Proceedings of the 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE), Larnaca, Cyprus, 11-13 November 2012

Enabling Data Protection through PKI encryption in IoT m-Health Devices

Charalampos Doukas,
Dept. of Information and Communication Systems Engineering
University of Aegean
doukas@aegean.gr

Ilias Maglogiannis
Dept. of Computer Science and Biomedical Informatics
University of Central Greece
imaglo@ucg.gr

Vassiliki Koufi, Flora Malamateniou, George Vassilacopoulos
Dept. of Digital Systems
University of Piraeus, Greece
{vassok; flora; gvass}@unipi.gr

Abstract— **Ambient Assisted Living (AAL) aims at providing unobtrusive support to frail and elderly people for their daily life based on their context and situation. To this end, systems and services are required which are user-centric and adaptable towards the needs and capabilities of the people in need of care. The continuous integration of leading-edge technologies, such as cloud and wireless communication technologies, in the context of the Internet of the Things (IoT), can meet this requirement by enabling a new form of communication between frail and elderly people, their environment and relevant groups of care givers. However, for IoT-based systems to reach their full potential, sound answers need to be provided to the important security questions arisen, particularly those regarding authentication of entities (people and environmental objects) and data privacy. This paper presents a system based on Gateways (GW) that aggregate health sensor data and resolve security issues through digital certificates and PKI data encryption.**

Keywords-component; Ambient Assistive Living, Internet of Things, PKI Security, wearable sensors

I. INTRODUCTION

Population ageing, along with the increasing survival rates from disabling accidents and illnesses, is expected to lead to an increase in the proportion of the population with impairments, disabilities or chronic illnesses. Ambient Assisted Living (AAL) services can provide support for these people in their daily routine to allow an independent and safe lifestyle for as long as possible [1]. Thus, care is moving out into the community with health systems requiring real-time information to enable the practice of care irrespective of the location of both the healthcare professional and the patient. To this end, AAL services are underpinned by home-based assistive technologies (e.g. intelligent, highly personalized network embedded objects, such as wireless devices and sensors) that are surrounding frail persons and are serving them in a customized manner [2]. These technologies offer data streams that delineate both the behavior and wellbeing of these people while providing new modes of interaction between them, their family, caregivers, and other healthcare professionals involved.

The "Internet of Things" (IoT) is an emerging global information service architecture, which will likely be one of the most important technological advances of this century impacting a wide range of fields, including homecare. Essentially, it will herald the start of a new era when all manner of devices will talk to each other and to intermediary services. The application and device management backbone needed to achieve inter-device and Internet communication can be provided by cloud computing, which facilitates scaling and provides support to billions of connected objects. In this context, the emergence of IoT can bring about increasing benefits in people's personal and community lives. However, there exist significant inhibitors to its growth and widespread adoption with security being among the most prominent ones.

The term security subsumes a wide range of different concepts, chief among them authentication, confidentiality, integrity and authorization. Opening network embedded objects, such as wireless devices and sensors, to the Internet is likely to spark novel and ingenious malicious models as location proximity will no longer be required to gain access to these objects. Hence, a suitable security infrastructure is required which will scale to accommodate the IoT's amalgam of sensors and devices. In order to prevent the growth of such malicious models or at least to mitigate their impact, different cryptographic mechanisms (e.g. signature algorithms) can be employed.

This paper presents a prototype Cloud-based system, which complies with the IoT concept [3]. The proposed system manages data collected by wearable – textile sensors (i.e. biosignals, motion data and contextual data (like location, ambient temperature, activity status, etc.), which, are forwarded to a gateway utilizing established techniques for IoT communication and then to the Cloud infrastructure. Appropriate interfaces enable the data dissemination to external applications (like medical record systems or emergency detection platforms) and a web-based application provides the essential data real-time monitoring and management. This paper focuses on the security framework incorporated in this system.

