A XML based, User-centered Privacy Model in Pervasive Computing Systems

Ali Dehghantanha, Ramlan Mahmod, and Nur Izura Udzir

Faculty of Computer Science & Information Technology, University of Putra, Malaysia

Summary
The fact that pervasive systems are typically embedded and invisible makes it difficult for users to know when, where, and how these devices are collecting data. So privacy is a major issue for pervasive computing applications and several privacy models have been proposed for pervasive environments. In this paper we present a XML based User-centered Privacy Model (UPM) which provides content, identity, location, and time privacy with low unobtrusiveness.

Key words:
privacy, pervasive computing, identity privacy, location privacy, time privacy

1. INTRODUCTION

Mark Weiser [1] for the first time described environments where devices weave themselves into a user's daily life and enable users to work in any environment, anytime, anywhere. He called this environment "Ubiquitous Computing" or "Pervasive Computing" environment.
Several research projects have attempted to achieve this idea. Aura project [2] was a wireless umbrella that pervasively connects different devices in Carnegie Mellon University campus. Oxygen project [3] aims to build a pervasive environment that devices weave themselves as ubiquitously as oxygen in users life. The Gaia project [4] was an effort to build a middle-ware for traditional devices to work and join to the pervasive environments. Microsoft Easy Living project [5] brings intelligent, computational devices to people's daily life.
The most noticeable characteristics of pervasive environments are [6], [7]:

- Ubiquity: Environmental services are everywhere for every user.
- Invisibility: Services invisibly weave themselves to the environment.
- Sensing: The invisible and ubiquitous devices can sense and detect environmental information.
- Inter connection and co-operation between devices: The sensitive, invisible, and ubiquitous devices cooperate and connect to each other for providing pervasive services.
- Memory amplification: The cooperative, sensitive, invisible, and ubiquitous devices increase environmental storage ability and amplify memory.

Manuscript received October 5, 2009
Manuscript revised October 20, 2009

On the other hand there are privacy principles based on the well known Fair Information Practices (FIP) [8] as listed below [9]:

- Notice*:* Users always should be aware of gathering of their personal data.
- Choice and Consent*:* Users should always have a choice to disclose their personal data or not.
- Proximity and Locality*:* Gathering of data should always happen in an environment that the user is present (proximity) and the processing of the data should be in the space where the data has been gathered (locality).
- Anonymity and Pseudonymity*:* Whenever the user identity is not required or the user did not consent, pseudonymity or anonymity mechanisms should be used.
- Access to Resources: Access to the user resources should only be allowed to authorized parties.

Comparing privacy principles and pervasive computing characteristics make it clear that pervasive environment characteristics are in direct conflict with privacy principles. The most profound privacy risks in pervasive systems are [10]:

- Pervasive devices exist everywhere, and with the enhancements in their saving capacities and little size, they can invisibly gather a lot of user private information.
- The communication between pervasive devices should be held by their own so they might reveal user private information in communication with each other.
- In most countries privacy regulations are in their very early stages and clarify the need for privacy models in pervasive environments to protect user.

Different privacy models have been proposed in pervasive computing. Earlier models' focus was on providing different privacy types (content, identity, location, and time privacy) for the user. The "Privacy Mirror Model" [11] supported time and content privacy, the "Identity Management Model" [12] supported identity privacy, the "Mist Protocol" [13] supported location privacy, the "Unified Privacy Tagging" [14] supported content privacy, and the "Mix Zones" [15] model supported location privacy.

The fast growth of privacy models necessitates standard factors and mechanisms for evaluating these models. Several evaluation factors have been proposed by [16] ,[17], [18] for privacy evaluation in pervasive environments, which can be ranked into four major categories as follows:

- Expressiveness of privacy policies: Measures with a number between 0-4, which represents the number of sub-factors has been supported. These sub-factors are support for mandatory and discretionary rules, context sensitivity, uncertainty handling, and conflict resolution.
- User Control over private information: Measures with a number between 0-4, representing the number of sub-factors have been supported. These sub-factors are content privacy, identity privacy, location privacy, and time privacy.
- Unobtrusiveness of privacy mechanisms: The percent of time that user interacts with privacy sub-system, base on the percentage will categorize in different groups.
- Model scalability: Measures with a number between 0-2 representing the number of sub-factors have been supported. These sub-factors are platform independency, and distributed decision making processes.

