Smart healthcare

Challenges and potential solutions using internet of things (IoT) and big data analytics

Sherali Zeadally
College of Communication and Information, University of Kentucky, Lexington, Kentucky, USA

Farhan Siddiqui
Department of Mathematics and Computer Science, Dickinson College, Carlisle, Pennsylvania, USA

Zubair Baig
School of Information Technology, Deakin University, Melbourne, Australia, and

Ahmed Ibrahim
Department of Computer Science, University of Virginia, Charlottesville, Virginia, USA

Received 11 August 2019
Revised 20 August 2019
Accepted 21 August 2019

Abstract

Purpose – The aim of this paper is to identify some of the challenges that need to be addressed to accelerate the deployment and adoption of smart health technologies for ubiquitous healthcare access. The paper also explores how internet of things (IoT) and big data technologies can be combined with smart health to provide better healthcare solutions.

Design/methodology/approach – The authors reviewed the literature to identify the challenges which have slowed down the deployment and adoption of smart health.

Findings – The authors discussed how IoT and big data technologies can be integrated with smart health to address some of the challenges to improve health-care availability, access and costs.

Originality/value – The results of this paper will help health-care designers, professionals and researchers design better health-care information systems.

Keywords Healthcare, Internet of things, Connected health, Smart health, Big data, Digital health, IoT

Paper type Research paper

1. Introduction

Enhancing the quality of health care and improving ease of access to health records while maintaining reasonable costs is challenging for health-care organizations globally (iScoop, 2018). The problem is further exacerbated by the rapidly increasing world population,

The authors thank the anonymous reviewers for their valuable comments which helped improve the content and presentation of this paper.

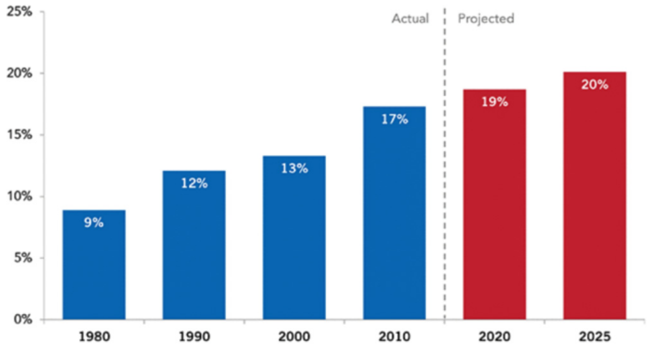
PSU Research Review
Emerald Publishing Limited
2399-1747
DOI 10.1108/PRR-08-2019-0027

especially the rate of increase of senior people (65 years old and higher). According to the World Health Organization (WHO, 2018), the number of senior people will increase to about 1.5 billion by 2050. An aging population implies increase in chronic diseases that require frequent visits to health-care providers, as well as increased hospitalization needs. The rise in the number of patients requiring constant care significantly increases medical treatment costs. For example, in the USA, the cost of health care was about 17.9 per cent of the gross domestic product in 2017 (CMS, 2019) and is expected to hit 19.4 per cent in 2027 (HealthAffairs, 2019). Figure 1 shows the national health-care costs in the USA over a period of about 45 years.

Over the past few decades, Information and Communication Technologies (ICT) have been widely adopted in the health-care environment to make health-care access and delivery easier and most cost-effective. The use of ICT has led to the development of electronic health record (EHR) systems. EHRs contain complete patient health history (current medications, immunizations, laboratory results, current diagnosis, and so on) and can be easily shared among various providers. They have shown to enhance patient-provider interaction (Haluza and Jungwirth, 2014). The adoption of ICT in the health sector is generally referred to as *digital health care* (BroadbandCommission, 2017).

Over the years, digital health care has extended from primarily maintaining electronic patient data and providing patient Web portals, to allowing further flexibility and convenience in health-care management, and is commonly referred to as *connected health* (Loiselle and Ahmed, 2017; IHS, 2015; Cisco, 2019). Connected health uses smart phones and mobile applications, together with wireless technologies (such as Bluetooth, Wi-Fi and long-term evolution) to allow patients to connect readily with their providers without visiting them frequently. For example, a typical hypertensive patient would see his/her doctor once in six months to report daily blood pressure readings. With a monitoring application, the patient can transmit daily or weekly blood pressure readings thereby enabling his/her doctor to detect a problem and intervene earlier.

