Security Analysis of Emerging Remote Obstetrics Monitoring Systems

Chiu C. Tan*, Li Bai†, Dimitrios S. Mastrogiannis‡, and Jie Wu*
*Department of Computer and Information Sciences, Temple University
†Department of Electrical and Computer Engineering, Temple University
‡Department of Obstetrics, Gynecology and Reproductive Sciences, Temple University School of Medicine
{cctan,jiewu}@temple.edu, lbai@temple.edu, dimitrios.mastrogiannis@tuhs.temple.edu

***Abstract*—Remote obstetrics care monitoring is currently being used in many different countries to improve the quality of prenatal care, with promising results. The next generation of remote monitoring systems take advantage of improvements in wireless communications and mobile phone technologies to incorporate off-the-shelf equipment, such as Android smartphones, into their design. This not only reduces the overall cost, but also allows for greater flexibility, since the patient can perform monitoring in the comfort of their home. However, our analysis suggests that recently proposed systems have inadequate security protections needed to meet HIPAA requirements for health data. We also proposed recommendations to improve the security of these emerging systems.**

Keywords: Obstetrics; Telemedicine; Security; Home monitoring; HIPAA.

I. Introduction

Assessment of fetal health is an important component of modern obstetrics care. According to the American College of Obstetricians and Gynecologists (ACOG), in 2002, electronic fetal monitoring was used in approximately 85% of births in America, making it the most common obstetrics procedure performed. The frequency of monitoring can range from weekly to continuous, in laboring or hospitalized pregnant patients. The majority of high risk obstetric patients requiring fetal assessment in the outpatient setting, are surveyed once or twice weekly. This sometimes places a high burden on patients, especially those living in remote areas, who have to travel long distances to a hospital to access specialized fetal care.

Telecommunication advances have made it possible to provide *remote* monitoring, where the patient can visit her nearby clinic that has been outfitted with the appropriate monitoring equipment, instead of visiting the hospital. The data collected in the clinic is then transmitted to the hospital for diagnosis. This type of remote monitoring system is increasingly being deployed in various countries, such as the United States [1], Australia [2], and Europe [3], [4]. In recent years, improvements in wireless communication and sensor technologies have led to a more advanced form of telemedicine that can allow monitoring at home instead of the clinic [5], [6].

The majority of research on remote obstetrics monitoring systems have either focused on the medical effectiveness of using these systems, or the technical challenges (battery power management, data processing, etc.) in designing one. There has been relatively little research on another important issue, which is the security of such systems. Recently reported vulnerabilities on other types of medical devices, such as pacemakers [7] only serve as a reminder on the importance of ensuring the security of obstetrics monitoring systems.

There are two additional factors which make the security of remote monitoring systems especially important. The first is the shift away from hospital-grade monitoring equipment towards the use of consumer-grade equipment, such as smartphones, to build these monitoring systems. Consequently, obstetrics monitoring systems will now have to deal with the security vulnerabilities of such consumer-grade equipment [8], [9], [10]. The second factor would be the legal requirements that govern systems, like remote obstetrics monitoring systems, that deal with electronic health data. An example of legal requirements are the specific requirements laid forth by the Health Insurance Portability and Accountability Act, HIPAA.

A. Related work

Remote obstetrics systems have been in operation for a number of years, and their medical and cost effectiveness are well studied [11], [12], [13]. A recent survey paper by [14] provides a good overview of this area.

Body sensor networks (BSN) [15], [16] and *mobile health (mHealth)* [17] systems are a growing trend of healthcare monitoring research that is characterized by the use of inexpensive off-the-shelf components, like smartphones, to build health monitoring systems. Given the importance of security, there has been extensive research on BSN [18], [19] and mHealth security [20]. Unlike our work, most security research in this area addresses more general security threats, and do not focus on specific HIPAA requirements.

