-oriented approach whereas GRBAC allows the defining of access control policy depending upon not only the subject but also on other essential and important factors like object or environment.

- **Gaia:** It is designed to assist the building of smart space applications [5,35], such as smart homes and meeting rooms. It consists of a set of core services and a framework for building distributed context-aware applications. Gaia's event manager service enables applications to be developed as loosely coupled components, and can provide basic fault tolerance by allowing failed event producers to be automatically replaced. Gaia's remaining four services support various forms of context-awareness, and include the following :

    - **Context service:** This allows applications to find providers for the context information they require.

    - **Presence service***:* This monitors the entities entering and leaving a smart space (including people as well as hardware and software components).

    - **Space repository:** This maintains descriptions of hardware and software components.

    - **Context file system:** This associates files with relevant context information and dynamically constructs virtual directory hierarchies according to the current context [23].

  According to Roman *et al.* [24] defined generic context-based software architecture for physical spaces, such as Gaia. Moreover, they defined physical space as a "geographic region with limited and well defined boundaries, containing physical objects, heterogeneous networked devices, and users performing a range of activities". Based and depending upon this very physical space, active space providers assist the users of context-aware systems and application to directly connect and therefore interact with the physical space. Again, this framework is being used to cover and acquire the step in the security requirement which is called the access control. Its main purpose is therefore giving permission or access to the authentic and real users to utilize the system facilities.

- **Cerberus & Kerberos:** Other frameworks like Cerberus & Kerberos are basically used for achieving the purpose of fulfilling and implementing various security requirements in the context-aware systems and applications such as identification, authentication and access control. Cerberus, however, is a framework for which the centre of attention concentrates on verification and validation of the identity of the user who is requesting access to services and facilities of context-aware systems. This validation and verification can be done by making use of information and data related with the user's context which includes fingerprint, voice and face recognition etc [24].

FRAMEWORKS	COMPATIBLE SECURITY REQUIREMENTS
Confab	Authentication
Uniform Access Control (UAC):	Access Control
General Role Based Access Control (GRBAC):	Access Control
Gaia	Authentication , Access Control
Cerberus	Authentication , Access Control, Privacy
Kerberos	Authentication , Access Control, Privacy

Table 1: Inter relationship between frameworks and security models

5. CONCLUSION

From the current study, we have come to understand the detailed concept of not only the context and context-aware systems them selves but also some constructive awareness regarding the privacy and security concerns along with the potential methods and requirements to be implemented. However, in order to overcome the privacy concerns mentioned by the users of context-aware systems, there are many essential security requirements raised by previous researchers recently which are required to be fulfilled and acquired for efficient and effective security. These are authentication, access control, privacy, availability and integrity of the data of relevant and authorized users of context-aware systems.

Many frameworks have been proposed and discussed for implementing and acquiring these security requirements on the user's context with the required level of efficiency and effectiveness. The most commonly used and preferred are Confab, Gaia, Cerberus, Kerberos, Uniform Access Control (UAC), General Role Based Access Control (GRBAC).Regarding a discussion about the most preferable and suitable one, we can make a conclusion that each of these have their own importance and therefore they are serving and providing assistance in fulfilling the security requirements individually in a much more efficient and effective manner. However, Kerberos along with Cerberos framework is highly preferable compared to the others as they concentrate on verification and validation of the identity of the user who is requesting access of services and facilities of context-aware systems. This validation and verification can be done by making use of information and data related with the user's context, which includes fingerprint, voice and face recognition, etc. Moreover, RBAC framework is a basic model which only covers and relates towards a subject-oriented approach whereas GRBAC allows defining an access control policy depending upon not only the subject but also on other essential and important factors like object or environment. Some further work needs to be done in order to overcome the core issues and challenges which faced by the context based security professionals and to come up with a more suitable and reliable framework. The issues and challenges are discussed briefly in the current study and there is still a need to give them serious thought in future potential research projects and high level studies linked with the implementation of Security and Privacy in Context Aware Systems.

REFERENCES

[1] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, P. Steggles, Towards a better understanding of context and context-awareness, in: HUC ’99: Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing, Springer-Verlag, London, UK, 1999, pp. 304–307

[2] B. Schilit, M. Theimer, Disseminating active map information to mobile hosts, IEEE Network 8 (5) (1994) 22–32. URL citeseer.ist.psu.edu/schilit94disseminating.html

[3] John, Meaney. Context. Amherst, NY: Pyr, 2005, pp.15-17.

[4] Dan Hong, Dickson K.W. Chiu. Vincent Y. Shen, Requirements Elicitation for the Design of Context-aware Applications in a Ubiquitous Environment, 2005.

[5] B. N. Schilit, N. Adams, and R. Want.Context-aware computing applications. In IEEE *Workshop on Mobile Computing Systems and Applications*, pages 85-90, Santa Cruz, CA, US, 1994. IEEE.

[6] G. Chen and D. Kotz.A survey of context-aware mobile computing research. Technical Report TR2000-381, Department of Computer Science, Dartmouth College, 2000.

[7] A. K. Det and G. D. Abowd, and D. Sabler. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications, *Human-Computer Interaction,* 16:97-166, 2001.

[8] R. Want, A. Hopper, V. Falcao, J. Gibbons, The active badge location system, Tech. Rep. 92.1, ORL, 24a Trumpington Street, Cambridge CB2 1QA (1992). URL citeseer.ist.psu.edu/want92active.html

[9] R. Want, B. Schilit, N. Adams, R. Gold, K. Petersen, J. Ellis, D. Goldberg,M. Weiser, The PARCTAB ubiquitous computing experiment, Tech. Rep. CSL- 95-1, Xerox Palo Alto Research Center (Mar. 1995).