In particular, the concept of IoT gateways is introduced for collecting signal and patient data and applying appropriate data encryption, user access control and secure transmission techniques for establishing the essential privacy and security

978-1-4673-4358-9/12/$31.00 ©2012 IEEE

required by health monitoring systems [4]. The paper is structured as follows: Section 2 presents related work in authentication and data privacy for IoT systems and Section 3 discusses the PKI (Public Key Encryption) security solution for IoT systems. Section 4 presents the proposed system architecture and technical details, while Section 5 describes an initial system evaluation based on wearable mobile and environmental sensors that store medical data on Cloud through an IoT-enabled gateway. Finally, Section 5 concludes the paper.

II. Related Work

During the last few years there has been a growing interest in the utilization of IoT-based systems in a wide range of applications, including homecare applications. The shift from an Internet interconnecting end-user devices to an Internet used for interconnecting physical objects that communicate with each other and/or with humans in order to provide a specific service encompasses the need to build a strong security infrastructure as new security challenges arise and traditional protection mechanisms are no longer adequate. Such security challenges are exacerbated by the sheer number of devices and the expected limitations in user interfaces. Among others, certain security aspects, such as authentication and data privacy, require innovative approaches.

As regards authentication, there is a need to define an object authentication mechanism in order to ensure that only authorized objects can gain access to certain portions of data exchanged within an IoT environment. In order for such a mechanism to be effective in an IoT-based system, an aspect that should be considered, prior to designing it, is identity management. This issue is considered to be critical due to the nature of IoT, which essentially constitutes a fusion of digital and physical world. Although user's identity management is a well-investigated topic in the literature, managing the identity of objects comprising an IoT environment raises a number of novel issues to be dealt with [6]. The concept of federation can serve as the basic context for achieving user identification and access control in a way that user convenience is maximized while privacy is being preserved in a cost-effective way [7]. However, in order to apply this concept in an IoT environment one needs to assess its potential ability to deal with both humans and smart objects (e.g. sensors, devices).

As regards data privacy, the nature of IoT-based systems and the technologies incorporated in it constitutes encryption in communication indispensable. Thus, security attacks such as eavesdropping, can be prevented. In IoT-based systems, data are usually obtained by multiple data sources, namely sensors and devices. In Wireless Sensor Networks (WSN) usually a gateway (aggregator node) aggregates data prior to sending them to a server, a Cloud infrastructure, etc. In order to preserve privacy, data should be encrypted prior to their transmission. Many solutions addressing data aggregation while preserving security, i.e. confidentiality, integrity, authentication, and availability, can be found in the literature ([5]-[16]). These can be classified in hop-by-hop encrypted data aggregation and end-to-end encrypted data aggregation [6]. According to the first approach, the data is encrypted by the WSN nodes and transmitted to the gateway. The gateway, in turn, decrypts these portions of data, aggregates them and encrypts the aggregated data again. The encrypted aggregated data are suitable for transition to other systems. According to the second approach, the WSN gateway aggregates the encrypted data received by the WSN nodes and transmits them to other systems.

III. PKI Encryption for IoT devices

The past few years a number of key distribution schemes have been proposed for hop-by-hop encryption of data [8]-[10]. In addition, a secure hop-by-hop data aggregation protocol, namely SEDAN [11] has been proposed, according to which each node can verify immediately the integrity of its two hops neighbors' data and the aggregation of the immediate neighbors by means a management of new type of key, called two hops pair-wise key. However, all proposed approaches could be considered vulnerable since the intermediate aggregator nodes, which hold decrypted sensor data, are easy to tamper with. This vulnerability can be addressed by end-to-end techniques for data encryption. These techniques also use a key scheme. In particular, according to some approaches a key is shared among all sensors and the system where aggregated data are transmitted to ([12]-[16]). The aggregator nodes collect and transmit encrypted data without performing any encryption/decryption operations on them. Furthermore, MyDAP ((Dynamic Data Aggregation with Privacy functions)) constitutes an alternative approach whereby an original aggregation algorithm able to deal with end-to-end encrypted data is coupled with a specific privacy management policy [15]. However, one important drawback of the approaches based on end-to-end encryption is that the whole network is compromised if the key used for encrypting sensor data is compromised in one of the sensing nodes.

PKI (Public Key Encryption) constitutes an effective approach to data encryption as it can provide an increased level of confidence for exchanging information over an increasingly insecure environment, such as IoT ([17], [18]). Public key cryptography uses a pair of mathematically related keys. If one key is used to encrypt information, then only the related key can decrypt that information. In case the public key gets compromised, still it is not computationally feasible to retrieve the private key.

