International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(2): 75-81
The Society of Digital Information and Wireless Communications, 2012 (ISSN: 2305-0012)

Authenticating Devices in Ubiquitous Computing Environment

Kamarularifin Abd Jalil[1], Qatrunnada Binti Abdul Rahman[2]
Faculty of Computer and Mathematical Sciences
Universiti Teknologi MARA,
40450 Shah Alam,
Selangor, Malaysia.
kamarul@tmsk.uitm.edu.my[1], qatrunnada.abd.rahman@gmail.com[2]

***Abstract* – The deficient of a good authentication protocol in a ubiquitous application environment has made it a good target for adversaries. As a result, all the devices which are participating in such environment are said to be exposed to attacks such as identity impostor, man-in-the-middle attacks and also unauthorized attacks. Thus, this has created skeptical among the users and has resulted them of keeping their distance from such applications. For this reason, in this paper, we are proposing a new authentication protocol to be used in such environment. Unlike other authentication protocols which can be adopted to be used in such environment, our proposed protocol could avoid a single point of failures, implements trust level in granting access and also promotes decentralization. It is hoped that the proposed authentication protocol can reduce or eliminate the problems mentioned.**

Keywords: Authentication protocol, Ubiquitous Computing, application security, decentralize.

I. INTRODUCTION

Ubiquitous computing can be said as the latest paradigm in the world of computers today. It allows devices and systems to be integrated and embedded together with computing and communication systems through wireless transmission [1]. In a related work, Weiser [2] has defined ubiquitous computing as "a model of computing in which computation is everywhere and computer functions are being integrated into everything. It will be built into the basic objects (smart devices), environments and the activities of our everyday lives in such a way that no one will notice its presence".

In a ubiquitous system, information can be processed and delivered seamlessly among the participating devices without the users' even notice it. This is in contrast with what is being practiced in a non-ubiquitous computing environment whereby the users themselves have to make certain adjustments (to the devices) in order to suit the current computing environment they are in. These capabilities might sound a bit futuristic, but in reality, the technology is already here.

Basically, any device that can be connected to a network via a wired or wireless link can be included in a ubiquitous computing environment. However, nowadays, such devices are referring to the smart devices which are portable and connected to each other via wireless technologies such as the Bluetooth, Wi-Fi, 3G, 4G and etc. Some of these devices might be used to browse the Internet and some are partially autonomous and have the capability to sense their environment as discussed in [3]. With these capabilities, information dissemination is just at anyone's finger tips.

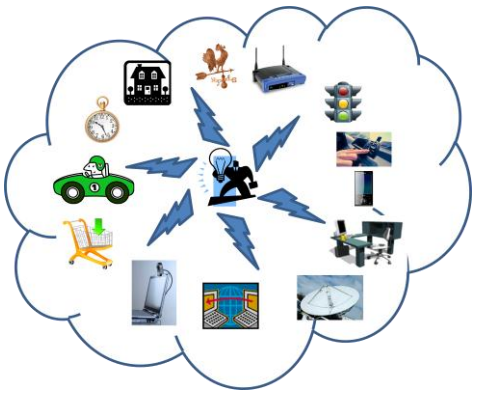


Figure 1.Ubiquitous Computing

Unfortunately, in this time and age, information can be easily misused or manipulated if not protected. The information that flows in the environment could fall into the wrong hands and could be manipulated maliciously. Such information can be said to be exposed to attacks such as unauthorized manipulation, illicit access, and also disruption of computing data and services. There have been many works to solve these problems, and using authentication protocol is one of them. Authentication protocol can ensure that users' information and privacy are safeguarded. In section III, some authentication protocols will be explained. These protocols can be seen as the potential candidates to be used in the ubiquitous computing applications. However, as mentioned in section III, it was found that all these candidates cannot satisfy

the needs of a ubiquitous computing application and that is why we are proposing a multi devices authentication protocol.