B. Our contributions

In this paper, we will focus on emerging remote monitoring systems that allow for at-home monitoring with consumer-grade devices. We will compare the security of two recently proposed systems found in the academic literature against the HIPAA guidelines, and suggest possible modifications to enhance security. *We stress that the systems used in the analysis are prototype systems and may include additional security measures that are present, but not reported in the literature.* The main contributions of this paper are as follows

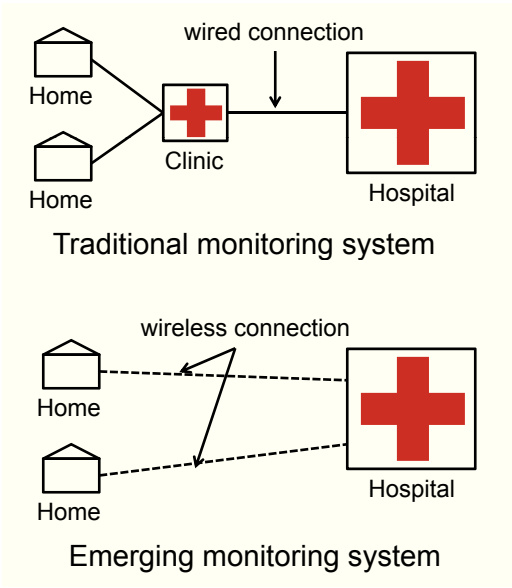

Fig. 1: Illustration of remote obstetrics monitoring systems.

- We provide an overview of the relevant security requirements needed for remote monitoring systems based on the HIPAA Security Rule.
- We analyzed two proposed systems to suggest potential security vulnerabilities, and provide possible enhancements. These can be applied to other types of remote medical monitoring systems beyond obstetrics monitoring.

The rest of the paper is as follows. Section II will explore such systems in greater detail, and Section III will provide an overview of the HIPAA security requirements. Sections IV and V contain the security analysis and recommendations respectively. Finally, Section VI concludes.

II. Overview of Remote Obstetrics Monitoring

In this section, we first categorize the different types of remote monitoring systems, followed by examining the key differences between them. Finally, we present a detailed description of two recently proposed monitoring systems.

A. Remote Monitoring System Classification

We classify remote obstetrics monitoring systems into two categories. Fig. 1 illustrates the two categories.

The first category are *traditional* systems where standard hospital monitoring equipment, like a fetal cardiotograph are installed in an off-site location such as a clinic [21]. Trained medical professionals operating the cardiotograph will treat the patient. The data collected by the cardiotoraph will then be transmitted to the hospital where specialized obstetricians will interpret and diagnose the data. Such a system can allow patients, especially those who are living in remote areas, access to a high level of care while reducing the financial cost. This is accomplished, in part, by leveraging the existing general care network to perform the monitoring with specialized diagnosis being performed in a centralized location. Traditional monitoring systems are well studied, and their effectiveness are well documented [11], [12].

TABLE I: Summary of differences between traditional and emerging monitoring systems.

	Traditional systems	Emerging systems
Treatment location	Clinic	Home
Personnel	Medically trained staff	Non-medical personnel
Hardware	Medical grade	Off-the-shelf

The second category of remote obstetrics monitoring are *emerging* systems where off-the-shelf equipment like smartphones modified for fetal monitoring [6] are used, in lieu of a more conventional fetal cardiotograph. For home-based monitoring systems [22], [23], [24], the patient herself will be operating the monitoring equipment. Similar to the traditional system, the data is transmitted to the hospital to be analyzed by the obstetrician. Emerging systems can further reduce costs by eliminating the need for a medical professional to administer the monitoring. Off-the-shelf monitoring equipment is also cheaper than standard monitoring equipment. The collected data from home-based monitoring will also be transmitted to a remote hospital where a specialized medical staff will interprete the results.

B. Key Differences

While both traditional and emerging systems allow for remote obstetrics monitoring, there are key differences with significant security implications. Table I summarizes the differences.

