Comprehensive study of Communication Security in the Internet of Things (IoT) in Healthcare

Nikhil Lohia, Arizona State University
nlohia1@asu.edu, 1211168085

***Abstract*— The advent of IoT is changing the face of health-care in a number of ways. IoT has the potential to revolutionize the way doctors interact with the patients within a health-care ecosystem. Like every upcoming technology, the security aspects of IoT health-care architecture seems to raise eyebrows and limit its applications. The recent attacks impose a question if the technology can be further carried out or not. Health-care can become a sensitive area unlike a cyber threat as the actual lives of patients is under threat. Among the communication security in Application Layer, Network Layer and Physical Layer, this report focuses on my contribution towards identifying the security issues, solution and challenges in Application Layer.**

I. Introduction

In the twenty first century technology has made its way into every aspect of an individual's life. From personal life to convenience, we are relying on technology and devices for our day to day tasks. An important aspect about these devices is that they are all connected to each other. Health-care is another one of those domains which is becoming technology-dependent with every upcoming advancement and innovation. From devices that measure the heart-beat of a patient, steps of an individual to devices that handle and store large amount of data all are quickly becoming a backbone of the industry.

Health-care data is sensitive than an ordinary data. If there is a threat or attack on a car insurance data, there can only be a monetary loss. However, if we take for instance a diabetic patient whose insulin levels are controlled by a digital device, a hack into the system can threaten the life on the individual. With more and more devices coming into the picture, the security concerns are rising day by day. The concept of IoT lies on the fact that the devices are talking to each other at all times. This increases the convenience but also increases the security concerns. Thus, there comes an urgent need to regulate and safeguard such technologies in today's world. Another concern could be the large number of vendors trying to capture the market, but that is out of scope of this report.

To understand the concerns the project investigates upon the communication security in Application Layer, Network Layer and Physical Layer. For each of the layer, we identify the security issues being addressed, findings and researches, the proposed solution and the security challenges that are encountered. Motivated by these factors I researched and explored upon the Application Layer and ways how communication can be secured in it.

II. System Goals and Scope

All health-care devices should communicate with each other in a fast and a secure manner. To ensure that patients and doctors receive the correct information at the right time, we need to ensure 3 major factors.

- **Data Availability:** We need to ensure that health-related data is available and accessible by doctors and patients on-demand. This is critical to lives of individuals and can often be a major deciding factor to make surgical decisions. Patient data could be continuously transmitted over the time and thus, we need to make sure that accurate and updated information is available to the individuals in the health-care ecosystem.

- **Data Integrity:** Accurate patient information at all times is one of the major security requirements in a health-care ecosystem. This poses a major challenge to the IoT architecture as the devices are connected to each other. A hacker who gains access to confidential patient information could modify it which may lead to catastrophic consequences. This information could even be used to manipulate a patient.

- **Data encryption:** Data encryption in any kind of communication is an important aspect of security. We do not want any eavesdropping on the data by any attacker or any third party. This could result in a leak of personal and confidential information. Many encryption algorithms are used in practice for multiple applications.

III. System Overview

A question arises, how does the network architecture of IoT health-care ensure network security across the entire communication channel. A quick glance at all the three layers can be given as

A. Application Layer

- Application layer vulnerabilities
- Solutions to address the vulnerabilities
- Encryption algorithms at application layer
- Sharing and presenting health-related data to the patient.
- Offloading data from software and hardware devices and storing on servers.

- Authorizing subjects to access patient related information.

B. Network Layer

- Authentication
- Authorization
- Encryption protocols
- eHealth Architecture
- Delegated authorization
- Network security protocol

C. Physical Layer

- Authentication in RFID Tagging
- DoS attack in wireless sensor networks
- Authentication in body sensor networks
- Security issues in wireless sensor networks
- Cancellation based friendly jamming
- Secure links for end-to-end communication

For the scope of this report I will concentrate on the Application Layer and the measures adopted to ensure a secure communication.

IV. Individual Contribution

The Application Layer deals with the high-level functions of programs that may utilize the network. User interface and primary function live at this layer. Doctors access and keep track of patient information using iPads/Tablets/PDAs and all hospitals these days have monitors that display patient queue information.
Suppose that we apply good security through the underlying layers (1 and 2 layer), with physical isolation (layer 1), private VLANs (layer 2), and firewalls with tight packet filter policies (layers 2 and 3). But then we are deficient on our application layer security (layer seven, and often layers six and five), using un-patched server software and poorly written application and script code.