Connected health has evolved into *smart health* wherein conventional mobile devices (such as smart phones) are used together with wearable medical devices (such as blood pressure monitors, glucometers, smart watches, smart contact lenses, and others) and internet of things (IoT) gadgets (such as implantable or ingestible sensors) to enable continuous patient monitoring and treatment even when patients are at their homes (Uddin *et al.*, 2017; Zilani *et al.*, 2018). Smart health is expected to keep hospitalization expenses low and provide timely treatment for various medical conditions (Sharma *et al.*, 2017) by placing



Source: Peterson (2019)

Figure 1.
National Health Expenditure (percentage of GDP)

IoT sensors on health monitoring equipment. The information collected by these microchips can then be sent to any remote destination (Chaudhury *et al.*, 2017). For example, wearable sensors (such as a temperature sensor and the heartbeat sensor) can act as data collecting units, collecting the physiological signals from the patient's body. The collected data are then forwarded to a local gateway server via a Wi-Fi network such that end-systems (such as a physician's laptop) can retrieve the collected data from the gateway server. Regular server updates allow physicians access to real-time patient data. These devices work together to create a unified medical report that can be accessed by various providers. This data is not only useful for the patient, but can be pooled together to study and predict health-care trends across cultures and countries. Figure 2 illustrates an example of a smart health-care system.

The amount of data that may be generated as a result of combining smart health devices with IoT sensors is massive. Such data are often referred to as "big data." Application of effective analytic technologies to Big Data can help provide meaningful information to physicians which would help them make more timely, informed decisions as well as take proactive measures for better health management (Johri *et al.*, 2017).

1.1 Main contributions of this work

In this paper, we identify technical challenges that are hindering the wide-scale adoption of smart and connected health-care systems. We also discuss how big data and IoT technologies can accelerate the speed at which connected health care can be implemented, deployed and adopted by all health-care stakeholders.

The rest of this paper is organized as follows. In Section 2 we present some of the current challenges to digital health-care adoption. Section 3 discusses how IoT and big data technologies can help promote digital health-care adoption and improve health-care efficiency. Finally, we make some concluding remarks in Section 4.

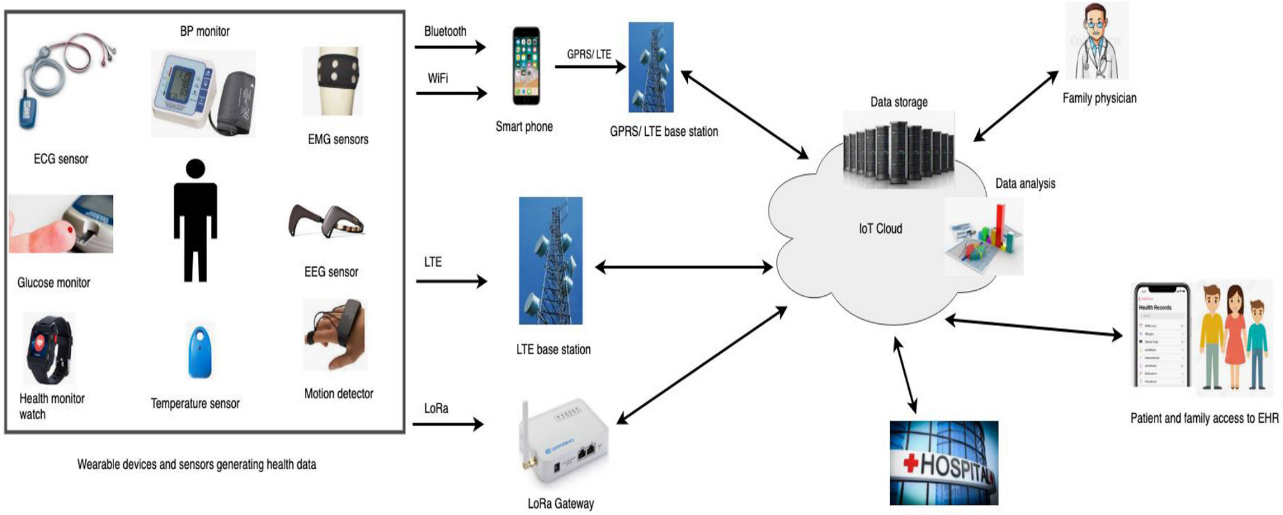
2. Challenges in digital health-care adoption