The first difference is that the monitoring is no longer restricted to a clinic, but the user's home. By performing monitoring at the clinic, system designers can assume a certain (higher) level of security protections. Off-site clinics are already likely to have in place, for instance, procedures and mechanisms to authenticate the patient, regulate equipment access, secure databases, up-to-date computers, and so on. However, these same assumptions cannot be made in a home environment, which in turn complicates the system design. For example, in a traditional system, the monitoring device may not need to be password-protected, since the clinic may very well have its own procedures to manage the problem. In the emerging system, some password protection mechanism, together with the corresponding password management, will need to be in place.

In home-based monitoring, there are no medical professionals at hand to operate the monitoring device. As a result, emerging systems may require a redesign of the user interface to provide adequate feedback, so that the user is able to operate the device correctly. Furthermore, emerging systems may have to manage the situation where the monitoring device detects an emergency situation, since there are no medical staff readily available to help the user.

Finally, emerging systems make extensive use of commercial smartphones as a means of coordinating the sensors, collecting the data, and transmitting it to the hospital servers.

Unlike dedicated medical devices used in traditional systems, these smartphones are multi-purpose devices which are open to greater security risks. For instance, the user may accidentally introduce a virus into the smartphone by downloading an app, which may in turn compromise the security of the monitoring system. This type of security threat is minimized in traditional monitoring systems which are dedicated to a particular task.

C. Emerging Systems in Detail

To better analyze the security implications of emerging obstetrics monitoring systems, we summarize two systems that have been recently proposed. We stress that both systems are still in the proof-of-concept stage, and thus any security features (or lack of), should not be interpreted as flaws in the systems. Furthermore, security regulations like HIPAA may not even be applicable, for instance, when the system is to be deployed outside the United States.

System I (Roham et. al [22]). The main components of the system are (1) monitoring devices, (2) central unit, (3) gateway device. Figure 2 illustrates the system architecture. There are two types of monitoring devices, a toco pressure sensor and a ultrasound Doppler heartbeat detector. The monitoring devices are connected to the central unit via a wired connection. The central unit does some data processing on the heartbeat data to filter out errors, and also forwards the collected data to the gateway device. The central unit and the gateway device uses a wireless communication channel in the form of Bluetooth. The gateway device is an Android smartphone. The gateway device will use WiFi, GPRS, Edge or a 3G wireless network to transmit the sensed data back to the hospital's server. The data transmission is performed using secure file transfer protocol (SFTP), which means that the gateway does not depend on the wireless network to provide security.

System II (Lee et. al [23]). The main components are (1) a handheld Doppler device and (2) a smartphone. The Doppler device is connected to the smartphone using an audio cable. The smartphone is a TyTN II phone running Windows Mobile OS. The smartphone processes the data and transmits it back to the hospital server using GSM or GPRS. This system incorporates a feedback design that informs the patient when the data has completed transmission to the hospital servers. Once the data is successfully transmitted, the hospital servers will send an electronic message to the medical professional that new data is available for diagnosis. A separate publication by the same group [25] notes that HTTPS protocol is used to encrypt the data during transmission to the servers. While this system does not incorporate a toco pressure sensor, the system allows the patient to manually input into the smartphone when there is any fetal activity. This input is timestamped and later matched with the fetal heartbeat information.

III. Security Requirements and Adversary Attacks

The general requirements for the HIPAA Security Rule are to provide the protections for the confidentiality, integrity, and availability of data, defend against reasonably anticipated security or integrity threats, and protect against data disclosures not allowed under the HIPAA Privacy Rule. In this context, *confidentiality* refers to preventing unauthorized personnel from accessing data, *integrity* refers to protecting the data against unauthorized alterations, and *availability* refers to ensuring the data is accessible and usable to authorized personnel on demand). Next, we will present an overview of HIPAA security requirements, followed by describing the adversary model.

A. Summary of HIPAA requirements

We will mainly focus on the technical safeguards (*Section 164.312*) and some portions of the physical safeguards (*Section 164.310*) of the HIPAA Security Rule.

The specific requirements are as follows. All except the last requirement fall under the technical safeguards. The last requirement belongs to the physical safeguards.

