A Survey on Data Privacy Approaches in Biomedical Sensor Network

Narasimha Kamath A
Department of Computer Science
PESIT-BSC
Bangalore

Chinthan Bhat
Department of Computer Science
PESIT-BSC
Bangalore

ABSTRACT
Wireless Sensors are a new class of devices. They have the potential of capturing, processing and communicating the data to the required destination within the given timestamp. Biomedical Sensor Network (BSN) is explicitly used for constant monitoring of patients. Within the hospital or extended care environment, there is an overwhelming need for BSN for effective patient monitoring and collaborative data processing. Data privacy is the relationship between the collection and dissemination of data. Privacy concerns exist wherever personal identifiable information is collected and stored-in digital form. Improper or non-existent disclosure control can be a root cause for privacy issues. In this paper, these concerns are discussed and how they are addressed by existing systems, and also discusses current issues and solutions to the privacy concerns in a BSN based system.

General Terms
Sensor Networks.

Keywords:
Biomedical Sensor Network (BSN), Privacy

1 . INTRODUCTION
There is been an increasing number of people having chronic medical conditions such as diabetes and heart disease. If these people's health conditions could be monitored continuously and remotely, medical professionals could react to life-threatening situations such as heart attacks much more quickly. Moreover, since each patient's data is collected over a long period of time, physicians could provide more accurate diagnoses and better treatment. Current monitoring solutions, however, are both cumbersome and costly [1]. Typically, a patient is attached to a number of medical sensors that convey information on his or her vital signs to a bedside monitoring device. However, because these connections are wired, such a setup severely limits the mobility of the patient, making it unsuitable for long-term continuous health monitoring.

Wireless sensor networks consist of many different types of sensors aiming at monitoring a wide variety of ambient conditions [1]. Recently, with the rapid development and implementations of wearable medical sensors and wireless communication, wireless body sensor networks (WBSNs) has played a significant role in e-healthcare, which allows the vital data or parameters of a human body to be collected by wearable or embedded sensors automatically. Further, the patients' vital data will be transmitted to the database through short-range wireless communication devices. A variety of sensors such as heart rate monitor sensors, blood pressure monitor sensor and pulse Oxi-meter SpO2 monitor sensors are already in use. As most sensor devices and their applications are wireless in nature, security and privacy are among the major areas of concerns [2].

Despite the increased range of these potential applications, the gap between the privacy requirements that they pose and the existing sensor network privacy mechanisms remains unresolved. Existing WSN research has focused on monitoring the physical environment. However, a BSN has distinct features, like the mobility of sensors and sensitive nature of data, which aggravate the privacy challenges. It is important in such networks that only authorized users can query or monitor the network and that medical data remain protected and uncorrupted.

Security and privacy in BSN have not been investigated in much depth before, and therefore, it provides ample avenues for research [3]. In this paper, an effort is being made to identify open questions and see whether and how they are addressed by existing proposed systems. Paper is structured as follows. Section 2 discusses about the overview of a BSN in medical care, while in section 3 talks about current privacy issues in the field of BSN, section 4 describes solutions to current issues and last section discusses about a future aspect of BSN.

2. OVERVIEW OF BSN IN MEDICAL CARE
BSN provides a variety of features that incorporates stringent technical prerequisites, along with a sophisticated communication environment, providing twofold services. Firstly, it will be a great help for elderly patients, it reduces the effort of travelling to the required medical center to get their health conditions updated. Secondly, they increase the efficiency of treatment in a hospital environment [3]. This section discusses some of the latest happenings in the field of BSN. So far quite familiar with the code blue architecture, SNAP architecture, WBSN group [3] which strived hard to ensure privacy mechanism in BSN. This section discusses about SPOC- A secure and privacy preserving opportunistic framework, PPSPC (Privacy Preserving Scalar Product Computation) in a few lines to understand how PHI (Personal Health Information) is privatized to demobilize data corruption.

