Issues in Information Systems
Volume 16, Issue IV, pp. 58-63, 2015

INTERNET OF THINGS-BASED HEALTH MONITORING AND MANAGEMENT DOMAIN-SPECIFIC ARCHITECTURE PATTERN

Robert E. Samuel, Widener University, robert.samuel@ieee.org
Dennis Connolly, Univ of Connecticut, dennis.connolly@cloudwhere.com

ABSTRACT

The rapid increase of the quantified self movement and internet of things technology is resulting in the need for robust and complex solutions. Particular focus is needed regarding the security, privacy and analytics for the collection and management of big data for healthcare applications. This paper proposes an architecture pattern for internet of things based solutions within the context of the healthcare industry.

Keywords: Healthcare, Architecture Pattern, Internet of Things, Quantified Self, Big Data, Analytics

INTRODUCTION

Recent consumer devices aimed towards the consumer healthcare marketplace has popularized the "quantified self" movement to increase self-knowledge and autonomy through numbers [11]. Gary Wolf and Kevin Kelly introduced quantified self in the introduction of their website in the year 2008 (http://www.quanitifiedself.com). They have observed an increased consumer population are using digital self-monitoring and self-modification devices. Wolf observed that over the past decade four things changed to enable one's ability to self-track, report and analyze data points such as social events, habits, behaviors, and health information. First, the increased miniaturization, reduced cost, and improved quality of sensors that are often embedded in wearables. Second, pervasive computing devices began to mainstream adoption. Third, the social media movement increased the general public's appetite to share. And fourth, the low entry barrier to cost-effective computing environments available through cloud technologies [14]. As a result, the healthcare industry is increasing interested in the quantified self movement to address general population health issues. Swan [12] highlights that the vast amount of data being generated by quantified self-tracking and medical information practices increases the importance of information management. Thus, she continues, security and privacy are tantamount concern of emerging healthcare solutions.

When viewed from a population health perspective, quantified self is an example of where a large volume of health related data is being stored at a rapid velocity which contains a variety of information with unknown veracity. Health wellness programs sponsored by employers are increasingly interested in understanding what data impacts employee performance and aids to reduce health expenses [2]. While the long term continuation of the quantified self movement is still to be determined, the pattern for "big data" manipulation for value has taken a strong foothold. Yet, healthcare information system architects are just beginning to understand the complexity of security and data protection mechanisms for this pattern [3].

The perceived value in the quantified self movement which requiring healthcare firms to architect for big data analytics is not just in the collection and aggregation for self-reporting, but rather in the behavioral changes recommended by computer algorithms. Singer [11] reports that "devices are asking consumers to cede their free will to machine algorithms." However, Husain and Spence [6] state that while primary caregivers recommend health apps, several studies highlight there is no current evidence in improving outcomes. Additionally, the studies also indicate that currently no evidence of harm. Regardless, the US Food and Drug Administration has published guidelines regulating mobile apps that enables mobile devices (e.g. smartphones) into medical devices [6]. As a result, additional research is needed to derive the value proposition of quantified self. To support the need to further investigate the healthcare value, a robust and secure architecture needs to be consistently applied across multiple research organizations to advance the studies in a timely manner.

Internet of Things in Healthcare

The sensing layer to enable the collection and transmission of data is commonly referred to as the internet of things (IoT). IoT is the machine to machine (M2M) communication by linking physical and virtual objects through exploitation of data capture and communication capabilities [7]. There is currently minimal number of publications on the architecture pattern in the healthcare domain with respect to the internet of things (IoT) for health monitoring and management. Meng et. al. [9] identified the following four key technologies for an IoT health monitoring and management system: 1) health signs sensing (wearable/portable sensors), 2) information security and privacy protection, 3) massive data storage, and 4) expert systems. For the healthcare insurance industry, IoT provides opportunities such as [4]:

- New insurance products and services
- Reduced claim cost and frequency
- Increased customer engagement
- Improved business intelligence
- Greater accuracy on underwriting decision

With the use of IoT technology, the healthcare industry can support usage-based insurance (UBI) similar to the advancements in the automotive property and causality insurance business with driver behavior monitoring [4]. Therefore, research has highlighted that financial incentives and expense management are the key business objects of IoT health monitoring and management solutions.