- Access control. The system needs to regulate access to the data by authorized personnel or programs. Specific details include requiring the system to be able to identify and track a specific user, and have a means of allowing access to the data in an emergency. Also, the system may need to include a feature to perform encryption/decryption of the data and session control (e.g. automatically logging out the user after a period of inactivity).
- Audit control. The system needs to implement a mechanism to record and examine the activities of the system.
- Integrity. The system needs to incorporate mechanisms to both protect the stored data, as well verify that the stored data has not been tampered with.
- Person/Entity authentication. This requires the system to verify that the identity of the entity accessing the data is correct. In other words, authentication allows a system that restricts access to a particular doctor to actually verify which doctor is accessing the data.
- Transmission security. This requires the system to prevent unauthorized access of the data during transmission over the network. This includes encryption of the data during transit, as well as methods to determine that the data has not been modified during transit.
- Device and media controls. This requires procedures to ensure that the data be safely deleted when the user is no longer using the system, or when the system is re-issued to a different user.

B. Adversary Model

We define an adversary whose goal is to violate one or more components described in Section III-A. We assume that the adversary has knowledge of the monitoring system, e.g., information such as communication protocols, schedule of data transmission, and so on. We also assume that the adversary will have access to any hardware necessary to communicate with the monitoring system. Thus, if some specialized hardware is used to communicate with the monitoring system, the adversary is assumed to have access to that hardware

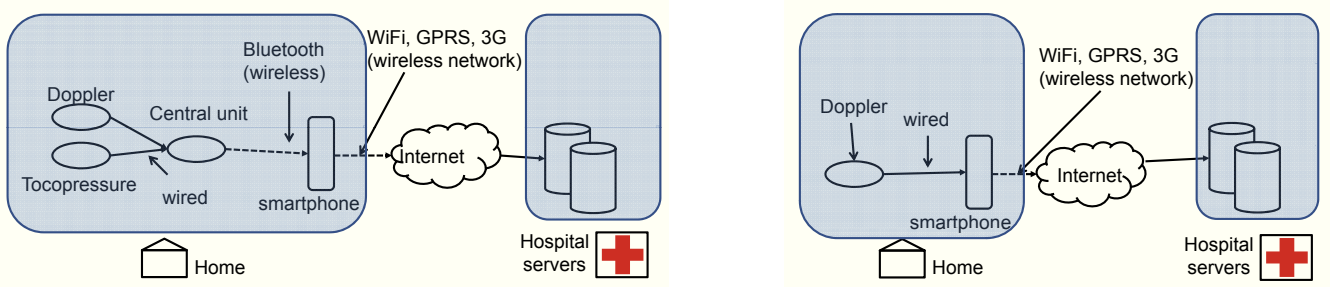

Fig. 2: System architecture of Systems I (left) and II (right)

as well. Our analysis excludes denial-of-service attacks, such as wireless jamming which can prevent any communications between the monitoring system and the hospital servers.

For convenience, we assume that all the data is to be stored into the hospital's servers. We restrict our discussion to attacks on the monitoring system itself, and not on the hospital information technology infrastructure. Once the data is stored into the hospital's database system, the data is considered secured. The hospital thus can be considered a trusted party.

IV. Security Analysis

Here, we will analyze the security features for Systems I and II, based on the system description found in [22] and [23] respectively. For meaningful analysis, we will assume that conventional security features common to most smartphones are present, regardless of whether it was mentioned in the original papers. Table II summarizes the results.

Access control. In System I, the data from the sensors are transmitted to the smartphone from the central unit using Bluetooth. The security of Bluetooth ensures that the data reaches the smartphone securely. Since most smartphones have a password feature, we can assume that only authorized personnel can have access to the password, and thus the data. Both smartphones appear to support a removable microSD card for larger storage capacity. Assuming that the data is stored in the microSD card, the card can be removed to access the contents in an emergency situation. An auto-log off feature can be easily added if necessary. In System II, the sensors are directly plugged into the smartphone, and the same features of the smartphone can be used to provide access control, as in System I.

However, neither System I nor II support encryption of the data while it is inside the smartphone. An adversary with physical access to the smartphone can remove the the microSD card to access the data. An adversary-controlled malicious app, which the user unknowingly installed on the smartphone can also potentially have access to the stored data.