2.1. SPOC
SPOC is a newly built privacy mechanism, using the user centric approach, to reduce fluctuating privacy issues in BSN [4]. Several privacy solutions have been proposed in protecting BSN's link layer communication, which constitutes the bottom layer of the sensor network protocol stack. More attention has been given to robust and efficient key management schemes, which serve as the fundamental requirement in encryption and authentication.

Advantages

- Allows medical user to decide who can participate in an opportunistic computing process to privatize his PHI to combat data corruption.
- User centric approach allows only the qualified medical user to access his PHI.

- Highly reliable PHI is less prone to data manipulation by the intruders.

2.2. PPSPC

PPSPC [4] framework focuses on initializing the system, the scenario depicting healthcare care monitoring under normal conditions and the health care monitoring during emergency situations.In the normal scenario health care prediction is totally based upon the analysis of patient data. The system initialization is done by the medical user and other attributes are looked after in a stringent fashion to overlay the quantitative factor. In an emergency scenario such as abnormal rise of heart rate the healthcare center monitors all these changes and act in this situation immediately by sending the medical professional according to the medical user's need. The advantage of PPSPC is entirely based upon its usage during emergencies as well as during the normal scenario that is, it's all about the evaluation of data and its maintenance to preserve the so called privacy factor via system models and other frameworks that ensures data privacy.

3. PRIVACY ISSUES

Within many kinds of privacy rights, patients' privacy rights in the medical care are seeking more importance in the modern world [5]. The process of authorization should not be overlooked and the user should not be given rights to have control over their data of any type. Privacy in a medical care environment comprises of two terminologies: anonymity and unlink ability [5]. Anonymity is the right given to the medical user to protect his documents from researches, managerial staff and insurance provider. Unlinkability indicates that multiple medical records cannot be clubbed to trace the patient profile. In BSN privacy issues incur during data transfer due to the disclosure of data to an intruder via an adversary can compromise a sensor node, alter the integrity of the data, eavesdrop on messages, inject fake message, and waste network resource. Moreover, disclosure of data via the wireless communication is highly unpredictable and seeks a solid foundation to deteriorate data disclosure and promote data hiding or abstraction. Designing a suitable privacy construct for a BSN has become a challenging task that we start by identifying the problems and attacks that can be conducted on BSN data. Privacy threat in BSN depends upon the different adversary models that can attack depends upon their capabilities and their view of the network. Typical adversaries include

- BSN software distributor or provider
- Network provider
- Third party
- Users [5]

Software provider develops a software application required for BSN, being responsible for the entire development of BSN application [5], sometimes may be due to accidental mistakes, privacy concerns are not taken care of and this can be a root cause for privacy issues in the application level. Network provider unlike the software provider may not be able to see the contents of messages being transferred to the destination. In case of Network providers, passive or long term attacks are more common. A third party is one who markets fake applications or use his applications to retrieve the data via the users. Users of the network can also take a role to de-privatize the data. He is usually an active attacker focusing on a single target. Note that although these attacks are presented as different problems that arise when dealing with location data, some of these attacks are in fact closely related. For instance, tracking attacks usually end up with the identification of the subjects. Moreover, these attacks are quite uncommon and can happen due to accidental mistakes made by any one of them. The next section discusses about privacy protection strategies and suggest some relative measures to overcome privacy issues

4. PRIVACY PROTECTION STRATEGIES

4.1. Privacy by Policy

Privacy policies are trust-based mechanisms that aim to protect location information and any other collected personal data from accidental disclosure or misuse. In the United States and Europe, these privacy policies are influenced by the Fair Information Practices (FIPs) [6], originally codified in the 1970s. A subset of them was later tailored by the Federal Trade Commission to eCommerce, emphasizing properties such as notice, choice, access, and security. They aim to inform individuals about the data collected, offer them choices as to whether they wish to share this data for other purposes, give them access to their data so that they can review or delete information, and, finally, protect the security of the information. Even though these codes are still considered a gold standard for privacy protection, they pose two main limitations. The first one is the assumption that corporations can be trusted to handle a user's personal information and those policies and regulations are generally enforceable. Privacy policies are ultimately vulnerable to disclosure of personal information, accidental or malicious. Second, not all people have the same privacy preferences. On location-based systems these preferences vary with place, social context, and even culture, assigning to privacy a specific, varied, and highly individual meaning. Against the second problem, the latest research directions for providing privacy for BSN sensing systems attempt to engage participants themselves to answer privacy dilemmas [7].