Architectural Patterns

Architectural patterns is described by Bass et. al. [1] as "a description of element and relation type together with a set of constraints on how they may be used." The software architect of a system will start with the most generic pattern that best fits the software design based on the business needs. For the purpose of this article, architecture pattern and architecture style can be referred to interchangeable. Examples of generic architectural patterns include client-server, peer-to-peer, and service-oriented for distributed systems; event-driven and publish-subscribe for messaging; and component-based, monolithic, layered, or pipes and filters for structured systems. Additionally, domain-specific architectural patterns are created to address technology domains such as user interfaces, information management, security, etc. and business/industry domains such as automotive, government, manufacturing, healthcare, etc. An architectural pattern is determined by [1]:

- A set of element types
- A topological layout of the elements indicating their interrelationships
- A set of semantic constraints
- A set of interaction mechanisms

Architecture patterns remain and important focus for modern software architecture. Software architecture continues mature over the past decade with both generic patterns and domain-specific patterns [8]. As Kim and Garlen highlight, it is not an easy task to define a new architecture pattern. The authors recognize the importance to establish an IoT-based healthcare domain-specific architectural pattern for monitoring and management.

RESEARCH METHODOLOGY

Our research centered upon the following research question: What are the core technical capabilities for a healthcare industry IoT-based architecture?

The research hypotheses to be tested are as follows:

H_1: Incentive rewarding and expense reducing healthcare business objectives have a greater importance than other healthcare business objectives.

H_2: Security and privacy related technical capabilities have a greater importance than other technical capabilities.

To test these hypotheses the authors used the DELPHI method to solicit predictions from 11 subject matter experts. Dalkey and Helmer [5] states the objective of the DELPHI method is "to obtain the most reliable consensus of opinion of a group of experts." This technique involves the repeated questioning of experts and avoids direct interaction between them. Centralized around a common theme, respondents estimate and contribute information to jointly arrive at a higher quality appraisal and more confident answer. The subject matter experts used in this study were all individuals within Enterprise Architecture organizations of Fortune 500 firms in the healthcare industry. Several rounds of inquiry were conducted based on a scenario describing a consumer community using quantified self devices to monitor and manage their healthcare data.

All communication was conducted through the means of email. The initial round requested the subject matter experts to identify the leading high-level business needs required for supplied scenario. The authors codified the business need responses, consolidated them into common themes, and rank ordered based on number of mentions. For the second round, the subject matter experts were then asked to provide the core technical capabilities that would support the architecture of the supplied scenario based on these common business needs. The authors codified the technical capability responses, consolidated them into common themes, and rank ordered based on number of mentions. The final presented the ranked order results of both the business needs and technical capabilities for review and comment. The subject matter experts were asked to review the relationship between the responses to indicate the architectural constraints and dependencies.

RESULTS

The first hypothesis tested the industry research that monetary drivers are the more significant drivers for technology adoption. The codified expert responses were rank ordered based on the number of mentions as shown in Table 1. To assess the first research hypothesis, the median was calculated and compared to the rank order. The median mention was calculated as 4. Incentive rewarding received 5 mentions and cost reduction mentions received 4 mentions. As a result, the authors conclude that the first hypothesis, H1, is accepted since the number of mentions for incentive rewarding and cost reduction are either equal to or greater than the median. However, other business objective mentions such as promoting healthier living, aggregating data, and tracking changes all had higher number of mentions.

Table 1. High Level Business Objectives Mentions

High Level Business Objectives	Number of Mentions
Ability to Promote Living Healthier	9
Ability to Aggregate Data from Various Devices	7
Ability to Track Event and Behavior Changes	6
Ability to Reward Behavior	5
Ability to Reduce Health Expenses	4
Ability to use Gaming	3
Ability to Compare to General Popluation Health	3
Ability to Share and Collaborate on Data	3
Ability to Track Location	2

The business objectives that impact or support human behavior (ability to promote living healthier, ability to aggregate data from various devices, ability to track event and behavior changes, ability to reward behavior) seem to align with recent healthcare industry trends associated with the term digital health. As outlined in the quantified-self movement healthcare providers, payers, and patients are increasingly focusing on patient engagement via digital methods [11]. Providing timely and relevant data points to both patients and physicians aids in the continuous management of effective medical protocols that reduces medical costs and potential hospitalization. Improved

patient safety, quality and care access are primary industry business drivers [4]. This research seems to support that the general industry trends are further promoted by digital health business objectives.