Audit control. Both systems perform some data processing on the data collected by the Doppler device. However, neither system appears to implement any system to record the operations of the sensing device or the smartphone. As such, it does not appear to be possible to perform any diagnosis of the system activities.

Integrity. System I uses SFTP to transfer the data from the phone to the hospital's servers. SFTP provides integrity protection during the data transfer [26]. However, there does not appear to be any notification in the event of network failure during the data transfer process from the smartphone to the servers. This can potentially create the following vulnerability.

System I allows the smartphone to choose the best wireless networks (WiFi, GPRS, 3G, and so on) to transmit the data. In an environment with poor network connectivity, different portions of the data could be uploaded using different wireless networks to the server. This might lead to a violation of integrity protection when, for instance, all but the last portion of the data was never uploaded successfully. The integrity protection offered by SFTP only applies to the data transmitted *within* each SFTP session, and the smartphone will have to create a new SFTP session each time it switches to a different wireless network. As a result, the doctors performing diagnosis on the data from the hospital's server may be incomplete, thus violating integrity.

System II uses HTTPS to transfer data from the phone to the hospital servers. HTTPS is built on top of transport layer security (TLC) [27] which provides integrity protection [28]. System II incorporates a user feedback mechanism that informs the user when the data has been successfully uploaded, and then informs the medical personnel that the data transfer is completed.

In the same scenario as before, the user is aware that the data on the hospital's server is incomplete and can try to upload the data again later, or inform the hospital, so as to prevent the obstetrician from using incomplete data for diagnosis. This will prevent medical personnel from diagnosis with incomplete information.

Person/Entity authentication. Both systems can use the password feature of the smartphone to satisfy person authentication requirement. However, neither system appears to perform any entity authentication on either the smartphone or the sensing devices, e.g. Doppler ultrasound. In other words, the hospital does not know whether the data is collected using a valid device or not.

The use of an invalid device can cause multiple problems. A wrongly calibrated device may be used for the monitoring, and thus resulting in incorrect data being used for diagnosis. An unauthorized smartphone will lack the necessary security

TABLE II: Summary of security analysis.

	Access control	Audit control	Integrity	Authentication	Transmission security	Device/Media controls
System I	Partial	No	Partial	Partial	Yes	Unknown*
System II	Partial	No	Yes	Partial	Yes	Unknown*

"*" indicates that requirement can be easily incorporated if not present.

protections that the hospital requires, such as the inability to install third-party applications. As a result, a user that transmits their data to the hospital using an unauthorized smartphone that may have be tampered with by the adversary.

It is worth noting that requiring the user to enter a password to access the smartphone only authenticates the user to the phone. We cannot assume that the phone is authorized, since the adversary can let the smartphone simply allow *any* password to be acceptable.

Transmission security. Both Systems I and II uses standard secure data transmission protocols to transmit data from the device to the hospital. Therefore, both systems provide transmission security.

Device/Media controls. Neither system details the procedures for device and media controls. However, since both systems uses a removable storage in the form of an microSD card, existing hospital policies on device and media controls can be extended to meet this requirement.

V. Security Recommendations

From the security analysis, we see that emerging systems tend to have good transmission security protections, but remain vulnerable to other types of attacks. The following are some recommendations that can help emerging monitoring systems better meet HIPAA Security Rule requirements

The first recommendation is to restrict smartphone capabilities. One of the reasons emerging monitoring systems incorporate smartphones into their system design is due to the general purpose computing capabilities of the phone. However, this flexibility increases the risk of potential vulnerabilities being introduced to the smartphone due to user activities, such as installing malicious applications. Restricting the smartphone capabilities by removing unnecessary applications and preventing the user from installing new applications will help reduce the risk of a compromised smartphone.