*A. **Hybrid security techniques for Internet of Thing Healthcare Applications**[3]*

Security Topic Addressed: Data Encryption over communication
Security Issue: Data compromise during transmission
Proposed Solution: Applications need to communicate with each other using standard security techniques for the protection and immunization of databases in IoT. We cannot have a standard cryptographic technique for every communicating device in IoT healthcare. The paper suggests a hybrid cryptographic technique which is based upon the following factors

- Use multiple ciphers of different types to take benefit of the strength of each type of cryptography.
- Generate a random secret key for a symmetric cipher, and then then encrypt this key via an asymmetric cipher using the recipient's public key. The recipient decrypts the secret key first and then uses that to decrypt the message.

We have 3 types of cryptographic techniques:

- **Secret Key Cryptography:**This technique uses the same key for both encryption and decryption.
- **Public Key Cryptography:**This technique employs a pair of keys. One to encrypt the message and the other to decrypt the message. The advantage of this method is that the public key can be advertised by the owner to anyone who wants it.
- **Hash Functions:**A hash function creates a fixed size blocks of data by using entry data with variable length. If the data is modified in any way, then the hash function generated will be different. This kind of security measure ensures that the information is transmitted and received exactly the way it was supposed to be. The most common hash algorithms used today are Message Digest (MD) and Secure Hash Algorithm(SHA).

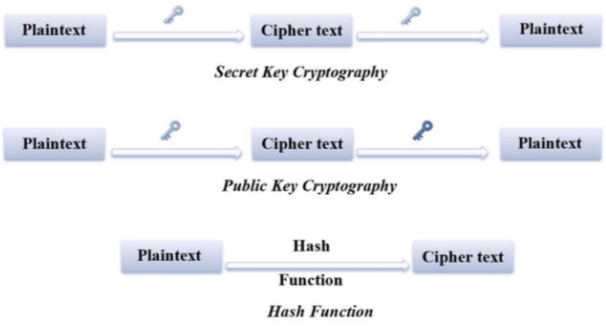

Fig. 1. Cryptographic Methods

A Hybrid technique has combined benefits and reduce the weakness of one method as much as possible by taking the advantage of one over the other. This can be applied to several health-care applications for remote monitoring, physical activity monitoring for aging people, chronic disease management etc.
Security Challenges:

- Extensive use of multiple complex cryptographic functions can make the implementation cumbersome and often requires a lot of time to establish the architecture. The architecture once setup cannot be ensured that it is safe of all the attacks possible. Only with the passage of time, one can get sure enough
- The personnel involved in setting up the architecture would be expected to know all the cryptographic techniques and a working knowledge. Replacing this personnel can have a security risk as some areas can be left exposed.

*B. **A Virtual PHR (Personal Health Record) Authorization System**[2]*

Security Topic: Policies and authorization to access patient information
Security Issues: Secure storage of patient information, maintaining the agile solution for extended periods of time
Proposed Solution: Any application in IoT health-care ecosystem must ensure that the individual accessing the

information must be authorized to do so. One should not be allowed to access the information not intended for him. We can define a role based model for this problem, but it is also possible that an individual can have different access privileges in different environments.
Basically, a personal health record system consists of the following components:

- A non health-care component containing health and social information. Example: Information collected by family members and social networks
- A medical device component containing health information transmitted from Internet connected medical devices. Example: Home care systems.
- A health-care professional component containing information stored into various health-care information systems. Example: Primary care and electronic medical records

Let us take a look at the PHR authorization system proposed by the research paper. It consists of the following components