The recent privacy models like Loc Serve [19], Context Model for Privacy [20], PSIUM and Anonymity Enhancer [21], Tachyon [22], IDRSC [23], and Loom Model [24] support all four types of private information (content, identity, location, and time). These models try to increase the expressiveness of privacy policies by providing support for mandatory and discretionary rules, reflect context sensitive information, handle uncertain situations and resolve conflict situations. These models attempt to increase their scalability by providing a common communication platform and distributing decision making processes. Finally these models decrease the unobtrusiveness of their privacy mechanisms (the percentage of time that user wastes on dealing with privacy sub-system).

As we described, none of the previous models could support all four characteristics of “expressiveness of privacy policies”, all four types of content, identity, location, and time privacy, and the two characteristics of scalability (platform independency, no centralized decision making point) with less than 10% of unobtrusiveness.

In this paper we propose a privacy model with the following characteristics:

1. The privacy policies should be expressive to support mandatory and discretionary rules, context sensitivity, uncertainty handling, and conflict resolution.
2. User control over private information should be at a level that provides user with content, identity, location, and time privacy.
3. The model should be highly scalable. It has to provide platform independence, and it should be a distributed model without any centralized decision making point.
4. With all the above characteristics the percent of time a user deals with privacy sub-system (the model's unobtrusiveness) should be less than 10%.

We continue by describing the proposed model in section 2 and finally conclude the paper in section 3.

2. Proposed Model

This section describes the proposed model parties and layers, model privacy files, model phases, and model encryption/decryption process.

2.1 The Model Parties and Layers

Five parties are communicating in our model as follows:

- User: User requests for services of a service provider.
- Service provider: Service provider provides services for the user and might use the data that is provided by the owner.
- Owner: Owner is the content provider.
- User light houses: Each user has one or more light houses. Light houses are user trusted parties that have user identity information but they never have any information of the user location, content, and time. Light houses provide other parties with user identity information based on a defined user identity privacy policy.
- Portals: portals are wireless nodes managing the user context. Each context consists of one portal which plays two roles:
    1. All devices of the context (including the users’ devices) sending and receiving data through the portal.
    2. A portal manages all devices that gather user private information in the context. By default a portal has access just to user location information but it does not have any access to user identity, content, and time information.

The model consists of three layers as follows:

- User context layer: This layer surrounds user. Context contains one portal and several devices which are capable of gathering user private data. These devices are managed and controlled by the portal. In a specific time, a user can be just within one portal covered environment but a user might move between several portals, hence experiencing different contexts.
- Service layer: User light houses and service providers are in this layer.
- Owner layer: Information owners are in this layer. This layer provides the required content for the service providers.

In the proposed model, a user sends data to the portal without sending any information of his identity. Then the portal hides user location and forwards data to the light house. By doing so the user portal only knows the user location and the user light house only knows his identity. The user light house is responsible for communicating with the service provider. The service provider receives the needed contents from the owners.

2.2 Model Privacy Files

The model privacy management method is based on XML files used for describing privacy policies and preferences. User, portal, and service provider have two XML privacy files namely privacy policy file and privacy preferences file as follows:

- The user privacy preference file identifies user preferred ID and location privacy level to join to the context as well as user preferred ID, location, and time privacy to use each service.
- The portal privacy preferences file identifies the context required ID, and location privacy to allow users join that context.
- The service provider privacy preferences file identifies the required level of ID, location, and time privacy that user should provide in order to use each service of that service provider.
- The owner privacy preferences file identifies the required location and time privacy level to provide content for the user and service provider. The owner just has a privacy preferences file that describes the content privacy because all parties should follow the owner content privacy during communication and no dealing can be made so the owner does not need to have a privacy policy file

The format and tags of both privacy preferences and privacy policy files for each party are similar but the privacy preferences file describes preferred level of privacy to communicate with other parties while privacy policy file describes each party's current privacy level during communication with other parties.

The identity privacy tag value can be as follows:

- Transparent ID: the party provides or asks the real identity in communication with other parties.
- Protected ID: the party does not provide or ask the real identity but it uses a pseudonym ID whose trustability and access level has been confirmed by a common trusted third party.
- Private ID: the party uses or asks an anonymous ID in communicating with other parties.