Digital health-care systems that leverage EHRs and use technologies such as IoT and big data are expected to seamlessly connect patients and providers across diverse health-care systems. These systems are also being increasingly connected via the Internet to various types of medical wearable technologies that are being worn for real-time health-care monitoring. Figure 3 shows the percentage of population (in millions) adopting the medical wearable technology.

However, several challenges need to be addressed before digital health care can develop stable, flexible and interoperable systems. Next we discuss some of the current challenges that are hindering the widespread adoption of digital health care (Firouzi *et al.*, 2018).

2.1 Security and privacy

IoT devices can pose a threat to users' security and privacy. Unauthorized access of IoT devices could create a serious risk to patients' health as well as to their private information (Zeadally *et al.*, 2016). Connected gadgets including medical and mobile devices capture, aggregate, process and transfer medical information to the cloud. The device layer is vulnerable to tag cloning, spoofing, RF jamming, and cloud polling. In cloud polling, traffic is redirected to allow command injections directly into a device through a man-in-the-middle attack. A direct connection attack involves the use of a service discovery protocol such as universal plug and play, or properties of Bluetooth low energy (BLE), to locate and target IoT devices.



ECG: Electrocardiogram
EEG: Electroencephalogram
LTE: Long Term Evolution
LoRa: Long Range

EMG: Electromyography
GPRS: General Packet Radio Service
WiFi: Wireless Fidelity
IoT: Internet of Things

BP: Blood Pressure
EHR: Electronic Health Records

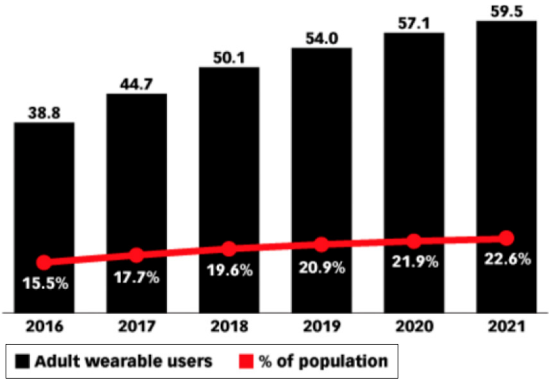
Sources: Gopi and Hwang (2016), Zagan *et al*. (2017), Yang *et al*. (2016)

Figure 2.
A smart health-care system

Denial of service (DoS) attacks can affect health-care systems and affect patient safety. While a common defense to DoS is redundancy (the use of multiple devices on the network), in a health-care environment the duplication of resources may not always be possible because some of the gadgets are implanted life-critical systems. The fast detection of potential security threats remains a challenge because of the number and complexity of emerging software and hardware vulnerabilities. This issue is getting worse as increasing number of devices are being connected to the Internet. Today, default authentication remains prevalent, and insecure Web-based interface access further increases the attack surface. Additionally, we have also seen a surge in the proliferation of wearable devices (including different types of embedded sensors and implanted medical devices) in recent years. The lack of security standards of these devices along with the availability of powerful search engines such as Shodan (2019) which enables locating Internet-connected devices (Williams and McCauley, 2016), make these wearable devices vulnerable to all kinds of attacks (Das *et al.*, 2018).

Recently, many wireless networking technologies have also been deployed in the health-care environment and these include Wi-Fi, BLE and ZigBee that are being used to provide connectivity to different types of medical devices and sensors (Zeadally and Bello, 2019). Security protection of these wireless and sensor technologies against eavesdropping, Sybil attacks, sinkhole attacks, and sleep deprivation attacks must be enforced. Centralized data sets of personal information, family history, electronic medical records and genomic data, should also be protected from hackers and malicious software to enforce security and privacy (Nambiar *et al.*, 2017).