In pervasive technologies like BSN, data collected is often aggregated, filtered and sent to the required destination. The problem with this kind of approach is, resource constrained BSN nodes are unable to handle data overloading and more than that efficiency of privacy based solutions aren't compatible with changing BSN requirements. Policy based privacy solutions are difficult to implement practically and if at all they can be implemented, 65% [7] will not be on the basis of policies. Policy based solution just provide an abstract view to the developer regarding the implementation and it is entirely dependent on him, so as to design a good policy based approach which can be implemented. The major issues a developer can face during the implementation phase are:

- Improper data
- Component design becomes tedious
- Compatibility issues
- Cost
- Component testing

These issues can be minimized, if a sensible policy is prescribed to the developer so that major issues regarding privacy can be resolved.

4.2. Privacy by Architecture

As discussed in the previous section, privacy by policy cannot protect from stronger attackers, who would not be deterred by policies and regulations. A consensus has not been reached in the privacy research community on how realistic these stronger attacker models are. A system is represented by a set of components and the overview or snapshot of the system containing these components is represented using an architecture diagram. MDA (Model Driven Architecture) is incorporated during system specification phase to combat privacy issues. Cryptography researchers are using advanced cryptography techniques to ensure data privacy. Privacy by architecture works under stronger attack models and covers the above concerns. The basic goal here is to actively design for non-identifiability of users and provide stronger privacy guarantees, in the sense that even if an attacker has access to the necessary information; no

personally identifiable data can be created or recreated with reasonable effort. In general, to achieve this goal some degree of noise needs to be introduced into the data set and thereby distort its contents and usefulness.

4.3. Anonymity based Techniques

This class includes all solutions based on the notion of anonymity, which is aimed at making an individual (i.e., her identity or personal information) not identifiable. Early solutions suggested the use of static pseudonymous IDs, but soon it was realized that it might be trivial to infer the true identity behind each pseudonym [9] by linking all user entries together. Therefore, pseudonyms must frequently change in order to decouple identity from location-time information. In general, the methods in this class do not guarantee that the process of linking a pseudonym to an individual is impossible, but that it requires a large effort.

4.4. Obfuscation based Techniques

As mentioned, even when identifying information is removed from reports, associating pairs of time and location data might still prove a rich source of information for inference about a user's location and activity. To make it harder to link reports back to the same user, an approach is to obfuscate location and time information, lowering their precision or accuracy and adding enough confusion in the data. As an example, consider AnonySense [10], a privacy-preserving architecture for realizing participatory sensing applications. AnonySense uses the concept of tessellation for protecting the location privacy of contributing users.

In tessellation a point coordinate is generalized to a plane in space, which is referred to as a tile. The sensor reports uploaded by users contain the tile ID and a time interval ID, rather than the absolute location and time. This generalization is guided by the principle of k-anonymity, which ensures that at least k users are located in the same title within a time interval. Hence, it is difficult for an adversary to distinguish between the k users, based on the location or timestamp within the reports. The problem with this solution is that it requires the presence of a sufficiently large number of active users, or else the tiles must be made impractically big

4.5. Network level Anonymity

Protecting the privacy of the user demands not only solutions at the data layer, but also at the network layer. Often, techniques for achieving anonymity on the network and data level are combined, as there is no real anonymity on the data level without anonymity on the network level. Providing anonymity at the first hop of communication (i.e., between the user and the mobile operator or WI-Fi [12] hotspot) is a problem that has not been addressed extensively. So here it is considered only attackers who are able to observe the traffic over the Internet between the access point and the service provider. At this level the goal is to provide communication anonymity, which means hiding the network identifiers in the network layer (i.e., MIP addresses).