The location privacy tag value can be as follow:

- Transparent Loc: The party provides or asks the exact location information of other communicating parties.
- Protected Loc: The party confirms its existence in a certain area through a common trusted third party or asks the other parties to confirm their existence in a certain area.
- Private Loc: The party does not reveal or ask any information about the location information in communication.

The time privacy tag value can be as follow:

- Transparent Time: The parties provide the real time information in communicating with each other.
- Protected Time: The parties confirm their time information through a trusted third party.
- Private Time: The parties do not reveal or ask information about each other time information in communication.

The content privacy policies are specified by the owner and consist of time and location privacy of each content part. The content privacy is provided in all inter-party communications with encryption methods.

The portal privacy policy just has ID and location privacy because in portal and user relationship there is no long term data transformation and portal services are real time and they are available only during the time that user is under their controlled environment so there is no need for a time privacy policy control mechanism. In the owner privacy preferences we have time and location privacy for each service because the owner can just specify the content privacy policy, and contents provided for the users through service providers so the identity privacy management is on the service provider side and the owner just specifies the required privacy for the content saving locations and the content availability time.

2.3 The Model Phases

The proposed model contains five phases as follows:

1. Authentication phase
2. Context joining phase
3. Service registration phase
4. Service usage phase
5. Saving data and finish phase

These phases provide privacy since the user authenticates until finishing the usage of the service and saves data. We describe each phase in the following sections.

2.3.1 Authentication Phase

In this phase user authenticates to his mobile device through one of the authentication mechanisms.

There are various authentication mechanisms from simple user name and password checking to biometric authentication methods. We relate a number in [0,100] called Authentication Precision Level (APL) to each authentication mechanism that shows the precision level of that authentication mechanism. More precise authentication methods have higher APLs. For example the APL for username and password checking

authentication method can be 30 and APL for fingerprint detection method can be 50. These authentication levels can be set by user or through default profiles by device producers.

The proposed model automation level depends on the user's APL. The APL is divided into three levels as follow:

- 0<= APL <= 25
- 25 < APL <= 75
- 75 < APL <= 100

These ranges cover all possible authentication scenarios (from 0 to 100 percent precision) while they reflect all three different situations that a user might encounters as follow

- Accept all privacy contradictions: When the APL is less than 25 in any conflicts or uncertain privacy situations between a user and other parties that the other party cannot provide the user required privacy level, the system automatically accepts and applies the highest provided privacy level by the other party.
- Make user consultation on each privacy contradiction: When the APL from 25 to 75 means the user receives alarms on joining the parties with lower privacy levels and may accept or deny any offer to join them, so we have user notice and choice in this level.
- Reject all privacy contradictions: With APL more than 75, the system does not accept any privacy level less than the user required privacy so if the other party could not provide the user required privacy level the system does not allow the user to use the other party's services.

With this division we confine the privacy alarms only to the authentication methods with APL levels from 25 to 75. APL is written and saves in <APL> tag of the user privacy policy file for later comparisons and decision making during the other phases.

Our model enhances previous model authentications by dividing the system based on APL into three divisions, each of which has a different automation level to decrease the system unobtrusiveness.

2.3.2 Context Joining Phase

After authenticating to the mobile device, user joins to the context. There are different devices that gather user private information in the context. In this phase user and portal make agreement on the context privacy level. Each portal contains four XML privacy files as follows:

- Device privacy preferences file: describes the level of private information that the device captures. The device privacy preferences file includes ID preference <IDPref> that identifies the level of private identity information captured by that device, location preferences <LocPref> that identifies the level of private location information captured by that device, and time preferences <TimePref> that specifies the time privacy level captured by that device.
- Device privacy policy file: contains the same information as the device privacy preference file but it shows the privacy level of each device while it is working in the environment.
- Context privacy preferences file: results from the context devices privacy preferences files and shows the context privacy level that portal prefers to provide for the users.
- Context privacy policy file: shows the current level of context privacy which resulted from the current context devices privacy policy file. For example if a user requires Private ID privacy level for its identity and context consists of a camera that reveals the user identity, if portal would be able to turn off the camera during the time that the user is inside the context, then the portal changes the camera tag of the device privacy policy file to Private ID and also changes the portal privacy policy identity tag to Private ID and sends a confirmation message to the user. Otherwise it sends privacy contradictions to the user.

If a user could join the context, the agreed context privacy policy level for ID and location would be written in <ContextPrivacyPolicy> tag of the user privacy policy file and <ContextPrivacyPolicy> tag of the context privacy policy file.