The second recommendation is to perform both user and device authentication. As outlined earlier, both user *and* device authentication are necessary to provide integrity protections. Ideally, all components (Doppler ultrasound, tocopressure, central unit, smartphone) should be authenticated. However, only the smartphone is a general purpose computing device where the user can easily install additional programs. This makes the smartphone more vulnerable then the rest of the components, which will are more difficult for the adversary to access. Therefore, at the minimum, the system should authenticate the smartphone before allowing the data to be stored into the hospital server.

The third recommendation is to improve the user feedback process in the data transfer process and the data collection process. Emerging monitoring systems rely on wireless networks (WiFi,3G, and so on) and consumer devices (smartphones) to transmit data from the home to the hospital. This increases the risk that the data transfer may be incomplete, due to wireless network unavailability, insufficient battery resources, misconfigured devices, and so on. A user feedback process like that implemented in System II will help address this problem. In addition, emerging systems should consider including automatic diagnostic software that tries to determine whether the collected data is indeed correct.

It is unclear whether it is necessary encrypt all the data stored within the smartphone device, since the data is already being encrypted during transmission to the hospital's server. Assuming that the data is to be transmitted to the hospital servers almost immediately after collection, and adequate mechanisms are in place to notify the user of a successful or unsuccessful transmission, the data can be deleted after the transmission has been completed. This reduces the risk of having data being exposed in the event that the phone is misplaced. Avoiding encryption on the phone itself also has two additional benefits. First, it simplifies the overall system design, since the hospital can avoid having to setup an additional key management system to manage the keys. Second, it becomes easier to handle emergency situations where the data needs to be accessed immediately. Without encryption, we can simply remove the microSD card to read the data, but encrypting the data will mean having additional procedures to have emergency access to the appropriate key to decrypt the data.

VI. Conclusion

Emerging remote obstetrics monitoring systems have the potential to lower the cost of providing quality obstetrics care by using commercial components. However, this also comes with additional security risks that are absent from traditional remote monitoring systems. In this paper, our analysis of two recent system designs suggests that additional security protections besides simply securing the data transmission is necessary to meet HIPAA requirements.

Acknowledgments

This research was supported in part by NSF grants ECCS 1241461,CNS-1156574,CNS 1138963, ECCS1128209, CNS 1065444, and CCF 1028167, as well as by the Formula Fund from the State of Pennsylvania.

References

[1] C. Lowery, J. Bronstein, J. McGhee, R. Ott, E. A. Reece, and G. P. Mays, "ANGELS and University of Arkansas for Medical Sciences paradigm for distant obstetrical care delivery," *Am. J. Obstet. Gynecol.*, vol. 196, no. 6, pp. 1–9, Jun 2007.

[2] F. Y. Chan, B. Soong, K. Lessing, D. Watson, R. Cincotta, S. Baker, M. Smith, E. Green, and J. Whitehall, "Clinical value of real-time tertiary fetal ultrasound consultation by telemedicine: preliminary evaluation," *Telemed J*, vol. 6, no. 2, pp. 237–242, 2000.

[3] N. M. Fisk, W. Sepulveda, K. Drysdale, D. Ridley, P. Garner, S. Bower, P. Kyle, H. Dhillon, J. S. Carvalho, and R. Wootton, "Fetal telemedicine: six month pilot of real-time ultrasound and video consultation between the Isle of Wight and London," *Br J Obstet Gynaecol*, vol. 103, no. 11, pp. 1092–1095, Nov 1996.

[4] A. Di Lieto, D. Catalano, M. Pontillo, F. Pollio, M. De Falco, F. Iannotti, and P. Schiraldi, "Telecardiotocography in prenatal telemedicine," *J Telemed Telecare*, vol. 7, no. 2, pp. 119–120, 2001.

[5] V. Jones, V. Gay, and P. Leijdekkers, "Body sensor networks for mobile health monitoring: Experience in europe and australia," in *International Conference on Digital Society (ICDS)*, 2010.

[6] H. Shim, J. H. Lee, S. O. Hwang, H. R. Yoon, and Y. R. Yoon, "Development of heart rate monitoring for mobile telemedicine using smartphone," in *International Conference on Biomedical Engineering (ICBME)*, 2009.