Since mixes were proposed in 1981 as a solution for achieving anonymous communication, multiple other protocols have appeared in the literature in order to provide anonymity over the Internet. The capability of BSN is entirely based on its usage and requires optimal privacy preserving algorithms to handle data in a subsequent manner. Management of data in the network layer requires crucial privacy concerns since packetized data are to be delivered to the right destination. The important parameters that are to be taken care of during network level data transmission are:

- Identification of destination and its purpose
- The Path along which data is to be transmitted
- Understanding the complexity of data
- Getting rid of intermediate users (eg: hacker)

Particularly approaches that are used to send data via wireless channel require improvements and that is where procedures are lacking to ensure a stable privacy.All the approaches that are used currently have their own pros and cons, ability to improvise the given problem requires understanding of basic constructs and that is where all approaches are lagging behind or have some or the other issues with them. In a traditional wireless network data binding or encapsulation follows a straight forward approach which makes it easy for intruders to extract the data via malicious applications. Cryptography and authentication mechanism provide a reasonable defense for mote-class outsider attacks. However, cryptography is inefficient in preventing against insider attacks. It remains an open problem for additional research and development. The key establishment method to secure communication in BSN has emerged to be biometrics.This method uses pseudo random number generation to encrypt and decrypt the data.

In particular, low-latency anonymous overlay networks seek to provide, from the user's point of view, a reasonable trade-off between anonymity and performance. Some of the most prominent low-latency approaches include Crowds, Tor, Jap, and Onion Routing [11]. Still, only a few of these anonymizing networks have been tested for the BSN scenario and it is an area that only lately attracted research interest. Performance plays a much more important role here than it does in the traditional wired Internet. Mobile networks generally have much lower bandwidth capability and more transmission errors than wired networks, a fact that causes even higher latency. Expensive cryptographic operations on the mobile phone also contribute to degradation of performance. The resulting latency significantly affects the user experience, and users are known to be impatient and willing to wait only a short time, especially in scenarios where they do not get a direct benefit. Most BSN sensing projects could tolerate some latency when it comes to the delivery of the message, at least compared to browsing the Internet. For example, Anonysense, the only BSN sensing project so far that employs an anonymizing network, integrates Mixmaster. Mixmaster [13] is the primary anonymizing network for sender anonymity in email messaging and belongs to the high-latency approaches. These approaches seek to provide a strong degree of anonymity at possibly increased delay. For example, instead of flushing all messages during each iteration, Mixmaster keeps a subset of messages in the proxy until the next round, meaning that messages may be delayed for hours or even days. This is clearly too much for some urban BSN sensing applications, like those that build real-time maps of noise and air.

4.5. Privacy Preserving Security Protocol

For most BSN sensing applications, it is essential to enforce access control in order to prevent service abuse and protect against malicious attacks. Access to services for users, offering data should be granted only based on pre-established trust between users and the service provider. Authentication gives users and service providers assurance that no intermediate devices have tampered with the data and that they are indeed interacting with the intended parties, and not some malicious entities. There are many approaches to privacy, as highlighted earlier; however, most of the time these approaches lead to a

chicken-and-egg conundrum. On one hand, a user has to be authenticated before accessing a service; on the other hand, the user's ID can serve as a unique identifier that can be used to track the user's whereabouts, preferences, and actions. So a question arises: If privacy is to be preserved through user anonymity, how can a service provider be convinced that an anonymous user is trustworthy? In response to this, a lot of research work has focused on anonymous user authentication that targets user privacy while maintaining access security.

