IMPROVING SECURITY AND PRIVACY OF INTERNET OF THINGS IN HEALTHCARE

Okafor, Nwamaka Uchenna
Department of Computer Science, Federal Polytechnic Nekede, Owerri, Nigeria.
+2348067981408, +234805855696,
makas4christ2000@yahoo.com

Oparah, Chidiebere Chukwuma
Department of Computer Science, Federal Polytechnic Nekede, Owerri, Nigeria.
+2348036183740,
canonchychuks@yahoo.com

ABSTRACT

The proliferation of Internet of Things (IoTs) in recent time has brought huge changes to all areas of human endeavors, the healthcare is no exception as it is now one of the most attractive areas of application for IoTs. With the introduction of IoT in the healthcare, the sector has witnessed a new phase in providing health care to patients, shifting from the traditional way of health monitoring to a more sophisticated and robust remote monitoring and response. The sector is expected to witness a huge adoption of IoT, flourishing through new ehealth Internet of Things devices and applications in the nearest future. There are many security challenges facing IoT-based devices used in healthcare, both medical practitioners and manufacturers of Internet of Things devices are usually faced with security concerns about the privacy of users' data collected with IoT devices, what if the data is hacked and collected by cyber criminals, what if a virus attacks the device and cause it to malfunction, thus causing harm to patients' lives.

This paper seeks to analyze distinct IoT security and privacy features such as security requirements and threat model within the healthcare perspective, it takes a closer look at security issues posed by the architecture and design pattern of IoT-based devices used in healthcare. It then identifies options available for addressing the many security challenges of IoT-based devices in healthcare, digging into scalable approach to provide a more robust security solution for current and emerging IoTs with focus on policy-based computing; reconfiguration and self-awareness.

Keywords

Healthcare, Internet of Things, policy-based computing,reconfiguration,security, self-awareness

1. INTRODUCTION

Although IoT could be said to be at its infancy in the healthcare, there has been an exponential growth in the application of IoT in healthcare in recent time and this is expected to escalate as time goes on. IoT-based healthcare system can be applied to diverse areas such as health monitoring, management of private health and fitness using wearable devices that can be worn or implanted in a patient's body, it could also be used for care for pediatric or elderly patients as well as for supervising chronic diseases. A patient's health profile could be captured with IoT-based medical device

usually with embedded sensors and attached to the patient's body, captured data could be analyzed remotely and stored, stored data from various sensored devices could then be aggregated and based on the analysis and aggregation, care givers and other medical practitioners can then remotely monitor patients and respond accordingly.

Using IOT-based devices such as ehealth wearables and other IP-based sensored devices to monitor patients' health such as blood pressure, temperature etc. and collecting and sharing vital data about patients' health status would greatly help to improve diagnosis, making continuous and real time monitoring possible and in turn helping care givers and other medical practitioners to easily intervene in time of emergency and also follow-up patient's health status so as to provide adequate preventive care, but this is not without some security challenges as a malicious hacker could steal the data captured by the device and modify it, thus causing harmful damage to the patient's health.

2. IOT SERVICES AND APPLICATIONS IN HEALTHCARE

Medical care and health care represents one of the most attractive areas of application for IoT (Riazul Islam et al., 2015). The emergence of IoT has giving rise to many healthcare applications including remote health monitoring, management of chronic diseases, fitness program and elderly care. Compliance with treatment and medication at home by patients and remote monitoring and response by care givers are also potential application areas of IoT in the healthcare sector.

IoTs can be embedded into various e- health wearable devices which in turn have the capabilities to remotely monitor patients' health, many diagnostic and imaging devices and sensors are smart systems that consist of core part of IoT. IoT-based healthcare devices are expected to enhance the quality of life and enrich users' experiences through the provisions of various healthcare services such as AMBIENT ASSISTED LIVING (AAL) in which an IOT platform powered by artificial intelligence is used to address the health needs of incapacitated or ageing individuals, thus, helping them to live an independent life in a convinient and safe manner.