Confidentiality and privacy are important concerns for physicians as well. Patients may not want to share their medical records because of the sensitive nature of the health data (for example, cancer or HIV test results). Concerns exist that the integration of connected technology into current medical information systems may compromise the confidentiality of health data (Sonune *et al.*, 2017). These privacy concerns stem from the fear that digital and connected technology may attract hackers. Furthermore, researchers sometimes argue that connected health technology would be implemented imperfectly, allowing for security vulnerabilities to be exploited (Poyner and Sherratt, 2018). Privacy concerns increase when the patient's information is shared among several applications. Low security and misconfigured device and network settings could affect the privacy of patients and their



Source: eMarketer (2017)

Figure 3.
US adult wearable users and market penetration, 2016-2021 (millions and percentage of population)

data. Additional risks arise because of linking geographical location with purchases from pharmacies which may provide a profile of an individual's health status. Another concern is the use of various providers which are mandated to submit confidential data to law enforcement agencies. This can affect the adoption and use of the technology where patients are concerned about privacy. The networks which transmit data are often highly heterogeneous and are frequently managed by third parties which makes the protection of security and privacy as well as governance of this data even more challenging (Williams and McCauley, 2016).

2.2 Inter-realm authentication and interoperability issues

Inter-realm authentication is essential for entities operating in different domains to establish trust for carrying out digital health transactions. Shibboleth is a federated identity solution that facilitates entity authentication both within and between organizational systems (Shibboleth, 2019). At a country level, Shibboleth, a system that provides inter-realm authentication has been deployed and tested successfully. A typical Shibboleth-based system enables a user of a digital health system to authenticate itself to an identity provider (IdP), and subsequently sends a service request for a service hosted on a service provider (SP). The IdP and SP share the user's identity information in the background. Through such a federated arrangement, Shibboleth facilitates single sign-on capabilities for digital health entities as in (eHealth, 2019).

Shibboleth-based systems are secure and provide strong authentication across multiple realms of a digital health system. However, not all digital health systems have Shibboleth implementations owing to the lack of facilities to host separate Identity and Service Providers in an organization within a nation, and to have these hosted across all similar digital health organizations. The lack of information technology (IT) skills and necessary funding especially in the third world, hinders the ready adoption of systems such as Shibboleth.

Another aspect that requires attention as a prevailing digital health issue for nations is the lack of interoperability between nations intending to cooperate on digital health ICT infrastructures. This shortcoming is due to not only the limited ICT infrastructures or dearth of IT skills, but also the lack of policy for global cooperation among nations on the exchange of sensitive medical data, which would facilitate telemedicine and provisioning of high-quality medical care remotely.

Projects such as Liberty Alliance (Broda, 2007) have fostered bringing together disparate platforms and standards for inter-realm authentication under one umbrella. These platforms and standards are: OpenID, inames, Openliberty, World Wide Web Consortium, Organization for the Advancement of Structured Information Standards (OASIS) and Liberty Alliance Project. The proposal of the Liberty Alliance Project aims to enable interoperability between standards at the Internet Identity Layer. They have also highlighted the need for collaboration among various stakeholders through public forums and certification programs.

The lack of interoperability among the heterogeneous platforms and standards that exist for inter-realm authentication is identified as a potential vulnerability that could lead to loss of data privacy, compliance regulation issues, as well as backward compatibility with legacy systems. The Liberty Alliance Project also identified that open technology standards, deployment policy guidance and independent third party certification are essential for enabling inter-realm authentication. The lack of proper standards for facilitating seamless digital health transactions among multiple domains, which may span several continents, restricted the widespread adoption of digital health especially in countries where network bandwidths were barely sufficient. Consequently, digital health applications of telemedicine and of patient data sharing across multiple domains have remained restricted. Inter-judicial boundaries have impeded ready acceptance of standards and policies for data sharing across geographies. The case study of Catalan digital health system (catCert, 2017) provides a good example of a federated authentication system that does the following:

- Authentication of medical doctors against hospital systems is achieved by using a user ID and a password or an X.509 digital certificate.
- Hospitals send a Security Assertion Markup Language (SAML) (SAML, 2019) assertion to Catalan health services for each new prescription.
- Pharmacies use X.509 digital certificates or user credentials (ID/password) to authenticate against the Catalan Council of Pharmacies database.
- For dispensing new medicines, the Catalan Council of Pharmacies sends an SAML assertion to Catalan Health Services, to give access to pending ePrescriptions.
- ePrescriptions are also to be signed by the doctors and dispensed medicines are reported to the Catalan Health Service.