The basic idea has been to verify the user's right to access a service, while at the same time keeping the user's identifying information secure. In what follows, a review some of these techniques and briefly discusses their merits in achieving privacy-preserving authentication in people-centric applications [16]. Blind signature schemes are just like ordinary signatures in which the contents of the message are not revealed to the signer of the message. Typically, to produce such a signature on a message m, the user first blinds the message by combining it with a random quantity r and then forwards the blinded message m to the signer. Once the message is signed, the user proceeds to remove the blinding factor, thus obtaining a signature on the original message. Blind signatures can be used in the BSN sensing scenario as a means to provide for authentication tokens by which a user can hide their identity and obtain access to a particular service. Care has to be taken, however, so that a malicious user cannot effectively mount a chosen message attack by obtaining signatures on arbitrary messages or simply reuse the tokens.

Another approach to enhancing anonymous authentication is to use group signatures (and the simpler ring signatures), on which a vast amount of research is being carried out worldwide. These technologies can be used to verify whether or not a user is allowed access without actually identifying the user. This is achieved by allowing a member of a group to sign a message on behalf of the group, without revealing which member produced the signature. Thus, the owner of the system can tell that a group member created the message, but not exactly which member. One problem in the case of group signatures arises from the fact that anonymity can be revoked by an authority, called the group manager, who, in case of disputes or unauthorized access, can identify the user — this last concept is not provided by ring signatures. This may act as a deterrent for malicious user behavior, but on the other hand, the revocation capability can be used by malicious group managers and service owners to track the actions of legitimate users as well. Now a discussion is being done at a different paradigm in which users can enjoy maximum privacy, provided they use a particular service a predefined number of times. This concept is called anonymous k-times authentication [14]. This scheme has two distinct features that make it very attractive in the BSN setting. First, it ensures that no one, not even an authority, can identify a user who has not exceeded the allowable number of authentication attempts. Second, it allows anyone to trace, without help from the authority [15], dishonest users who are overusing a particular service. Thus, this scheme is more preferable than the identity escrow/group signature schemes, in which the authorities have the ability to trace users. Additionally, the scheme is not confined to one particular service, but can be applied to multiple services, provided the access threshold has not been exceeded. However, each role can be, distributed among multiple entities, guaranteeing user privacy even in the case of colluding authorities. An added benefit of this separation of powers is that it provides for accountability in addition to achieving privacy and security: the user's true identity will be revealed when the user is overusing a service (i.e., for more than k times).

5.Privacy based Approaches in BSN

This section depicts the overall work done and approaches followed in the field of BSN. Many kinds of privacy threats have been existed, such as authenticated or unauthorized access, message disclosure, message modification, denial-of-service, node capture and compromised node, and routing attacks, etc. Among which two kinds of threats play the leading role, the threats from device compromise and the threats from network dynamics. The problem of privacy is rising nowadays. Now a day, Wireless Sensors Network (WSN) is becoming a assured technology in the realm of advanced applications. The one of its latent position is in the form of an unguided BSN to determine physiological sign. The security and privacy of patient-related data are two indispensable components for the system security of the BSN. By data privacy, it means the protection of information from unauthorized users while data being stored and transferred and data privacy means right of individuals to control the collection and use of personal information about themselves. Security and privacy issues are raised automatically when the data is created, transferred, stored and processed in information systems [8]. BSN is a unguided network utilized for interaction among sensor nodes in or about the human body in order to supervise critical body parameters and activities. These supervising signs are collected by a personal server, e.g. PDC or Smart phones which acts as a sink for the information of the sensors and send them to caregivers for proper health supervising. The Health Insurance Portability and Accountability Act (HIPAA) mandates that, as the sensors in BSN collect the wearer's health data (which is regarded as personal information), care needs to be taken to protect it from unauthorized access and tampering.