CHILDREN HEALTH INFORMATION (CHI) in recent time, researchers have developed a specialized IOT service called children health information which aims to address the needs of children with emotional, behavioral or mental health issues by raising the awareness of the public, the children themselves and their families to the needs of these children. (vicini, S. et al, 2012) proposed an interactive totem aimed at educating, empowering and entertaining children in the pediatric ward.Also, (vasquez-Briseno, M. et al, 2012), proposed an interactive system that would encourage children to obtain good nutritional habits through the help of their parents and carers.

SEMANTIC MEDICAL ACCESS (SMA) the use of semantics and ontologies to share large data is now being considered in the health sector. IOT healthcare applications uses medical rule engines to analyze very large amount of sensored data stored in the cloud. A pervasivedata-accessing method that can collect, integrate, and interact with IoT data for emergency medical serviceshas been developed.

3. SECURITY CHALLENGES OF IOTs IN HEALTHCARE

IoT-based health care devices and applications are expected to deal with critical personal information such as private health data, such intelligent devices may be connected to global information network to make them easy to be accessed at any point in time from any location (Rghioui et al., 2014).

There are many security challenges facing IoT-based devices used in healthcare, both medical practitioners and manufacturers of Internet of Things devices are usually faced with security concerns about the privacy of users' data collected with IoT devices, what if the data is hacked and collected by cyber criminals, what if a virus attacks the device and cause it to malfunction, thus causing harm to patients' lives.

The use of IoT in healthcare is faced with many security challenges which if not properly managed could impede the full adoption and application of IoT in the health sector, hence the urgent need to critically identify and evaluate distinct IoT security and privacy challenges including current and forecasted security issues, security requirements, vulnerabilities, threat models and various approaches to provide more robust security. Some of these security issues include:

i. Data Modification: If a patient medical data is intercepted by a malicious either from the source node of an IoT-based device or during data exchange between nodes, he/she could modify the data, thereby presenting a wrong data to caregivers who responds based on the wrong data, this could spell disaster for the patient whose health is monitored using this device.

ii. Impersonation: Every node on the network has an identity and IoT-based network devices are no exception as they all have their unique identities which possibly may contain some of the patient's information, when an intruder steals this identity, he could use it to spy on the patient's health records.

iii. Replay attack: an attacker can retransmit the data exchanged between nodes on the network and this may likely lead to treatment malfunction

iv. Eavesdropping: IoT devices makes use of wireless channels to communicate, this makes it easier for an intruder to be able to listen to the communications between nodes, thus compromising the confidentiality of the patients' data, using such data for more dangerous attacks than stealing the patient's private information.

Other attacks may be based on host and network properties and these include:

i. Hardware attacks: an attacker may steal and tamper with the device physically, extracting the device program codes, security codes, and data and can reprogram the program code of the device with malicious codes, causing it to function abnormally

ii. Software attacks: a malicious may attack the software (operating system, application software), vulnerabilities and bugs and forcefully cause IoT-based healthcare devices to malfunction

iii. Standard protocol attacks: An attacker may deviate from standard applications and network protocols and acts maliciously to compromise message confidentiality, authenticity, availability, and integrity

iv. Network protocol stack attacks: the IETF working group proposed a layered networking model of secured IoT

Table 1: A layered network model of secured IoT

Application
Middleware
Transport
Networks
Adaptation *(Ipv6 low powered personal Area Network*)
MAC
Physical

and each proposed layer is faced with different kinds of vulnerabilities which an intruder may exploit to launch malicious activities. Therefore, to improve the performance of IoT healthcare networks, security must be maintained on each layer of the protocol stack

In identifying the inherent security challenges and countermeasures, adequate attention need to be paid to some challenges posed by the design architecture of IOT-based devices, these includes

i. Computational Limitation: the central processing unit embedded in IoT devises are usually not too powerful in terms of speed and they are not designed to perform highly computational tasks, they just act as sensors or actuators. Therefore, in proposing a security measure for this device, this must be fully taking into account.

ii. Memory Limitation: this may pose a very serious impediment to security in most IoT devices because these devices are usually low on device memory and their memory may not be sufficient to execute complicated security protocol.