The presence of a centralized Certification Authority (CA) for the issuance of X.509 digital certificates enables both encryption as well as digital signing of patient prescriptions. In addition, the presence of a SAML backend system facilitates the sharing of authentication data between federated digital health systems. The SAML architecture (Oasis, 2005) allows making statements on user attributes and authorizations for authenticated entities. Examples of such attributes include medical or financial data. It provides context to the operation being carried out, details on how an authentication transaction is conducted, the type of transaction being carried out and details on the user, including mechanisms used for his or her authentication. However, some of the shortcomings of SAML are:

- The level of confidentiality of digital health attribute assertions is entirely dependent on the strength of the cipher being used.
- Targeted confidential messages cannot be crafted unless a holistic certification mechanism is in place to issue and maintain public-private key pairs to facilitate data encryption and decryption.
- Anonymity of subjects is not the same as pseudonymity. Consequently, the ability of the SAML-based digital health authentication system to ensure that users remain anonymous, is restricted, because of the limitation of the SAML standard.
- The original SAML specification is vulnerable to collusion-based attacks, wherein two or more malicious system entities cooperate to share information exchanged from previous transactions, and consequently compromise the confidentiality of messages exchanged.

Recent implementations of federated identification and authentication based on SAML include the presence of a CA to facilitate public key-based data encryption and/or data integrity verification. However, the scope of verification of an entity's identity will only be limited to within the zone covered by the CA. In particular, a digital health system that relies on the presence of a CA within a geographical bound such as city or state limits, will not be able to provide authentication services for other entities outside the CA bounds.

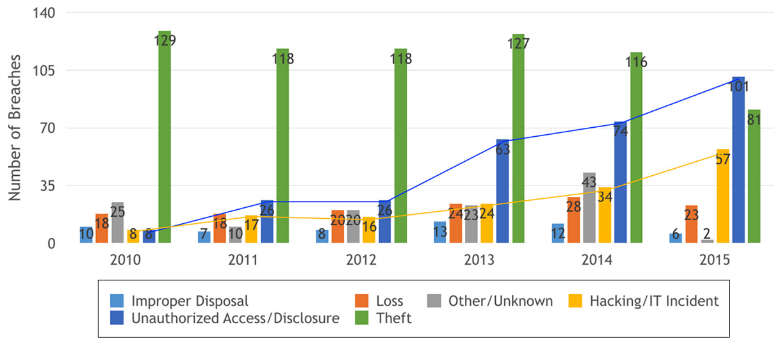
2.3 Health information exchange barriers

Health Information Exchange (HIE) enhances health-care delivery by providing the ability to electronically share health-care information among diverse health-care organizations in a reliable and secure manner. Currently, HIE is implemented by using one of the following methods: consumer-mediated exchange, directed exchange, and query-based exchange (Williams *et al.*, 2012).

Consumer-mediated exchange provides patients with access to their own electronic records, thus allowing them to track their health conditions, determine whether there is erroneous billing or medical data, and update their self-reports. Directed exchange is conducted when a health-care organization transfers such vital information such as laboratory test results and medication dosage to other specialists involved in the care of the same patient. Query-based exchange usually occurs in unplanned medical care when a health-care organization needs the previous health records of a new patient. This is done by requesting access to these records through the HIE system.