II. COMPUTER SECURITY COMPONENTS

Computer security as defined by NIST [4] is the defenses employed by information systems to maintain three elements and those are confidentiality, integrity and availability of its computing resources. The three elements mentioned in the definition are essentials to information systems security purposes as elaborated in [5] and often referred as the CIA triad. In order to fulfill these security objectives, information system developers and organization security managers are following security architecture for OSI which is featured in ITU-T Recommendation i.e. the X.800 [6], a standard for providing security. It emphasizes on Security Attack, Security Mechanism and Security Service. Our research is about utilizing some of these Security Mechanisms and Security Services to avert Security Attacks prominent in ubiquitous computing applications.

Security Service, according to X.800 [6], is a service offered by a layer of corresponding open systems that ensures sufficient protection of the systems or data transfers. There are five types of services, namely: Non-repudiation, Authentication, Data Integrity, Data Confidentiality and Access Control. Since this paper deals with authenticating devices in Ubiquitous computing environment, the focus will be more on Authentication service. Authentication is about making sure interacting entities are who they claimed to be. The X.800 standard has divided the Authentication service into two particular services, Data-origin authentication and Peer Entity authentication. The purpose of this paper is to provide Peer Entity authentication type of service which is to grant assurance and trust among interacting entities.

On the other hand, Security Mechanism is a method to avoid, detect or recover from security attacks. It is divided into two categories, Specific Security mechanisms, which may be deployed in any protocol layer or Security Services and Pervasive Security mechanisms, which are not particular to any protocol layer or Security Services. Moreover, there are many different types of Security Mechanisms and further elaboration on these can be seen in [6]. For this paper, only three mechanisms will be utilized in the development of the new authentication protocol. Those three Security Mechanisms which falls under Specific Security mechanism category are; Authentication Exchange, Digital Signature, and Encipherment. The purpose of Authentication Exchange is to identify an entity through the exchange of information meanwhile Digital Signature will provide integrity to the information so that its origin will not be doubted whereas Encipherment will alter the information, making it unreadable during transmission of the information.

In order to create the new authentication protocol, basic missions in a security service need to be established, indeed, Stallings [7] has identified four significant missions that can fit into any security services. The first one is an algorithm needs to be created for security purposes. The second one is generation of secret information to be utilized with the algorithm and this secret needs to be conveyed, so, the third mission is to create a process to satisfy that purpose. The last mission is to identify a protocol in order to utilize the secret information and the algorithm to fulfill certain security service. Figure 2 is a depiction of a basic form of network security for two or more interacting entities that can be fitted by security services and security mechanisms discussed earlier in order to secure particular network services.

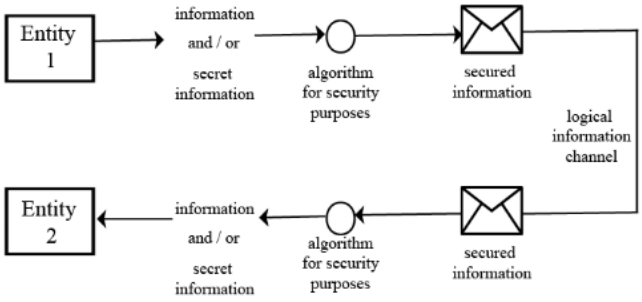


Figure 2.Basic form of network security
Source: [7]

All in all, based on the discussion earlier we know that there are many security services which implement certain security mechanisms in order to prevent security attacks, and among all the security services mentioned, this paper only concentrates on designing a new authentication protocol which can be categorized as Peer Entity Authentication security service. The proposed protocol will utilize the Authentication Exchange, Digital Signature, and Encipherment security mechanism. Furthermore, figure 2 is also the basic form for the new authentication protocol design, but it will be altered to achieve the objective of assurance in the identity of communicating entities. More information about the proposed protocol can be found in section V of this paper.

III. AUTHENTICATION PROTOCOLS

Authentication is important in order to maintain the integrity of an entity. On the other hand, integrity is essential in determining that an entity is really who it claims to be. Moreover, authentication can be used to ensure that an entity has full authority and accountability over its data. Therefore, in maintaining an entity's integrity, many authentication protocols have been introduced. Protocols such as Kerberos, SSO and OpenID are some of the examples that are widely used. Most of these authentication protocols required a dedicated access to a server for either validation process or to acquire digital certificates, tickets or tokens. On the other hand, users who utilize OpenID needs to register to an OpenID

identifier with an identity provider in order to sign in to the websites which employ the OpenID authentication.