In the case of IoT and healthcare, devices that generate patient-related information (like body sensor readings) can encrypt data using a public key and the health monitoring applications (e.g., cloud or web systems operated by caregivers or relatives) can use the private key to decrypt the data. Using also PKI digital certificates the proper authentication of the devices can be achieved, in addition to the secure data transmission.

However the establishment of PKI in IoT systems introduces a major challenge: Even the encryption process with the public key requires computational and memory resources that existing wireless sensor technologies do not provide, especially when frequent data transmission is required (e.g., heart signal transmission) [19]. The proposed system addresses this issue by introducing IoT-enabled gateways. The IoT

gateways are devices with computational abilities comparable to desktop computers, come with integrated full operating system (usually Linux) and have many communication interfaces. These gateways can also address an additional security issue for IoT devices: registration of new sensor devices and key management. When a new monitoring device that transmits data through the Internet is introduced, the device needs to have access to the public key for properly encrypting the data. The latter process raises key management and distribution issues. By using an IoT gateway key management is essential only for the gateway device itself and not every sensor device connecting to the latter. The communication between the IoT gateway and the sensor device can be secured using symmetric encryption (which is less computational intensive than PKI). In addition, the gateway has the ability to receive a new key if required since it is a central communication point always connected to the Internet.

More information about the gateways is provided in the following Section.

IV. The Proposed Architecture

The proposed system enables medical data collection from various mobile/wearable sensors, contextual data (like room conditions, user habits, etc.) collection and secure transmission to caregivers and family members using a Cloud-based infrastructure. The architecture (see Figure 1) consists mainly of three components; the mobile and contextual sensors, the IoT gateways and the Back-end infrastructure.

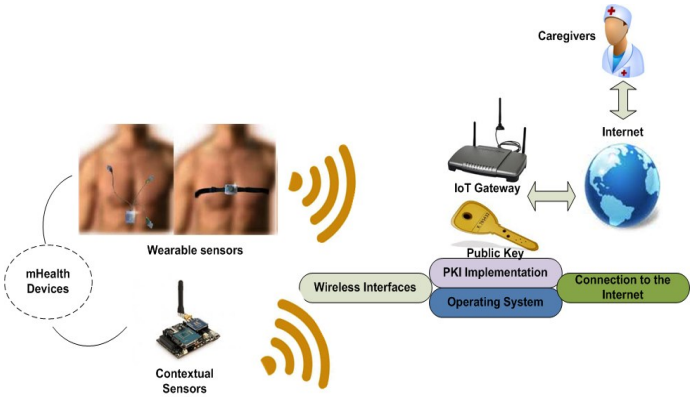

Figure 1. An illustration of the proposed system architecture

A. Mobile and Contextual Sensors

The mobile and contextual sensor devices can continuously or periodically sense data about the patient status (e.g., heart/pulse rate, temperature, etc.) and their context (e.g., room temperature, air quality, lighting conditions, etc.). Usually such sensor devices have a microcontroller unit that receives analog or digital sensor data, interprets them into quantitative values and transmits them to a monitoring/data collection device using a wireless interface (e.g., Bluetooth or ZigBee).

The latter wireless technologies support infrastructure-based networking modes and/or mesh networks. This means that modules that support such technologies can be automatically self-configured and connected to existing wireless networks that are created by the IoT gateways.

B. IoT Gateways

The IoT gateways are computational devices, Linux-based board computers (e.g., the RaspberryPi [20] or the Beagleboard [21]) that have the essential networking interfaces for communicating with sensors (e.g., Bluetooth and ZigBee interfaces) and can also communicate with the Internet using wireless (e.g., WiFi) or wired interfaces. The gateways have better computational resources (usually come with at least 1GHz ARM processor and 512Mb or RAM memory) and host a complete operating system that provides PKI tools (like the OpenSSL).

Through appropriate configuration of the network interfaces and the Linux OS networking the gateways can apply PKI encryption to the incoming data and then forward the latter to web-based medical applications using Web Services or other real-time communication technologies (e.g., WebSockets).