iii. Low energy: IoT devices are generally made up of limited battery power (e.g. Blood pressure sensors, temperature sensors) these devices conserve energy by enable power saving modes when no sensor reading needs to be reported

iv. Multi-Protocol: when planning for sound security solutions for IoT devices, it is important to consider the fact that these devices communicates in a multi-protocol environment, for instance, IoT devices may communicate with other similar devices in a local network using a proprietary protocol and the same IoT device may communicate with IoT service provider over an IP network. Therefore, it is important to plan and devise a security solution that will be scalable in such condition

v. Multiple devices: There are so many healthcare devices that are part of IoT health network, ranging from personal computers to low-end RFID tags all these devices have varying capacities in terms of memory, energy, computational power and embedded software, therefore it is pertinent to consider these when planning for security, security solutions should be implemented to accommodate the simplest of the devices.

vi. Mobility: Another fact that is worthy of consideration when planning for security of IoT devices is that these devices are mobile and not static, they are connected to the internet through an IoT service providers, for example, IoT wearable heart monitor may be connected to the internet and notifies the care giver of a patient's health condition, the device would be connected to the patient's home network when he/she is home and would be connected to the office network when in the office. Therefore, security solution must be designed to accommodate such mobility

vii. Topology: Security solutions must be designed to accommodate the dynamic network topology of IoT health devices. It is usual for a health device to join any IoT health network at any point in time in any location. The temporal admission characteristics of medical devices makes the network topology dynamic.

4. POLICY-BASED COMPUTING AS A SOLUTION TO SECURITY CHALLENGES OF IOT-BASED DEVICES USED IN HEALTHCARE

Policy based computing could be described as a software paradigm developed around the concept of building autonomous systems that provide system administrators and decision makers with interfaces that let them set general guiding principles and policies to govern the behavior and interactions of a managed systems.(Lobo, 2007).

(Appleby, K. et al, 2004), described policy-based computing as a software paradigm that incorporates a set of decision-making technologies into its management components in order to simplify and automate the administration of computer systems. A significant part of this simplification is achieved by allowing administrators and operators to specify management operations in terms of

objectives or goals, rather than detailed instructions that need to be executed. A higher level of abstraction is thus supported, while permitting dynamic adjustment of the behavior of the running system without changing its implementation.

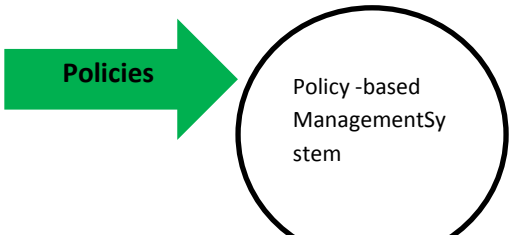
Policy-based computing is one of the many available techniques used to implement autonomous computer systems; it is usually expressed in terms of some behavioral rules to be performed in certain situations. This concept could be gainfully employed to solve most of the security challenges of IoT- based devices used in health care, health monitoring IoT-based devices could be controlled by policies that enables the device to take certain security critical decisions based on an environmental condition. For instance, when there is a sudden influx of data sent and received to a centralized server from a node on which an IoT-based device which is remotely monitoring a patient's health is connected, it could be suspected that there could be an eminent denial of service (DOS) attack, in this case, the server should be able to suspend receipt of data from that particular node, alerting the system administrators and care givers, data from the affected node can then be analyzed to determine any threat.

Policy-based configuration is highly versatile and generally applicable across a very wide application space. When compared with other autonomics techniques, policies represent one of the lowest risk and lowest cost solutions; because there is relatively low complexity with policy implementation.

Policies are a set of rules which are usually stored centrally in a policy data repository. With respect to specific environmental condition at runtime, a specific policy is selected and evaluated.

A policy may even refer to additional policies and applications as needed to solve advanced issues or provide for more dynamic applications. (Appleby et al., 2004)

Figure 1 illustrates a simple model of policy-based computing which can be applied to quality of service, security, or even provisioning and configuration.