Some of these authentication protocols are not suitable for ubiquitous computing environment. For example, Kerberos, which is a computer network authentication protocol that consists of a centralized Key distribution Centre (KDC) which actually is two logically separate parts comprises of Authentication Server and Ticket Granting Server as mentioned in [8]. Although centralization is good in managing multiple users at one time, but it still has a disadvantage because if the KDC server is compromised or the service is down, users may not be able to authenticate themselves. Accordingly, KDC can be the single-point-of-failure which is the major drawback for Kerberos protocol as argued in [9].

Another current authentication protocol which is widely used is the Single sign-on (SSO). According to [10], it enables a user to gain access to several systems or applications by a single login. A user does not have to reiterate the login process to every application that he or she is trying to access. This means that, SSO is a centralized authentication system that has access control to multiple applications that are unified under it. In SSO, once the user logged in, he or she can access other applications too. This makes the authentication system to be highly vital. If the authentication system availability is disrupted then the users can face the denial of access to the other applications that employed the SSO authentication system. This is a major drawback of the SSO authentication system as shown in [11].

Nonetheless, there is still authentication protocol which implements decentralized system. OpenID enables users to choose their preferable identity providers in order to create accounts. The users are able to sign in to any application that acknowledges the authentication by using those accounts. Nevertheless, that is also the downside of it. As OpenID account can only be used to sign in to websites that acknowledges it. Although OpenId is already widely being implemented there are more websites which do not, so relying on it for integrity conformation is not convenient. Moreover, it is also susceptible to phishing attacks. The phishing attack can be in such a way that a user account can be tampered with when a user is swindled into believing that he or she is filling credentials into the real identity provider authentication page whereas it is actually a fake authentication page. Upon giving his or her credentials into this fake site, the malicious person that is controlling it can use those credentials to access the user's account and then log into any application that associate with that particular user's OpenID as mentioned in [12].

Recently, there is a different approached in authentication, which specialized in securing communications between devices by using the knowledge of their radio environment as a proof of physical proximity. This new authentication protocol is called Amigo. According to Varshavsky et al. in [13], Amigo is a technique which extends the Diffie-Hellman key exchange with verification of device co-location. This protocol can ensure that the key is exchanged with the right device. In doing this, a device's location or specifically its radio environment will be verified whether it is in the same proximity or not. This technique is interesting as it involves comparing the proximity of the devices. The only downside of this technique is that the interacting devices would only know the proximity of one another and not their exact identities. This is not enough if a user wants to execute trust in communications.

Based on the related authentication protocols features mentioned above, there are many attributes that need to be improved in order to suit the ubiquitous computing volatile and decentralized environment.

IV. JUSTIFICATIONS AND REQUIREMENTS FOR THE PROPOSED PROTOCOL

In Section III, we have presented the current protocols that can be used in the ubiquitous computing applications. From the discussions, it can be deduced that there are three issues with these protocols that need to be addressed by the proposed protocol. The first one is the issue of centralization. The second one is the issue of accessibility (need Internet in order to use the protocol). The third and the last one is the issue of trust.

According to Colouris [14], due to its volatile environment as compared to the existing computing environment, ubiquitous computing needs a special authentication and authorization protocol. In a volatile environment, heterogeneous devices may come in contact with each other spontaneously and could start interacting with each other and also may suddenly leave from the established network connections [15]. The volatility and dynamicity of mobile devices in a ubiquitous computing environment could contribute to the fluctuating usage environment such as user's location, device's context and user's activity that varies randomly. As a result, the current rigid and centralized authentication protocol that relied on certification authorities in order to confirm the identity of the entity involved will not be sufficient for a volatile environment such as smart environment as demonstrated by Nixon [16]. In this paper, we have identified three requirements for the proposed authentication protocol (see Figure 3). These requirements are seen as vital in order for the proposed protocol to be accepted by the users.