Because BSN systems and their supporting infrastructure are operated with extremely stringent constraints, they present a greater challenge in the areas of throughput, data integrity and data security when compared to traditional clinical systems. BSN is a unguided network utilized for interaction among sensor nodes in or about the human body in order to supervise critical body parameters and activities. These supervising signs are collected by a personal server, e.g. PDC or Smart phones which acts as a sink for the information of the sensors and send them to caregivers for proper health supervising. Especially, the privacy of communication through the Internet may be at risk of attacking in a number of ways. Online collecting, transmitting, and processing of personal data causes a severe threat to privacy. Once the utilization of Internet-based services is concerned on-line, the lack of privacy in network communication is the main conversation in the public.

This problem is far more significant in the modern medical environment, as e-healthcare networks are implemented and developed. According to common standards, the network linked with general practitioners, hospitals, and social centers on a national or international scale. While suffering the risk of leaking the privacy, data such networks' privacy information is facing great danger. Hence, much attention must be paid to the privacy principle of transparency, so that patients must know who has access to their data and for what purpose.

Table 1: list of data privacy based approaches in BSN

Brief Summary	Authors	The Approach used/followed
The paper focused on security and privacy related issues and discussed relative solutions like elliptic curve cryptography, biometrics and hardware encryption.	Tassos Dimitriou, Krontiris Ioannis	• An approach to organize autonomous but cooperative IDS agents. • These agents are distributed over the network to detect the incoming attacks [1]
A computing framework which was mainly focused on location based criteria and the main aim of the paper was to privatize PHI (Personal Health Information) via SPOC framework	Rongxing Lu, Xiaodong Lin and Xuemin (Sherman) Shen	• The Proposed SPOC framework is formulated using Bilinear pairing. • User-Centric Privacy Access Control for m- Healthcare Emergency. • Privacy analysis using theorem proving approach • Performance evaluation of SPOC framework using NQH (Number Of Qualified Helpers) and RCR (Resource Consumption Ratio) approach [4]
This paper presents a general view of information flow in healthcare and evolving regulatory landscape.	Ajit Appari and M. Eric Johnson.	• Role-Based Access Control (RBAC) originally developed to manage access to resources in a large computer network.[6]
Role Based Access Control (RBAC) that offers the flexibility to specify users, roles, permissions, actions, and the objects to privatize. Used the Z Notation for formal specification of RBAC privacy policies and for queries to review these privacy policies. To ease the effort in creating the correct specification of the security policies, RBAC-based graphical models (such as Secure UML) are used and automatically translated into the corresponding Z specification.	Nafees Qamar, Johannes Faber, Yves Ledru, and Zhiming Liu	• Formal querying and Z model approach for healthcare privacy policy. • Z notation and jaza tool following first order logic and set theory approach to specify software system.[8]
A thesis on privacy preserving methods and future directions regarding the privacy preserving approaches.	Ioannis Krontiris, Felix C. Freling, Tassos Dimitrou	• Advanced cryptography techniques like blind signature and group signature. • Uses anonymity based approach in the network level and incorporates privacy strategies in architecture level which follows MDA (Model Driven Architecture). [7]
In this paper, a survey was conducted on security and privacy challenges introduced by these emerging sensing networks and identify some key concepts to deal with them, aiming to incentive further research in this area	Jordi Herrera-Joancomart´, Cristian Tanas, Cristina P´erez-Sol`a	• Uses in-site validation approach to have sensor network managers traveling to the location of the sensor node and verifying that the sensor readings provided correspond to reality. • Reputation based and credit based approach to foster network cooperation. [5]
Paper focused on general security and privacy issues in a Body Area Sensor Network by giving relevant challenges and possible solutions	E. Toch, Y. Wang, and L. F. Cranor	• Uses data integrality, authentication, encryption and freshness protection approaches to prevent privacy and security risks. • ID-based cryptography and propose a novel secure architecture to enable secure communications in large-scale wireless networks. [6]

6. CONCLUSION

This paper has focused on privacy issues in BSNand has also looked upon privacy issues in BSN by stating the possible reasons for privacy based attacks. An attempt being made to discuss privacy protection strategies at the architecture level, network level, policy level and anonymity based approaches to combat privacy issues. Currently BSN is making its move towards advanced techniques to resolve privacy issues this includes MDA (Model Driven Architecture), rolling code cryptography. Next step is to provide a strong privacy mechanism to minimize privacy threats in a BSN based system.