The number of mentions for high level business objectives also indicates an underlying ability to provide contextual awareness for IoT health applications. Similar to how the advancement of mobility technology has introduced a low-cost and pervasive location awareness, IoT could advance contextual awareness to enable pervasive computing for health-oriented applications [7]. The relationship between collected data streams, environment, and recent computing events provides the connection for health-based contextual awareness. To create contextual awareness, collected information could consist of any of the following examples:

- the user identity
- time/day/week/month/year/season
- environment temperature/humidity/ambient light
- body temperature/motion/velocity/pulse/blood pressure
- emotional status
- mental clarity
- and nearby objects/people.

The second hypothesis tested the industry focus that security and privacy are the core technologies within the healthcare solution architecture. The codified expert responses were rank ordered based on the number of mentions as shown in Table 2. To assess the second research hypothesis, the median was calculated and compared to the rank order. The median mention was calculated as 5. Identity and access management received 5 mentions and privacy and device management mentions received 4 mentions. As a result, the authors conclude that the second hypothesis, H2, is rejected since the number of identity and access management mentions is equal to the median but privacy and device management mentions is below the median. However, other technical capability mentions such as analytics, data repository, user interface, and data management all had higher number of mentions.

Table 2. Technical Capability Mentions

Technical Capabilities	Number of Mentions
Analytics	14
Data Repository	5
Identity and Access Management	5
User Interface	5
Data Management	5
Integration Engine	4
Data Visualization	4
Privacy and Device Management	4
Device	4

Based on the expert technical capability responses, the authors assessed the relationship between the capabilities into an architecture pattern as shown in Figure 1.

The uniqueness of this architecture pattern include a dual interaction model from the constituent to 1) the device collecting the data and minimal feedback and 2) the user interface that provides a highly graphical application for reporting, graphing, and administration. An additional unique attribute of this architecture pattern is the focus of the analytics and data visualization capabilities. The following provides a description for each of the technical capabilities:

- Device – generic term to describe the hardware and software object(s) that primarily collects data from embedded sensors or user input through buttons, touchscreens, or primitive interfaces. A remote sensor can

be connected to a communication device to create a mobile body area network commonly referred to as wearable.

- User Interface – a graphical interface that is designed for constituent use. Often represented as a website and/or mobile app to allow for filtering and reporting of collected data, dashboards, and data visualization.
- Integration Engine – service orchestration, service bus, and interoperability standards mapping
- Privacy and Device Management – policy management and device logging
- Identity and Access Management – authorization and authentication services providing policy enforcement to permit access rules to information and applications
- Data Repository – book of record of structured and unstructured content
- Data Management – data extract, transformation, loading, cleansing, and aggregation
- Data Visualization - ability to provide graphical representation of data in a manner to improve understanding
- Analytics – prescriptive and predictive analysis using advance technology of machine learning, cognitive computing, etc.

Ryu and Song [10] reports that big data analytics in healthcare must be prepared systematically and of good quality. Architecturally, this requires a focus on the fundamental technical capabilities of data repository, data management, data visualization, and analytics as the core aspect of the architecture pattern. The architecture pattern must be capable of handling a wide range of health related datasets that differ widely in their volume, variety, and velocity [13].