A. Decentralization

The decentralization of an authentication protocol is actually referring to the distribution of the authentication process to the respective devices. This is opposite to the

current practice which provides a centralized authentication protocol that relied on hierarchies of certification authorities that provide certificates and confirmations of the respective owners using a dedicated server. The decentralization of the authentication process in the proposed protocol is achieved through multiple trusted agreements among the devices involved.

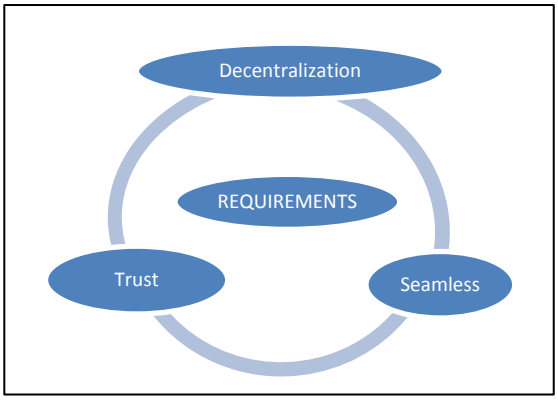


Figure 3.Requirements for the New Authentication Protocol

The act of using multiple trusted devices to verify the identity of an entity will eliminate the need for constant access to an online dedicated server for authentication process. This would be useful in the case of interruption in the network access whereby the respective devices cannot get access to the Internet. In the proposed protocol, the only network connection needed in order for the authentication process to take place is the connection between the communicating devices. As pointed out in [17], processors are now being embedded into common everyday objects and surrounding infrastructures, for that reason it is not efficient to provide an authentication process that requires constant online access to a dedicated server and certificate authority. Besides that, there are many questions regarding public key infrastructure practicality as mentioned by Creese et al. in [18], who questioned the Certification Authority practicality which needs constant online access.

Decentralization of authentication process can also eliminate the single-point-of-failure problem. A centralized authentication protocol does have high chances of having a single-point-of –failure due to high dependency in dedicated servers for validation processes. If this single-point-of-failure risk can be minimized or can be avoided, then the usability and availability of an authentication system can be improved.

B. Trust

Trust can be said as the second requirements for the new authentication protocol. Coulouris et al. in [14], has stated that the devices' trust needs to be lowered in order to spontaneously interact. When this situation happens, they will be short of of knowledge of each other and a trusted third party will be needed to ensure the identity of one another. In addition, Varshavsky et al. in [13] had mentioned about mobile devices that have wireless capabilities may spontaneously interact with one another whenever they come in close proximity, so this sort of communications are risky as the trust among them are not priory established. Eventually, this lack of trust may give opportunity to malicious attacker to be connected with any devices in presence. Hence, an approach to solve this problem is proposed by adopting a trust level mechanism where user can choose to set their devices' trust level accordingly for authentication process.

In a normal scenario of ubiquitous computing environment, some users may already know each other beforehand and some may not. So each user may want to set different trust level for different situation or people. As, suggested by Westin in [19], there are three types of respondents, namely; privacy fundamentalists, privacy pragmatists, and privacy unconcerned. Based on that argument, users should be given a choice to choose their privacy settings.

C. Seamless

The third requirement for the new authentication protocol can be said as making the interaction in the authentication process to be seamless to the users. This is because; one of ubiquitous computing characteristics as emphasized by Weiser [2] is that the technology should blend into the surroundings to the extent that the people are not aware of it and do not need to know how it is done. This concurs with Stringer et al [20] and also Bardram and Friday [15], who acknowledged that ubiquitous computing is about disappearing computing application which blends into objects and surroundings. As, stated by Langheinrich [21] processors and sensors are being embedded into almost everything.

Because of that, the form of interaction of ubiquitous applications and devices are beyond the traditional computing interaction where it is done via sensors that sense an entity presence, sound or gesture implicitly. Consequently, it is appropriate to design an authentication protocol that suits to this characteristic of ubiquitous computing, which involve authenticating entities without having the entity to interfere in the process and is unobtrusive.