[7] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE Symposium on Security and Privacy*, May 2008.

[8] C. Mulliner, "Security of Smart Phones," Master's thesis, Department of Computer Science, University of California Santa Barbara, June 2006.

[9] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A study of android application security," in *USENIX conference on Security*, 2011, pp. 21–21.

[10] Y. Zhou, X. Zhang, X. Jiang, and V. W. Freeh, "Taming information-stealing smartphone applications (on android)," in *International conference on Trust and trustworthy computing*, 2011, pp. 93–107.

[11] R. Kerner, Y. Yogev, A. Belkin, A. Ben-Haroush, B. Zeevi, and M. Hod, "Maternal self-administered fetal heart rate monitoring and transmission from home in high-risk pregnancies," *International Journal of Gynecology and Obstetrics*, 2004.

[12] E. Kosa, C. Horvath, N. Kersner, K. Kadar, F. Kovacs, M. Torok, and G. Hosszu, "Experiences with fetal phonocardiographic telemonitoring and future possibilities," in *IEEE International Conference of Engineering in Medicine and Biology Society (EMBS)*, 2008.

[13] A. Ippolito, M. De Falco, M. Triassi, and A. Di Lieto, "A cost study of prenatal telemedicine," *J Telemed Telecare*, vol. 9, no. 5, pp. 288–291, 2003.

[14] E. F. Magann, S. S. McKelvey, W. C. Hitt, M. V. Smith, G. A. Azam, and C. L. Lowery, "The use of telemedicine in obstetrics: a review of the literature," *Obstet Gynecol Surv*, vol. 66, no. 3, pp. 170–178, Mar 2011.

[15] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body area networks: A survey," *Mobile Network Applications*, vol. 16, no. 2, pp. 171–193, 2011.

[16] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. Leung, "Body area networks: A survey," *Mobile Networks and Applications*, vol. 16, pp. 171–193, 2011.

[17] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Computing Surveys*, July 2011.

[18] H. Ng, M. Sim, and C. Tan, "Security issues of wireless sensor networks in healthcare applications," *BT Technology Journal*, vol. 24, pp. 138–144, 2006.

[19] S. Lim, T. H. Oh, Y. B. Choi, and T. Lakshman, "Security issues on wireless body area network for remote healthcare monitoring," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, 2010, pp. 327–332.

[20] D. Kotz, "A threat taxonomy for mHealth privacy," in *Workshop on Networked Healthcare Technology (NetHealth)*, January 2011.

[21] A. D. Lieto, M. D. Falco, M. Campanile, M. Torok, S. Gabor, M. Scaramellino, P. Schiraldi, and F. Ciociola, "Regional and international prenatal telemedicine network for computerized antepartum cardiotocography," in *Telemedicine and e-Health*, 2008.

[22] M. Roham, E. Saldivar, S. Raghavan, M. Zurcher, J. Mack, and M. Mehregany, "A mobile wearable wireless fetal heart monitoring system," in *International Symposium on Medical Information Communication Technology (ISMICT)*, 2011.

[23] C. S. Lee, M. Masek, C. P. Lam, and K. Tan, "Advances in fetal heart rate monitoring using smart phones," in *International Symposium on Communications and Information Technology (ISCIT)*, 2009.

[24] S. Garverick, H. Ghasemzadeh, M. Zurcher, M. Roham, and E. Saldivar, "Wireless fetal monitoring device with provisions for multiple births," in *International Conference on Body Sensor Networks (BSN)*, 2011.

[25] M. Masek, C. S. Lee, C. P. Lam, K. Tan, and A. Fyneman, "Remote home-based ante and post natal care," in *International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2009.

[26] T. Ylonen and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol," RFC 4253 (Proposed Standard), Internet Engineering Task Force, 2006.

[27] E. Rescorla, "HTTP Over TLS," RFC 2818 (Informational), Internet Engineering Task Force, 2000.

[28] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246 (Proposed Standard), Internet Engineering Task Force, 2008, updated by RFCs 5746, 5878, 6176.