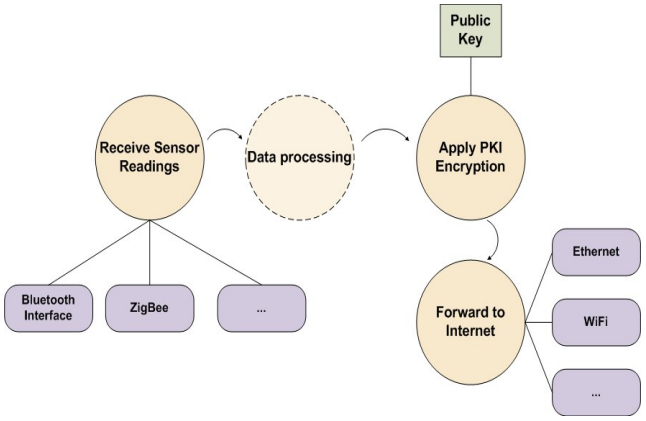

Figure 2. Data Flow Diagram illustrating the basic funcitonality of an IoT gateway.

Figure 2 illustrates the basic functionality of an IoT gateway as described also in previous paragraph. An additional feature is the ability to perform some initial data preprocessing (e.g., data filtering, compression or pattern analysis) before data is encrypted using PKI and forwarded to the Internet using a WiFi or an Ethernet network interface.

Most of the aforementioned Linux development boards come with integrated networking interfaces (like WiFi and/or Ethernet) and also feature GPIOs (General Peripheral Input Outputs). The latter can be connected to various RF modules (like Bluetooth, ZigBee, etc.) enabling thus the communication of the device with various mobile or contextual sensors that monitor patient status.

C. Cloud (Back-end) Infrastructure

Cloud Computing is a model for enabling convenient, on-demand network access to a shared group of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider

interaction. The latter features make Cloud computing a very suitable model for building back-end infrastructures that support data management and visualization of IoT m-health devices. In addition, Cloud resources can provide the essential requirements for PKI information encryption/decryption (like computational resources) and encryption/decryption key management. More information and examples of Cloud utilization for IoT and m-health can be found in [7][4].

V. Initial System Evaluation

In order to evaluate the performance of the proposed system a prototype implementation has been developed. The prototype consists of a wireless (Bluetooth) pulse oxymeter (see Figure 3), a contextual sensor (see Figure 4) that measures room temperature, humidity, air quality and light conditions, an IoT gateway implementation (see Figure 5) and a Cloud-based platform for managing sensor readings.

The wireless sensor measures users oxygen blood saturation and heart pulse rate and can transmit the latter readings to any Bluetooth enabled device. The contextual sensor consists of an Arduino microcontroller device, a digital temperature and humidity sensor, an analog light sensor and an analog air quality sensor. The Arduino can be connected to the home network of the user either through Ethernet of WiFi network interfaces.

Figure 3. A mobile pulse oxymeter by Contek utilized in the prototype implementation

The IoT gateway consists of an open source, WiFi enabled gateway board [22] properly modified to host additional wireless interfaces (like Bluetooth and ZigBee) and a Beagle board Linux board computer. The gateway board collects all information transmitted from the wireless oxymeter and the Arduino microcontroller. Then it forwards the data to the Beagleboard using a serial communication (UART) interface that exists on both devices.

The Beagleboard runs a Python script that accepts data from the UART interface and then applies PKI encryption using a pre-stored public key (1024 bit key length). Then encrypted data are forwarded to a sample Cloud application ([3], [23]) using a REST Web Service. The Cloud application decrypts the data using the private key and presents sensor data to users.