A transparent ID value for identity tag means the user's real identity might be revealed in this context, Protected ID means context at most reveal user existence among some other users in the context, and Private ID means the context does not reveal user identity. The context location tag can be as follows:

- Transparent Loc: which means the context might reveal the exact location of the user.
- Protected Loc: which means the context reveals the location of the user in an area.
- Private Loc: which means the context will not reveal any location information of the user.

So in this phase:

- The proposed model divides context privacy to location and identity and considers the effect of both on user privacy.
- The model used XML tags for describing context private information which allow the portal and context devices to interact without any platform dependencies. Platform independency increases the variety of devices that can be used in the context environment and makes adding new devices easier.

2.3.3 Service Registration Phase

If a user could join the context, then in this phase the user registers on the service provider and chooses a service to use.

Four files are involved in this phase, namely the user privacy preferences file, user privacy policy file, service provider privacy preferences file, and service provider privacy policy file.
All the above files have service registration privacy policy/preferences tag for each of their services which define identity, location, and time privacy.
The identity tag may have Transparent ID, Protected ID, or Private ID values.
Transparent ID means the user has to register with the service provider with his real identity so the user's real identity should be sent to service provider by user light house during service registration. There should be enough trust level between the user light house and the service provider to convince the service provider that the identity provided by the user light house is the user's real identity.
Protected ID means the service provider does not need real identity of the user but the user identity should be confirmed by a third trusted party between user light house and service provider light house. Private ID means the service provider will generate a random identity to be used by the user.
The location tag can have Private Loc, Protected Loc, and Transparent Loc values. Transparent Loc value means the service provider needs the user's exact physical location to register the user. The exact location confirmation key is used for controlling user exact physical location. The encrypting algorithm encrypts data based on the user provided location information on the service provider side, whereas the decryption algorithm decrypts the data on the portal side by giving current user location information to decryption algorithms, then the portal sends the data to the user. We use the algorithm proposed by [25] for encrypting and decrypting data.
Protected Loc means the service provider light house does not need a user's real location information; instead the user should be under an environment controlled by a trusted portal to use the service. The system protects user location through a symmetric key called the location confirmation key. The service provider has the encryption key and the trusted portals have the corresponding decryption key. When the service provider sends information with protected location policy it encrypts all information and at the entrance of the portal, the portal decrypts the information and forwards it to the user so that only users under the trusted portals covered environment get access to the information.
Private Loc means the user location is not required for registering user on the service provider and the portal fully hides user location from the service provider.
The time tag can have transparent time, protected time, or private time values. Private time means the service provider generated username is valid just for one time using of one of the services on the service provider, which expires after the user disconnects from service provider or finishes using the service. Protected time means the user light house and service provider light house should make an agreement on a certain amount of time that registered username is valid on the service provider for that service, whereas transparent time means the registered username is valid for unlimited time.
As the basic rule in the proposed model the user light house always tries to provide highest possible privacy for the user.
The agreed privacy policy would be written in service registration privacy policy tags <ServiceRegistrationPrivacyPolicy> of user privacy policy and service provider privacy policy files. So in this phase:

- The proposed model increases the end user's ease of movement and model scalability by sending a username and key to the user that can be used under different portals without any need of communication with a centralized server.
- By using XML our model provides a common communication platform to accommodate different devices.

2.3.4 Service Usage Phase

In the previous phase user registered for a service on the service provider. In this phase the user starts using the service and gets access to the service content.
Three files are involved in this phase namely user privacy policy file, service provider privacy policy file, and owner privacy preferences file. There is a service content privacy tag which consists of several "Information Space" tags in all previous files for each service in each service provider. Each information space relates to a content part and identifies location and time privacy policy of the related content.
Location privacy policy can be one of transparent location, protected location, or private location. Transparent location value means the content is available for the user just during the time that user real location can be tested by the service provider. Protected location means the content is available for the user only if the user location can be confirmed by the service provider, and private location means the content would be available for the user regardless of the user location.
Time privacy policy can have one of three values namely private time, protected time, or transparent time. Private time policy means the content is available just during the time that user using the service and then all the contents would be deleted. Protected time means the content is available just for a specific time period. Transparent time means the content is available in all the times.
Identity privacy manages by the service provider base on the service registration phase agreement.
The content privacy policy defines time and location privacy of the content. The owner- defined content privacy

policies are mandatory rules and no dealing can be made on them. Therefore all parties should fully accept the content privacy policies or the owner would not send any content to them.
The content-required location and time privacy (identified in this phase) should be less than or equal to the service registered location and time privacy (identified in the service-registration phase) to not allow the service provider access to a higher privacy level than the service registered privacy in the previous phase. So in this phase:

- The proposed model preserves data privacy even after the owner releases the content without attaching any tag or increasing the size of the content.
- All parties can interact with XML tags and enjoy scalability and platform independence of the model.