7. ACKNOWLEDGEMENT

The authors would like to thank their parents and friends for their support and encouragement and would like to express their sincere gratitude to all faculty members for their moral support.

8. REFERENCE

[1] Security Issues in Biomedical Sensor Networks Tassos Dimitriou, Krontiris Ioannis Athens Information Technology, 19002 Peania, Athens, Greece {tdim,ikro}@ait.edu.gr

[2] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: Challenges and opportunities," IEEE Pervasive Computing, vol. 3, no. 4, pp. 16–23, 2013.

[3] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," Department of Computer Science, University of Virginia, Tech. Rep. CS-2006-1, 2006.

[4] Secure and Privacy Approach in Mobile-Healthcare emergency Using PPSPC technique 1MOWNIKA.K, 2K.C.PRADEEP 1,2Dept. of CSE, KAKINADA INSTITUTE OF ENGINEERING & TECHNOLOGY., Yanam Road, Korangi, E.G.Dt,AP, India

[5] Security and Privacy Challenges in Smart Sensor Networks Cristian Tanas Dept. Eng. de la Informaci´o i les Comunicacions Univertsitat Aut`onoma de Barcelona ctanas@deic.uab.cat Cristina P´erez-Sol`a Dept. Eng. de la Informaci´o i les Comunicacions Univertsitat Aut`onoma de Barcelona cperez@deic.uab.cat Jordi Herrera-Joancomart´I Univertsitat Aut`onoma de Barcelona jherrera@deic.uab.cat IN3 - Univertsitat Oberta de Catalunya jherreraj@uoc.edu.

[6] E. Toch, Y. Wang, and L. F. Cranor, "Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems," User Modeling and User Adapted Interaction, vol. 22, no. 1, pp. 203–220, Apr. 2012

[7] Location Privacy In UrBSN Sensing Networks: Research Challenges And Directions Ioannis Krontirois, Goethe University Felix C. Freling, University Of Mannheim Tassos Dimitriou, Athens Information Technology.

[8] C. Cornelius, A. Kapadia, and N. Triandopoulos, "Anony-Sense: Privacy-Aware People-Centric Sensing," Proc. 6th ACM MobiSys '08, Breckenridge, CO, June 2008, pp. 211–24.

[9] C. Ruiz Vicente, D. Freni, C. Bettini, and C. S. Jensen, "Locationrelated privacy in geo-social networks," IEEE Internet Computing,vol. 15, no. 3, pp. 20–27, May 2013

[10] I. Teranishi, J. Furukawa, and K. Sako, "k-times Anonymous Authentication," Proc. 10th ASIACRYPT '04, Dec.2012, pp. 308–22.

[11] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN 2008), vol. 0, pp. 245–256, 2008.

[12] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Transactions on Parallel Distributed and Systems, to appear.

[13] H. G. Hwang, H. E. Han, K. M. Kuo, and C. F. Liu, The differing privacy concerns re-garding exchanging electronic medical records of internet users in taiwan, Journal of Medi-cal System, 36, 6, (2012)

[14] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Over-exposed?: privacy patterns and considerations in online and mobile photo sharing," in CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems. New York, NY, USA: ACM, 2007, pp. 357–366

[15] C. Ruiz Vicente, D. Freni, C. Bettini, and C. S. Jensen, "Locationrelated privacy in geo-social networks," IEEE Internet Computing, vol. 15, no. 3, pp. 20–27, May 2011.

[16] M. Healy, T. Newe, and E. Lewis, "Efficiently securing data on a wireless sensor network," Journal of Physics: Conference Series, vol. 76, 2010.