V. THE PROPOSED AUTHENTICATION PROTOCOL

Since the current authentication protocols are more suitable being implemented by the rigid computing infrastructure which is centralized and required constant access to a dedicated server, the new design for the proposed authentication protocol will be developed to be suitable with the volatile environment of ubiquitous computing. Figure 4 will explain more about the multiple trusted devices authentication protocol for Ubiquitous Computing application.

In order to understand the proposed authentication protocol, a scenario is used.

In the scenario, there are 3 persons A (P_A), B (P_B) and C (P_C) who each has a smart phone device A (D_A), B (D_B) and C (D_C). P_A and P_B had just met but P_C is a mutual friend of P_A and P_B. P_B has a collection of interesting pictures that he had taken while visiting an art gallery in Paris. P_A on the other hand, really wants to have those pictures so he decided to copy it from P_B. P_B do not mind to share it with P_A, and all P_A has to do is to access P_B's device. In order to do so, he must have the authority to access device D_B. As P_A and P_B have just met, therefore, P_A must first register with device D_B. Whereas, since P_C is a mutual friend to both P_A and P_B, therefore, it is assumed that he has already registered to both of his friends' devices. Therefore, he will not have a problem in accessing both of his friends' devices. Hence, Figure 4 depicts how device D_A will be granted the access to device D_B.

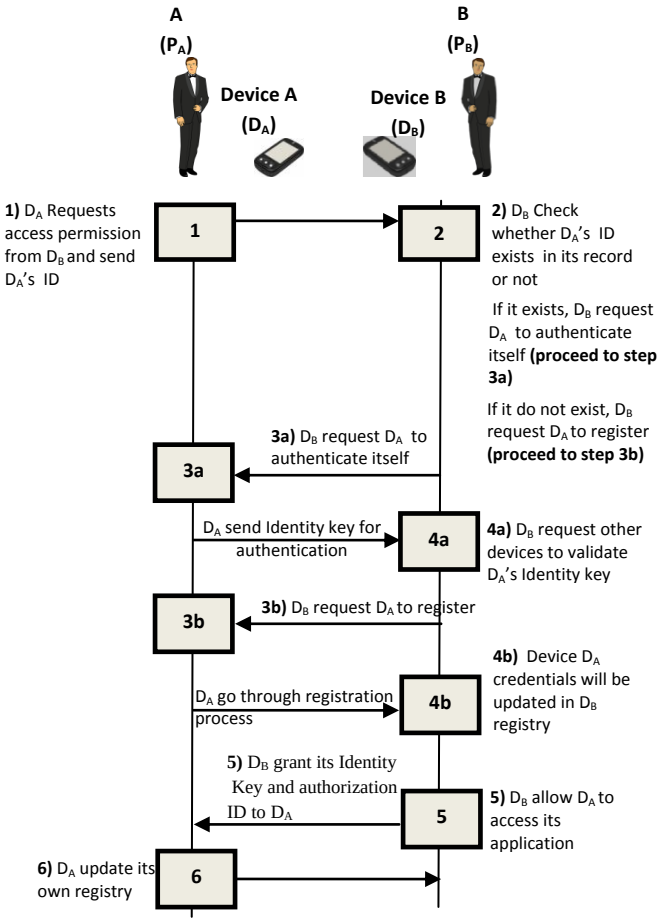


Figure 4. The proposed authentication protocol

First of all, in step 1 device D_A must request permission to access device D_B. In doing so, D_A must show or send its ID to D_B so that D_B is able to check in its registry whether D_A is already in it or not. This ID is actually a random value that D_A can generate and renew whenever it is needed. This ID is not permanent; nevertheless each time it is being renewed, the old ID which is in the other devices registry will become invalid. As a result, a device must go through the registration process each time the ID is being renewed.