2.3.5 Save Data and Finish Phase

In the previous phase, the content privacy policy has been set and user starts using services. In this phase our model preserves the content privacy after using the service and saving the contents.
When a user decides to finish off using services or saving content, in the first step the system checks the time privacy policy of the information that the user wants to save.
If the time privacy is "Private Time" - meaning the user can use content just during the service time- then once the user finishes using the service all the contents should be deleted from both the service provider and the user device sides.
If the time privacy is "Protected Time" - meaning the user can use contents just during a specified time period and this policy should preserve even after saving the data - then the contents can be saved only on the service provider and it is available only during the specified time period.
If the time privacy is "Transparent Time" - there is no restriction on the time of using content - so the content may be saved on the user device as well.
After controlling the time privacy, system checks the content location privacy. If the location privacy value is "Private Location", then the user can use the service only when service provider detects his real location, so no data can be saved on either the user device or the service provider side.
If the location policy is "Protected Location" then the data can be saved only on the service provider but not on the user device and the user location should be confirmed for a later content access.
If the location policy is "Transparent Location" then the contents can be saved on both user devices and the service provider. So in this phase:

- The model provides a complete content privacy from the time of the content production until the saving data without adding any attachments to the content or increasing the size of the saved data.
- All the saving content policies are applied through XML tags and because some parts of the data can be saved on the service provider so the access time for those data would be decreased and the scalability is increased.
- We have explained all five phases of our model. In following section we explain the proposed model encryption/decryption processes.

2.4 The Model Encryption/ Decryption Processes

All parties in our model use public/private keys. A 160-Bit ECC key provides the same security level as a 1024 RSA key, while the smaller key size leads to less power consumptions and less memory and bandwidth usage[26].

All communications before the service registration phase are encrypted and decrypted using these keys.

During service registration phase the user receives a pair of public/private keys for each registered service called service using key. From this point all communications between the user and the service provider for that service would be encrypted and decrypted using this key.
If the agreed location privacy policy between the user and the service provider in the service registration phase is protected location or transparent location, two other symmetric encryption/decryption keys should be used namely the location confirmation key and the exact location confirmation key.
The location confirmation encryption key is held in the service provider while the correspondence decryption key is held in certain trusted portals that have enough trust level with the service provider to confirm the user location. When the service provider sends the content with the location confirmation privacy it encrypts them with the location confirmation key so only users that are in the covered area of trusted portals get access to the contents after the portal decrypts them.
The exact location confirmation encryption key is held in the service provider and decryption key is held in portals that have enough trust level to check the exact user location. The location confirmation key can be any simple symmetric key. This key uses the user's exact geographical location information to encrypt the data at the service provider side. At the portal side the portal reads the user exact geographical location information and feeds the user location to decrypt the data, then sends the decrypted data to the user.

3. Conclusion

In this paper we proposed a privacy model which provides users full control over private information by providing user control over content, identity, location, and time privacy. The model is highly scalable because of its

distributed decision making processes and its platform independence. The model unobtrusiveness is less than 10%, and the policies are able to support mandatory and discretionary rules, context sensitivity, uncertainty handling, and conflict resolution to provide high expressiveness.

This research can be extended to the following areas:

a) Adding mechanisms to support concurrent, multiple authentication methods to increase the accuracy of the user APL that increases the model privacy.
b) Applying "secret sharing" techniques to overcome the probability of collusion attack that can result from the collusion of light houses and portals that will divulge parties private information, this technique can be used for eliminating the software trust-ability assumption too.

REFRENCES

[1] Weiser, M. (1995). The computer for the 21st century. 933-940.

[2] Carnegie Mellon University. (2002). *Project Aura.* Retrieved 1 Feb, 2007.

[3] MIT University Computer Science and Artificial Intelligence Laboratory. (2006). *MIT project oxygen.* Retrieved 15 Jan, 2007.