Impediments in the deployment of HIE systems are mainly owing to security and privacy concerns. Some of the issues associated with current HIE systems are as follows: First, abuse of access rights by authorized insiders (Szerejko, 2015). This usually happens when health-care organizations share medical records of their patients with unauthorized individuals, either out of irresponsibility, for personal reasons, or in exchange for some kind of gain. For instance, medical records of celebrities and politicians frequently leak out of Healthcare Information Management Systems (HIMSs) into the media. Second, violation of rules by unauthorized insiders, who may have access to the system itself but not to the records (Strauss *et al.*, 2015). For instance, hospital employees who do not provide direct patient care or former employees who have not yet been electronically restricted from data retrieval. The former group can use the existing access to hack the private informational database while the latter may decide to seek vengeance on their former employers by undermining the HIMS's security. Third, unauthorized intruder attempts to enter the system either by attacking it directly or by pretending to be part of the health-care team (Saiz *et al.*, 2014). Figure 4 shows the increase in the number of breaches according to "Unauthorized Access/Disclosure" and "Hacking/IT Incident" between 2010 and 2015 according to the numbers published by the United States Department of Health and Human Services (DHHS) (US DHHS, 2019).

The emergence of health care-related cybercrime is a major concern and an emerging threat to HIMSs (Agha, 2015). Security breaches in hospitals can cost them as much as $7 million in terms of damaged reputation, fines, litigation and so on (Claunch and McMillan, 2013). Major breaches have occurred in organizations such as Anthem, CareFirst, Premera and UCLA Health systems. As a result, a total of 143 million patient records were exploited



Source: US DHHS (2019)

Figure 4.
Number of breaches between 2010 and 2015 according to the DHHS

by cyberattacks, which amounted to 45 per cent of the American population (iSheriff, 2015) as shown in Figure 5.

A cyber security assessment by the Healthcare Information and Management Systems Society in 2015 showed that in the previous 12 months, 64 per cent of health-care organizations had been exposed to external cyberattacks (Mohammed *et al.*, 2015). Bloomer News claimed that in the previous 2 years, of all health-care organizations, 90 per cent have been attacked (Pettypiece, 2015). Furthermore, most data breaches occur in health-care and medical industries as compared to financial, governmental, or educational sectors (Gleeson and Friel, 2013).

2.4 Device communication

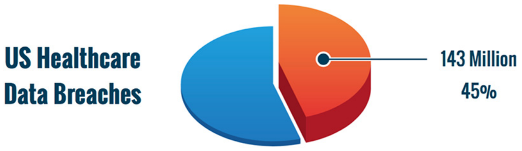
One of the major challenges to implementing smart or connected health is communication. Many devices now have sensors to collect data and they often communicate with the server in their own language. Each manufacturer has its own proprietary protocol, which means sensors made by different manufacturers cannot necessarily communicate with each other. This fragmented software environment, coupled with privacy concerns, frequently isolates valuable information on data islands, undermining the main idea behind IoT (Dimitrov, 2016).

The presence of several devices also opens up concerns related to connecting medical devices using wireless network technologies. For instance, people using a Wireless Personal Area Network (WPAN)-enabled device are expected to move freely but mobility can result in collisions when WPANs that operate in similar frequency channel are within close range. Collision in WPANs has several disruptive effects because it reduces performance and may lead to disastrous situations especially when health-care delivery is concerned. Therefore, it is essential to make sure that medical devices operate properly when connected using various types of wireless communication technologies (Gawanmeh, 2016).

Smart health systems are not always easy to use by physicians. The presence of a large number of features could sometimes make a system complex which in turn demotivates health-care workers in learning how to use it (Grood *et al.*, 2016).

Users and service providers both require interoperability within individual IoT domains and amongst themselves. This creates complex challenges because the various disciplines captured by IoT are regulated by a diverse group of regulatory agencies. This complexity is further exacerbated in connected health scenarios wherein medical standards require particularly strict regulations. Companies that want to build smart health applications in the medical area must consider the regulations imposed by Food and Drug Administration, the Centers for Medicare and Medicaid Services, and the Federal Communications Commission (FCC) (Firouzi *et al.*, 2018).

A truly interoperable connected health system is one in which data flows with both one-to-one and one-to-many connections, leading to the exchange of information among multiple interfaces which require systems to cooperate with one another. In health-care



Source: iSheriff (2015)

Figure 5. Total number of patient records breached between 2009 and 2015 by cyberattacks according to DHHS

environments, it is important for devices to be compatible with many transmission formats and protocols for authentication and encryption. Device management will require directories of devices' functionality, protocols, terminologies and standards compliance. The level of "plug and play" interoperability now commonplace in non-health areas remains a challenge for medical devices (Williams and McCauley, 2016).