In step 2, D_B will check (by using D_A's ID just now) whether it has D_A's ID recorded in its registry or not. This action will result in two conditions either D_A's ID is found or not found. So, if it is found, it will proceed to step 3a if not it will proceed to step 3b. Then, in step 3a, when it is confirmed that D_A has already registered in the registry, D_B will proceed to request D_A to authenticate itself by giving its Identity Key. This Identity key is also a sequence of random value and also can be generated and renew whenever it is needed. Apart from that, this Identity key will be conveyed partially, see figure 5. Hence, only a portion of the whole Identity key and its metadata of Identity key sequence will be sent. This is to avoid malicious device that might be eavesdropping. Although the Identity Key will be partially revealed, D_B will not have any problem to verify it as it will compare the sequence of D_A Identity Key being sent with the one that is already in its registry. Furthermore, in step 4a, D_B will also seek other device to participate in validating the Identity Key. Nonetheless, all information during these transmissions will be encrypted using the existing cryptographic algorithm.

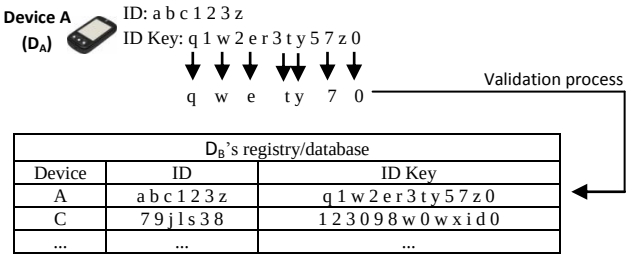
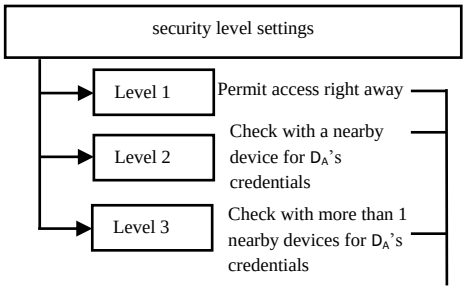


Figure 5. Identity Key

During step 4a, apart from finding D_A's ID Key in the registry and then validates it, there will also be security level settings depicted in figure 6 that D_B has to set for D_A. This security level setting will determine how the validation process will take place (in this phase, P_B is free to set different security level for different device that P_B encounters). There are currently three levels of security settings in this protocol. If D_A is set to Level 1 then, after D_B has validate its Identity Key it can access D_B right away. But if it is set to level 2, then after D_B has validate its Identity Key, D_B will proceed to ask other device which may be nearby to check for D_A's credentials. However, if D_A is set to Level 3, then its credentials will be validated by more than 1 nearby devices.



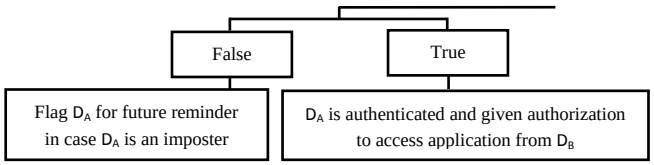


Figure 6. Security level settings

Nevertheless, steps 3a and 4a deal with a situation where D_A has already registered in D_B's registry. If it is not then it will continue to step 3b, where it is prompt to register first in order to access D_B's application. Here, D_A will go through the registration process where it will provide its ID as well as its Identity Key. After that, in step 4b, D_A's credentials will be updated inside D_B's registry. Next, after step 3a and 4a or 3b and 4b have been completed, step 5 will take place, where D_B is ready to give permission and authorization for D_A to access its application. D_B will also grant its Identity Key and its authorization ID to D_A.

Finally, in step 6, after D_A has accepted D_B's ID Key and authorization ID, it will update them in its database/registry. Then it will proceed to use the authorization ID to access the desired application on device D_B.

VI. CONCLUSIONS

In this paper, we have discussed a number of possible authentication protocols to be used in the ubiquitous application environment. From the discussion, we have shown that there is no protocol that can really suit the needs of the application running in such environment. Therefore, in this paper, we are proposing a new authentication protocol which can satisfy the needs of the applications running in a ubiquitous environment. The proposed protocol uses multiple trusted devices and this has resulted in the decentralization of the authentication process in order to suit the volatile and dynamic environment of Ubiquitous Computing. It is hope that in the near future, the proposed protocol can be tested in a test bed environment.