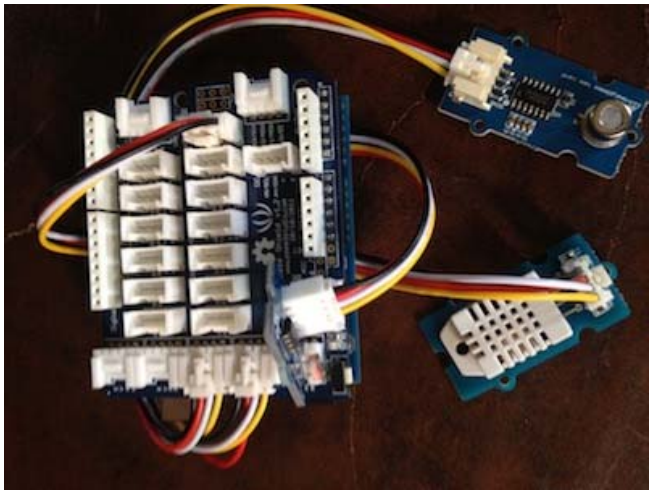

Figure 4. An Arduino microcontroller equiped with temperature, humidity, light and air quality sensors.

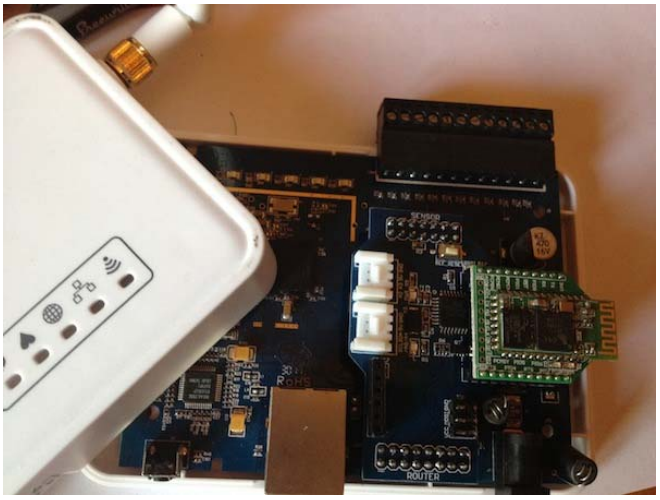

Figure 5. The Dragino open source IoT gateway equiped with a Bluetooth wireless sensor communication module. The gateway features also a embedded WiFi interface that can communicate directly with Cloud-based health systems.

Data (average sensor values) are transmitted in 1-minute intervals. The Python script that encrypts the data has been modified to provide information about the time needed to encrypt the sensor readings (total message length less than 100Kb). Respectively, the J2EE application on the Cloud has been modified to present the time needed to decrypt the data before presenting them to users. According to initial metrics, the total encryption process adds a 24.5% overhead in the total transmission time (about 800msec) and less than 1 second overhead in data decryption. The latter overhead is acceptable in both cases for mobile health applications.

VI. CONCLUSION

The Internet of Things enables the collective aggregation of patient data and patient information that can lead to more accurate and instant diagnosis of health incidents. M-health devices utilize several different communication technologies (Low energy Bluetooth, ZigBee, Wireless, etc.) and different data protocols introducing this way several interoperability issues. Data protection is also quite weak since sensor devices lack the resources for protecting user anonymity, and providing proper authentication and data encryption at the same time. Several security solutions have been provided in the past, but in most cases individual sensor devices and systems are considered or security credentials (such as encryption keys) can be compromised when having access to the devices.

In this paper we presented the conceptual design and prototype implementation of a system based on IoT gateways that aggregate health sensor data and resolve security issues through digital certificates and PKI data encryption. The IoT gateway can both resolve sensor communication interoperability issues and provide a less vulnerable mean for securely authenticating to services and sending patient data. The IoT architecture is considered to have security vulnerabilities, thus the proposed schema could be quite useful for IoT developers especially in the domain of electronic healthcare. Future work includes the extended evaluation of the system with more sensors in a real environment. In addition, private key management and access control should be further investigated.

REFERENCES

[1] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in Information Technology: New Generations (ITNG), 2010 Seventh International Conference on, april 2010, pp. 804 –809.

[2] M. Mulvenna, W. Carswell, P. Mccullagh, J. Augusto, H. Zheng, P. Jeffers, H. Wang, and S. Martin, "Visualization of data for ambient assisted living services," Communications Magazine, IEEE, vol. 49, no. 1, pp. 110 –117, january 2011.

[3] C. Doukas, and I. Maglogiannis, "Bringing iot and cloud computing towards pervasive healthcare," in IEEE International Workshop of Extending Seamlessly to the Internet of Things, July 2012.