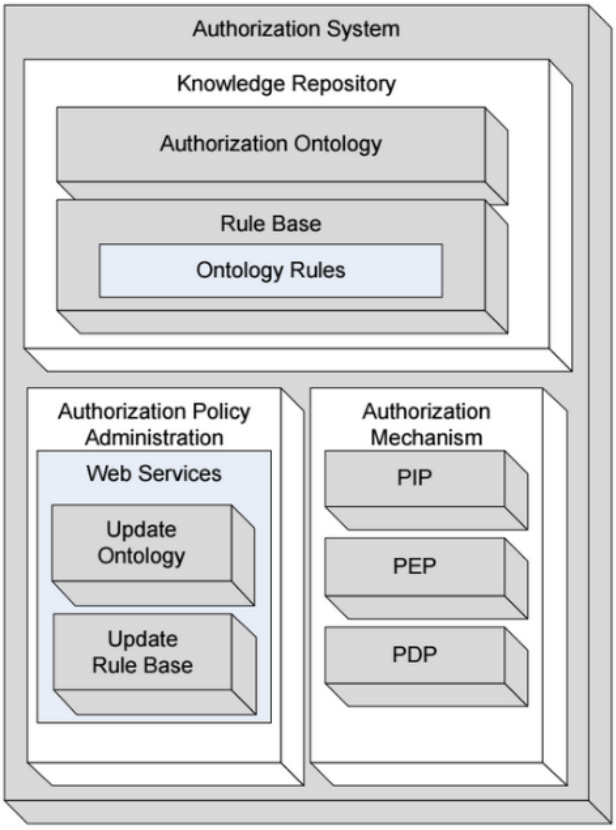

Fig. 2. PHR Authorization System

- Knowledge Repository: This repository hosts an authorization ontology and a base rule. It defines the relationships between the subjects, the environment and related attributes. It automatically infers authorization based upon the RABAC model and applies the required permissions.
- Authorization Policy Administration: This module uses a a bunch of web services to update the knowledge repository based upon the information collected from several devices. It basically updates the ontology and base rule.
- Authorization Mechanism: It consists of 3 parts
  1) PIP (Policy Information point) creates subject to role rules
  2) PEP (Policy Enforcement point) creates the subject to access requests
  3) PDP (Policy Decision point) combines information from the above 2 points and makes a decision whether the access should be permitted or denied.

Security Challenges:

- In this cloud-based PHR environment, the system is implemented as a service which assumes that health-care system are interlaced with interacting services. This means that the authorization information and personnel roles should have the capability to be extracted on the fly.
- One major concern is that all potential subjects are not known in advance. Such a system would require constant updates and a learning methodology to implement.

V. Findings and Analysis

There can be a lot of challenges when handling data in IoT devices and applications. This data if placed in wrong hands can be dangerous and reveal private information about the patient.

- We have several security and encryption techniques available to secure information communication between two nodes but when it comes to health-devices we cannot afford them to be expensive. One major point to consider about health-care devices is also that they should not be power hungry. We need to use techniques that takes care of memory requirements and power utilization as well.
  The research paper[3] suggests to use hybrid cryptographic techniques to ensure secure transmission of information. We can use a mixture of two such that the shortcomings of one can be traded with the benefits of other. Such techniques must however by applied with care as the architecture could become complex to manage over time.
- Information authorization is also really important in an IoT health-care ecosystem. The fact that all devices are connected to each other can become a threat if the authorization mechanism is not put into place correctly. A “cardiologist” must not be able to access the information related to brain of the patient. However, a brain surgeon must have access to the heart information if he is inside the “hospital cardiology department”. Thus, the environment also makes a difference for who can access an information.
  The PHR system addressed in the research paper[2] defines a role and architecture based access control system which helps in determining which kind of role will be assigned to the subject.

VI. Recommendations

Developing a system to ensure proper authorization and access control not only increases transparency but also encapsulates the information.

- Such kind of a protocol can be followed by maintaining en exhaustive hierarchy of user roles and their working environment. This is essential because different settings could change a user role. A personnel can have different access rights under different circumstances as well. An emergency situation could call for an information required which is generally not available for an individual. Hence, rules must be made keeping all such situations in mind.
- Sharing information between applications should take advantage of hybrid cryptographic methods. The weakness of a method must be identified and a stronger method must not be implemented just because it is available. The applications in an IoT health-care ecosystem require only specific controls and the encryption standards must be evaluated before implementing them.

VII. Conclusion

IoT as a new technology has been more widely used and is constantly evolving. Even in health-care applications; the open nature of the information/data media has brought risks to the security of the wireless sensor networks and their collected data. Several techniques can be applied in securing the data transmission between these applications but we need to make sure that it remains cheap and efficient. Apart from the transmission we also need a system on the application level to determine which user can access which information. There cannot be an exhaustive set of rules to determine which subject has what role. A system needs to be created in such a way that the subjects are assigned roles dynamically based upon the environment they are working in.

Many people around the world have access to some kind of PHR but problems regarding privacy and security of patient sensitive data could pose a serious impediment to further PHR development and usage. The main objective of the authorization system is to empower patient control to their health and social data and enable providers to share their data with others in order to support continuity of care.

References

[1] Al-Janabi, Samaher, et al. "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications." *Egyptian Informatics Journal*, (2016).

[2] Poulymenopoulou, Mikaela, Flora Malamateniou, and George Vassilacopoulos. "A virtual PHR authorization system." *Biomedical and Health Informatics (BHI)*, 2014 IEEE-EMBS International Conference on. IEEE, 2014.

[3] Yehia, Lobna, Ayman Khedr, and Ashraf Darwish. "Hybrid Security Techniques for Internet of Things Healthcare Applications." *Advances in Internet of Things*, 5.03 (2015): 21.d

[4] Gong, Tianhe, et al. "A medical healthcare system for privacy protection based on IoT." *Parallel Architectures, Algorithms and Programming (PAAP)*, 2015 Seventh International Symposium on. IEEE, 2015.