REFERENCES

1. R. Want, "An introduction to ubiquitous computing, Ubiquitous Computing Fundamentals," J. Krumm, Ed. Redmond,Washington, U.S.A:CRC Press, ch.1, pp. 2-27.
2. M. Weiser, "The computer for the 21st century, Mobile Computing and Communications Review," New York, NY, USA, pp. 3(3):3–11, (1999).
3. S. Yahya, E. A. Ahmad, K. Abd Jalil, "The definition and characteristics of ubiquitous learning: A discussion," International Journal of Education and Development using Information and Communication Technology, pp. 117-127, (2010).
4. B. Guttman and E. A. Roback, "Introduction, An Introduction to Computer Security: The NIST Handbook," Gaithersburg, MD: NIST special Publication 800-12, ch.1, pp.5, (1995).
5. Standards for Security Categorization of Federal Information and Information Systems, Federal Information processing Standards Publication. Gaithersburg, MD, p. 2, (2004).
6. Security Architecture for Open Systems Interconnection for CCITT Applications, Recommendation X.800. Geneva, p.8-9, (1991).
7. W. Stallings, "A Model for Network Security, Cryptography and Network Security 5th ed." Prentice Hall, Upper Saddle River, NY: ch. 1, pp. 25-26, (2011).
8. J. Garman, "Pieces of the puzzle, Kerberos the definitive guide," Sebastopol, CA: O'Reilly & Associates, Inc, ch. 2, pp. 17-23, (2010).
9. J. Garman, "Security, Kerberos the definitive guide," Sebastopol, CA: O'Reilly & Associates, Inc, ch. 6, pp. 100-125, (2010).
10. B. Ballad, T. Ballad, E. K. Banks, "Single Sign-on (SSO), access control, authentication, and public key infrastructure," Sudbury, MA : Jones & Bartlett Learnings, ch. 10, pp. 229-231, (2011).
11. J. Pyles, "Getting started with Microsoft Office SharePoint Server, McTs," Microsoft Office Sharepoint Server 2007 Configuration Study Guide. Indianapolis, Indiana: Wiley Publishing, Inc., ch. 1, pp. 14, (2008).
12. R. U. Rehman, "OpenID Protocol: Miscellaneous Topics, Get Ready for OpenID," 1st ed. Conformix Technologies Inc., ch. 8, pp. 205-207, (2008).
13. A. Varshavsky, A. Scannell, A. E. Lara LaMarca, "Amigo: Proximity-based Authentication of Mobile Devices," Proc. 2007: The 9th international conference on Ubiquitous computing, Berlin, Heidelberg, pp. 253-270, (2007).
14. G. Coulouris, "Mobile and Ubiquitous Computing, distributed systems," Concepts and Design. 4th ed., Addison-Wesley, Reading, MA : Addison-Wesley, ch. 16, pp. 683-704, (2005).
15. J. Bardram, A. Friday, "Ubiquitous Computing Systems, Ubiquitous Computing Fundamentals," J. Krumm, Ed. Redmond, Washington, U.S.A: CRC Press, ch. 2, pp. 39-41, (2010).
16. P. Nixon, W. Wagealla, C. English, and S. Terzis, "Privacy, Security, and Trust Issues in Smart Environments," In Smart Environments: Technology, Protocols and Applications. Wiley, London, UK, pp. 220-240. ISBN 978-0-471-54448-7, (2004).
17. Middleware Architecture for Ambient Intelligence in the Networked Home, Handbook of Ambient Intelligence and Smart Environments. Springer-Verlag US, p. 1139, (2010).
18. S. Creese, M. Goldsmith, B. Roscoe, I. Zakiuddin, "Authentication for Pervasive Computing. Security in pervasive computing," First International Conference, Boppard, Germany, pp. 117-129, (2003).

19. A. F. Westin, "Privacy and Freedom", New York, NY, USA: Atheneum, (1967).
20. M. Stringer, et al "Situating Ubiquitous Computing in Everyday Life: Some Useful Strategies" [Online]. Available: http://www.informatics.sussex.ac.uk/ research/groups/interact/publications/stringer_ubicomp05.pdf.
21. M. Langheinrich, "Privacy by Design - Principles of Privacy- Aware Ubiquitous Systems," Proc of the 3rd international conference on Ubiquitous Computing, London, UK, (2001).