[4] F. Kargl, E. Lawrence, M. Fischer, and Y. Y. Lim, "Security, privacy and legal issues in pervasive ehealth monitoring systems," in Proceedings of the 2008 7th International Conference on Mobile Business, ser. ICMB '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 296–304. [Online]. Available: http://dx.doi.org/10.1109/ICMB.2008.31

[5] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," Computer Networks, vol. 53, no. 12, pp. 2022 – 2037, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128609000863

[6] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497 – 1516, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870512000674

[7] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino, "Trust negotiation in identity management," Security Privacy, IEEE, vol. 5, no. 2, pp. 55–63, march-april 2007.

[8] L. Hu, and D. Evans, "Secure data aggregation in wireless sensor networks," in Workshop on Security and Assurance in Ad hoc Networks, 2003, pp. 93–105.

[9] A. Mahimkar and T. Rappaport, "Securedav: a secure data aggregation and verification protocol for sensor networks," in Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE, vol. 4, nov.-3 dec. 2004, pp. 2175 – 2179 Vol.4.

[10] B. Przydatek, D. Song, and A. Perrig, "Sia: secure information aggregation in sensor networks," in Proceedings of the 1st international conference on Embedded networked sensor systems, ser. SenSys '03. New York, NY, USA: ACM, 2003, pp. 255–265. [Online]. Available: http://doi.acm.org/10.1145/958491.958521

[11] M. Bagaa, N. Lasla, A. Ouadjaout, and Y. Challal, "Sedan: Secure and efficient protocol for data aggregation in wireless sensor networks," Local Computer Networks, Annual IEEE Conference on, vol. 0, pp. 1053–1060, 2007.

[12] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on, july 2005, pp. 109 – 117.

[13] J. Girao, D. Westhoff, and M. Schneider, "Cda: concealed data aggregation for reverse multicast traffic in wireless sensor networks," in Communications, 2005. ICC 2005. 2005 IEEE International Conference on, vol. 5, may 2005, pp. 3044 – 3049 Vol. 5.

[14] R. Riggio and S. Sicari, "Secure aggregation in hybrid mesh/sensor networks," in Ultra Modern Telecommunications Workshops, 2009. ICUMT '09. International Conference on, oct. 2009, pp. 1 –6.

[15] S. Sicari, L. A. Grieco, G. Boggia, and A. Coen-Porisini, "Dydap: A dynamic data aggregation scheme for privacy aware wireless sensor networks," Journal of Systems and Software, vol. 85, no. 1, pp. 152 – 166, 2012, ¡ce:title¿Dynamic Analysis and Testing of Embedded Software¡/ce:title¿. [Online]. Available: http: //www.sciencedirect.com/science/article/pii/S0164121211002068

[16] A. Coen Porisini and S. Sicari, "Sedap: Secure data aggregation protocol in privacy aware wireless sensor networks," in Sensor Systems and Software, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, G. Par and P. Morrow, Eds. Springer Berlin Heidelberg, 2011, vol. 57, pp. 135–150. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-23583-2 10

[17] E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryptoschemes for data concealment in wireless sensor networks," in Communications, 2006. ICC '06. IEEE International Conference on, vol. 5, june 2006, pp. 2288 –2295.

[18] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," Computers & Electrical Engineering, vol. 37, no. 2, pp. 147 –159, 2011, ¡ce:title¿Modern Trends in Applied Security: Architectures, Implementations and Applications¡/ce:title¿. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790611000176

[19] K. Piotrowski, P. Langendoerfer, and S. Peter, "How public key cryptography influences wireless sensor node lifetime," in Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks, ser. SASN '06. New York, NY, USA: ACM, 2006, pp. 169–176. [Online]. Available: http://doi.acm.org/10.1145/1180345.1180366

[20] "The raspberrypi board computer." [Online]. Available: http://www.raspberrypi.org/

[21] "The beagleboard board computer." [Online]. Available: http://beagleboard.org/

[22] "Dragino open source gateway." [Online]. Available: http://www.dragino.com/

[23] C. Doukas and I. Maglogiannis, "Managing wearable sensor data through cloud computing," in Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, 29 2011- dec. 1 2011, pp. 440 –445.