[4] University of Illinois. *The Gaia homepage, Retrieved Aug 2007.*

[5] Microsoft Co. (2007). *Easy living.* Retrieved 1 Feb, 2007.

[6] Lahlou, S., Langheinrich, M., & Rocker, C. (2005). "Privacy and trust issues with invisible computers". *Communications of the ACM, 48*(3), 59-60.

[7] Russell, D., Streitz, N., & Winograd, T. (2005). "Building disappearing computers". *Communications of the ACM, 48*(3), 42-48.

[8] Recommendation of Council Concerning Guidelines Governing the Protection of Privacy and Transboarder Flows of Personal Data, (1980).

[9] Lahlou, S., & Jegou, F. (2004). Ambient agoras programme report.

[10] Dritsas, S., Gritzalis, D., & Lambrinoudakis, C. (2005). "Protecting privacy and anonymity in pervasive computing: Trends and perspectives". *Telematics and Informatics, 23*(3), 196-210.

[11] Nguyen, D. H., & Mynatt, E. D. (2002). "Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems" (GIT-GVU-02-16): Georgia Institute of Technology.

[12] Rennhard, M., & Plattner, B. (2003). "Practical anonymity for the masses with mix-networks". *Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE2003.Proceedings.*255-260.

[13] Al-Muhtadi, J., Ranganathan, A., Campbell, R., & Mickunas, M. D. (2002). "A flexible, privacy-preserving authentication framework for ubiquitous computing environments". *International Workshop on Smart Appliances and Wearable Computing (IWSAWC 2002),* 771-776.

[14] Jiang, X., & Landay, J. A. (2002). "Modeling privacy control in context-aware systems". *IEEE Pervasive Computing, 1*(3), 59-63.

[15] Beresford, A. R., & Stajano, F. (2004). Mix zones: "User privacy in location-aware services". *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004.* 127-131.

[16] Blaine, A. P., Adam, K., & Nuseibeh, B. (2004). "Keeping ubiquitous computing to yourself:A practical model for user control of privacy". *International Journal of Human-Computer Studies,63*(1-2),228-253.

[17] Dritsas, S., Gritzalis, D., & Lambrinoudakis, C. (2005). "Protecting privacy and anonymity in pervasive computing: Trends and perspectives". *Telematics and Informatics, 23*(3), 196-210.

[18] Ranganathan, A., Al-Muhtadi, J., Biehl, J., Ziebart, B., Campbell, R. H., & Bailey, B. (2005). "Towards a pervasive computing benchmark". *3rd International Conf. on Pervasive Computing and Communications Workshops(PerCom2005 Workshops),* 194-198.

[19] Myles, G., Friday, A., & Davies, N. (2003). "Preserving privacy in environments with location-based applications". *Pervasive Computing, IEEE, 2*(1), 56-64.

[20] Henricksen, K., Wishart, R., McFadden, T., & Indulska, J. (2005). "Extending context models for privacy in pervasive computing environments". *Third IEEE International Conference on Pervasive Computing and Communications Workshops, 2005.PerCom2005 Workshops.* 20-24.

[21] Cheng, H. S., Zhang, D., & Tan, J. G. (2005). "Protection of privacy in pervasive computing environments". *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on, 2,* 242-247.

[22] Iwai, M., & Tokuda, H. (2005). "RFID-based location information management system with privacy awareness". *The 2005 Symposium on Applications and the Internet Workshops, 2005. Saint Workshops 2005. ,* 468-471.

[23] Xinyi, H., Susilo, W., Yi, M., & Futai, Z. (2005). "Identity-based ring signcryption schemes: Cryptographic primitives for preserving privacy and authenticity in the ubiquitous world". *19th International Conference on Advanced Information Networking and Applications, 2005. AINA 2005. ,* 649-654.

[24] Imada, M., Ohta, M., & Yamaguchi, M. (2006). "LooM: An anonymity quantification method in pervasive computing environments". *20th International Conference on Advanced Information Networking and Applications, 2006. AINA 2006,*92-96.

[25] Al-Muhtadi, J., Hill, R., Campbell, R., & Mickunas, M. D. (2006). "Context and location-aware encryption for pervasive computing environments". *Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference.*

[26] Gupta, V. M.,M.Fung. (2005). "Sizzle: A standards-based end-to-end security architecture for the embedded internet". *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications,* 247-25