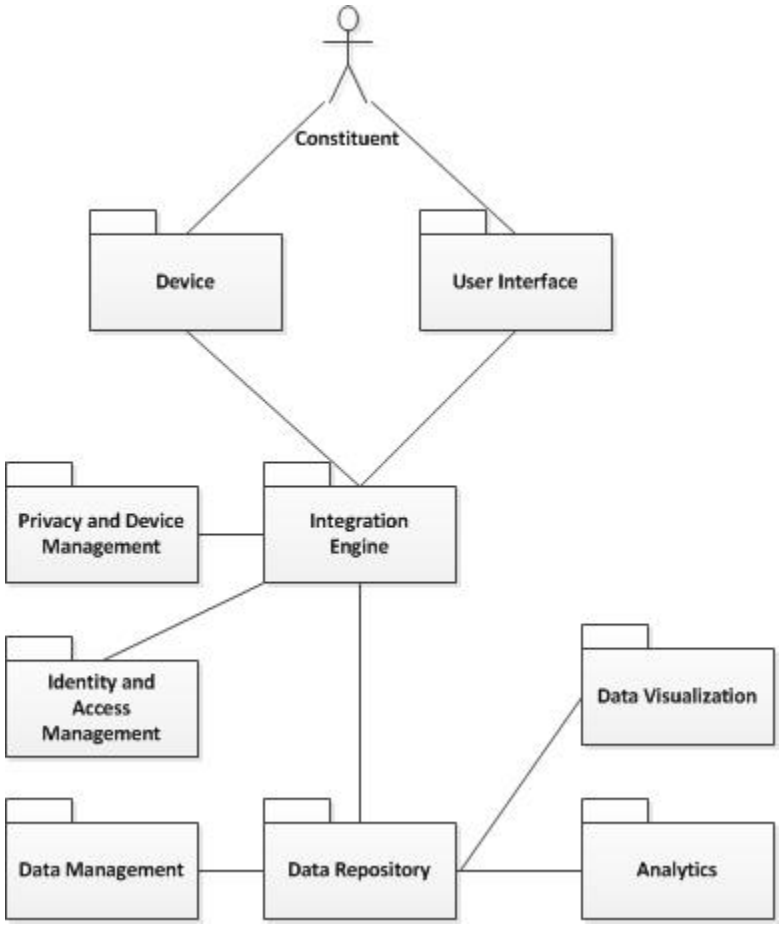

Figure 1. IoT-based Health Monitoring and Management Architecture Pattern

CONCLUSIONS

This paper provides the basis of an architecture pattern to highlight the emerging e-health business needs and the associated technical capabilities. As with any architecture pattern, it requires implementation and continuous refinement and additional definition to establish it as a proven architecture for broad adoption. The authors recognize the multiple facets and complexity of this type of architecture. The authors purposely refrained for addressing the various technology products and implementation approaches which would best be highlighted in a reference architecture versus an architecture pattern. The IoT aspects of this architecture pattern along with the heavy emphasis on analytics provides a uniqueness to this pattern that will particular serve data science solutions.

Further research could explore the concerns regarding the consumer's trust in technology of health related applications which provide guidance and advice. Additionally, the generic analytics technology capability could be further architected to highlight the importance and architectural trade-off analysis for emerging technical capabilities that are associated with business intelligence and advance analytics.

REFERENCES

1. Bass, L., Clements, P. and Kazman, R. 2003. Software Architecture in Practice, Second Edition. Person Education, Inc. Boston MA.
2. Bottles, Kent. 2012. Will the Quantified Self Movement Take Off in Health Care? Technology Today. September/October 2012.
3. Caldwell, Tracey. 2014. The quantified self: a threat to enterprise security? Computer Fraud and Security. November 2014.
4. Chen, Nicholas. 2015. Name Two Transformative Disruptors: If You Answered Digital Revolution and IoT, Two Points. TowersWatson Emphasis 2015.
5. Dalkey, Norman and Helmer, Olaf. 1963. An Experimental Application of the Delphi Method to the Use of Experts. Management Science. 9(3). 458-467.
6. Husain, IItifat and Spence, Des. 2015. Can healthy people benefit from health apps? BMJ. April 14, 2015. BMJ2015:350:h1887.
7. Jara, A. J., Zamora, M. A., Skarmeta, A. F. & G. 2011. An internet of things-based personal device for diabetes therapy management in ambient assisted living (AAL). Personal and Ubiquitous Computing, 15(4), 431-440.
8. Kim, Soo Kim and Garlan, David. 2010. Analyzing Architecture Styles. The Journal of Systems and Software. 83. Pg 1216-1235.
9. Meng, X., Cui, H., and Hua R. 2014. An IoT-based Remote Health Monitoring and Management System. Applied Mechanics and Materials. 571-572. 1176-1179.
10. Ryu, S. and Song. T.M. 2014. Big Data Analysis in Healthcare. Healthcare Informatics Research. October 2014. 20(4). 247-248.
11. Singer, Natasha. 2015. Technology That Prods You to Take Action, Not Just Collect Data. The New York Times. April 19, 2015. http://nyti.ms/1CZ49Fw
12. Swan, M. 2012. Health 2050: The Realization of Personalized Medicine through Crowdsourcing, the Quantified Self, and the Participatory BioCitizen. Journal of Personalized Medicine. 2. 93-118
13. Wang, L., et. al. 2015. Software Tools and Techniques for Big Data Computing in Healthcare Clouds. Future Generation Computer Systems. 43-44. 38-39.
14. Wolf, Gary. 2010. The Data-Driven Life. The New York Times, May 2, online edition. http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?_r=0