[10] G. D. Abowd, C. G. Atkenson, J. Hong, S. Long, R. Kooper, and M. Pinkerton. Cyberguide: A mobile context-aware tour guide, *Wireless Networks,* 3(5):421-433, Oct. 1997.

[11] K. Cheverst, N. Davies, K. Mitchell, A. Friday, and C. Efstratiou.Developing a context-aware electronic tourist guide: Some issues and experiences. In *CHI 2000,* pages 17-24, The Hague, The Netherlands, April 2000. ACM Press.

[12] R. Fithian, G. Iachello, J. Moghazy, Z. Pousman, and J. Stasko.The design and evaluation of a mobile location aware handheld event planner. In *Mobile hci 2003,* pages 145-160, Udine, Italy, September 2003, Springer-Verlag.

[13] P. Klante, J. Krosche, and S. Boll.Accesssighs – a multimodal location-aware mobile tourist information system. In *International Conference on Computers Helping People with Special Needs (ICCHP)*2004, pages 187-294, Paris, France, 2004. Springer-Verlag.

[14] Chen and Kotz, “A survey of Context-aware Mobile computing research,” Dartmouth Computer Science Technical Report TR2000381.

[15] Y. Sumi, T. Etani, S. Felsyand, N. Simonetz, K. Kobayashix, and K. Mase.Cyberguide: A mobile context-aware tour guide. In *Community Computing and Support Systems*, pages 137-154, Kyoto, Japan, 1998. Springer-Verlag.

[16]B. Shneiderman and C. Plainsant. Designing the User Interface: Strategies for Effective Human-Computer Interaction, Addison-Wesley, San Francisco, USA. Fourth edition, 2005.

[17] Tariq Bashir Ahmad, Security and Privacy in Context-AwarComputing inside a Hospital, 2008.

[18] Douglas McIlwraith, Security and Privacy for Context AwareComputing, 2006.

[19] J. I. Hong and J. A. Landay, An architecture for privacy-sensitive ubiquitous computing, in MobiSYS ’04: Proceedings of the 2nd international conference on Mobile systems, applications, and services. ACM Press, 2004,pp. 177–189.

[20] N. Shankar and D. Bafanz, Enabling secure ad-hoc communication using context-aware security services, in UNBICOMP 02: Workshop on Security in Ubiquitous Computing, 2002. http://www.teco.edu/philip/ubicomp2002ws/organize/palo.pdf

[21] Z. Z. Michael J. Covington PrahladFogla and M. Ahamad, A context-aware security architecture for emerging applications, in Proceedings of the Annual Computer Security Applications Conference (ACSAC), Las Vegas Nevada USA, 2002.

[22] M. J. C. M. J. Moyer and M. Ahamad., Generalized role-based access control for securing future applications, 2000.

[23] M. R. C. K. H. R. C. A. R. R. H. Campbell and K. Nahrstedt, Gaia: A middleware infrastructure to enable active spaces, 2002. http://gaia.cs.uiuc.edu/papers/GaiaSubmitted3.pdf

[24] M. R. Bussard L., Roudier Y., Untraceable secret credentials: Trust establishment with privacy, in PERCOMMW'04. Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004.

[25] Aldabbas, H. Alwada'n, T. Janicke, H. andA.Al-Bayatti. Data Confidentiality in Mobile Ad hoc Networks, in International Journal of Wireless & Mobile Networks (IJWMN), Vol. 4, No. 1, February 2012.

[26] W. Li and A. Joshi. Security Issues in Mobile Ad Hoc Networks-A Survey. Department of Computer Science and Electrical Engineering, University of Maryland, 2008.

[27] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone.Handbook of applied cryptography.CRC, 1997.

[28] A. Toninelli, R. Montanari, L. Kagal and O. Lassila, "A semantic context-aware access control framework for secure collaborations in pervasive computing environments," The Semantic Web-ISWC 2006, pp. 473-486, 2006.

[29] K. Wrona and L. Gomez, "Context-aware security and secure context-awareness in ubiquitous computing environments," in f Polish Information Processing Society Conference Proceedings Conference, pp.255-265, 2005.

[30] M. Weiser. The Computer for the Twenty-First Century.Scientific American,265(3):94{104, 1991.

[31] Schilit, B.N., Theimer, M.M.: Disseminating active map information to mobile hosts. IEEE Network, 22–32, (1994).

[32] Choi, J. "Context-driven requirement analysis". In Proceeding of Computational Science and its Application [ICCSA 2007], Lecture Notes in Computer Science, vol. 4707, pp.739-748, 2007.

[33]Almuatiri, A. and Siewe, F. "CA-UCON: A context-aware usage control model". In Proceeding of the 5th ACM International Workshop on Context-Awareness for Self-Managing Systems [CASEMANS '11], pp. 38-34, 2011.

[34]Alkhaldi, W, Almutairi, S. Almutairi, A. Aldrawiesh, K.: Toward Development Context Aware Advertisement system (Case Study). In: IEEE, International Conference on Computer Applications and Network Security (ICCANS 2011). IEEE Press, CFP1182M-PRT/ISBN: 978-1-4244-9764-5. Maldives. (2011)

[35] M, Baldauf ,S.Dustdar and F.Rosenberg: A survey on context-aware systems. Int. J. Ad Hoc and Ubiquitous Computing, Vol. 2, No. 4, 2007.

[36] J. Bardram, R. E. Kjær, and M.ØPedersen, "Context-aware user authentication– Supporting proximity-based login in pervasive computing," in Proc. UBICOMP, 2003, pp. 107–123.

[37] Li Han; Jyri, S.; Jian Ma; Kuifei Yu; , "Research on Context-Aware Mobile Computing," *Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on*, pp.24-30, 25-28 March 2008 doi: 10.1109/WAINA.2008.115