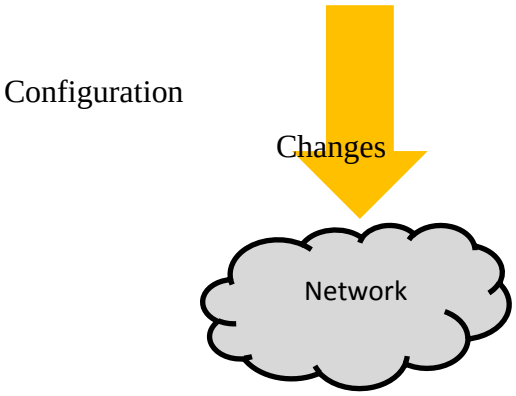


Figure 1: Simple model of policy-based computing.

Policies are quite simple to create and implement provided the set of rules depending on various environmental conditions have been well specified and defined.

In policy based systems, decisions are specified as policies in the software. This concept is used in computer management and is of great help for administrators and system users in general.

5. CONCLUSION

Internet of Things is widely being adopted for use in the healthcare sector as it finds numerous applications in various healthcare services, it is also very useful in many medical devices which monitorspatients' health, and also finds application in assistive living technologies. There are many security challenges which affects the use ofIoT-based devices in the health sector, some of these security issuescould be traced to the design/architecture of these devices as well as their software components. A lot have been done to provide adequate security of these devices so asto forestall the effect of security breaches on these devices in the lives of patients' whose well-being may depend partially or wholly on the proper functioning of these devices. This paper considers the use of policy-based computing in hardening the security of IoT-based devices

used in healthcare, proposing self-reconfiguration of the device's security mechanism based on environmental conditions for adequate security.

References

Riazul Islam, Daehan Kwak, Humaun Kabir, M., Hossain, M. and Kyung-Sup Kwak, (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 3, pp.678-708.

Vicini, S., Bellini S., Rosi S., and Sanna, S., (2012) An Internet of Thingsenabled interactive totem for children in a living lab setting, *ICE Int. Conf. Eng., Technol. Innov. (ICE)*, pp. 1_10.

Vazquez-Briseno, M., Navarro-Cota, C., Nieto-Hipolito, J., Jimenez-Garcia, E., and Sanchez-Lopez, J.,(2012) A proposal for usingthe Internet of Things concept to increase children's health awareness, in *Proc. 22nd Int. Conf. Elect. Commun. Comput. (CONIELECOMP)*, pp. 168_172.

Rghioui, A., L'aarje, A., Elouaai, F. and Bouhorma, M. (2014). The Internet of Things for healthcare monitoring: Security review and proposed solution. *2014 Third IEEE International Colloquium in Information Science and Technology (CIST)*.

Lobo J. (2007), Policy-based computing: from systems and applications to theory. Lecture Notes in Computer Science. Volume 4483, pp 2-2.

Appleby, K., Calo, S., Giles, J. and Lee, K. (2004). Policy-based automated provisioning. *IBM Syst. J.*, 43(1), pp.121-135.

Bibliography

Almotiri, S., Khan, M. and Alghamdi, M. (2016). Mobile Health (m-Health) System in the Context of IoT. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*.

Blake, M. (2015). An Internet of Things for Healthcare. *IEEE Internet Computing*,19(4),pp.4

Ding, D., Conti, M. and Solanas, A. (2016). A smart health application and its related privacy issues. *2016 Smart City Security and Privacy Workshop (SCSP-W)*.

Lin, H. and Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information*, 7(3), p.44.

Rghioui, A., L'aarje, A., Elouaai, F. and Bouhorma, M. (2014). The Internet of Things for healthcare monitoring: Security review and proposed solution. *2014 Third IEEE International Colloquium in Information Science and Technology (CIST)*.

Riazul Islam, S., Daehan Kwak, Humaun Kabir, M., Hossain, M. and Kyung-Sup Kwak, (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 3, pp.678-708.

SathishKumar, J. and R. Patel, D. (2014). A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications*, 90(11), pp.20-26.