2.5 Collection and management of data

Digital health care that leverages IoT sensor devices faces several data management challenges. The data originates from medical sensors, which are worn or implanted inside the human body. Because the state of the human body is constantly changing, there is a continuous influx of data that is being produced. Furthermore, the captured data are heterogeneous (consisting of various data formats). For example, Electro Cardio Graph (ECG) data are often encoded in XML format, while data received from camera-based IoT devices is typically recorded in a wide variety of image formats. A connected health scenario consists of heterogeneous connected components including user devices, networks, systems (with large data volumes), variety and velocity (collected from various sources), and veracity (uncertain data). Digital health systems need to be designed using suitable data-driven learning techniques to handle its continuously varying cyber-physical components. Proper analysis of data can give valuable information about patients' health conditions. When a lot of patients' data are not analyzed and knowledge is not extracted from it, we do not reap the maximum usefulness of this data, and its collection also wastes computing resources. Over the past decade, various data analysis tools have been developed by researchers, pharmaceutical companies, and health-care providers (Nambiar *et al.*, 2017) to enable the fast extraction of useful knowledge from patients' data. Several challenges exist because of the absence of standardized data collection formats as well as the volume and velocity of data generated in health-care settings. Integrity is also crucial with respect to big data. Inaccurate data can lead to incorrect decisions and long term strategic planning. Because health-care data often comes from various sources, robust authentication systems are needed to ensure that health-care data are submitted from actual registered clinics, hospitals, and medical institutions (Tse *et al.*, 2018).

Collecting data that is clean, formatted, thorough, and precise in a health-care system is challenging (Anagnostopoulos *et al.*, 2016). In addition, health-care definitions are complex and metrics are constantly changing in the health-care industry. For example, the length of stay (LOS) metric is a key financial measure that is also reported by clinicians. The LOS definitions can vary and decisions can be skewed if users either do not know which metric to use or do not know the definition of the metric that was reported. Clinicians calculate LOS by how long a patient physically stays in the bed. But from a financial perspective, LOS is calculated on a 24-hour scale that ends at midnight. As a result of the discrepancy in LOS definitions, the data recorded could be incorrectly interpreted (Burke, 2015).

The complexity of data in the health-care industry makes integrating big data challenging. While some information, such as health variables, have to be updated frequently, more passive information such as geographic location and contact information need not be updated that often. Data integrity should be maintained while updating information. Inappropriate document control may pose a risk to data integrity. Maintaining these databases is challenging because of the costs of maintenance as well as HIPAA regulations (Hipaa, 2019) rules.

2.6 Design and implementation based on multi-disciplinary knowledge

Digital health (including connected and smart health) is developed using expertise in many fields including embedded systems, network design, data analytics and bioengineering. The design and implementation of such a heterogeneous system requires extensive knowledge in multi-disciplinary areas. The system also needs to evolve continuously to address constantly changing needs. For example, currently there is limited integration of smart health systems with some medical systems such as ultrasound and CAT scan imaging.

3. Improving the adoption of digital health care with internet of things and big data technologies

In this section, we discuss some of the ways in which IoT and big data can together help improve the adoption of smart health which will result in improved health-care delivery and access.

3.1 Evidence-based care

The exponential increase in the volume of health-care data generated by IoT devices makes data processing very challenging. Big data can provide evidence-based care by aggregating data sets from diverse sources. Analysis of data can provide useful insights into detecting anomalies and providing appropriate treatments to patients. Intelligent analysis using new methods can provide substantial financial savings on the order of several hundred billion dollars, which amounts to about 8 per cent of the national health expenses (Olaronke and Oluwaseun, 2016).

The study of health-related information with efficient methods promotes early identification of disease patterns, which expands public health surveillance. This ensures that appropriate and timely decisions on the treatment of a particular disease are taken thereby reducing patient mortality. Big data enhances the type of care patients receive as treatment decisions are based upon knowledge gathered from analyzing large data sets.

3.2 Self-learning and self-improvement

IoT sensors enable data collection, but IoT alone cannot provide rehabilitation treatments. Accurate and timely treatments can be made based on fast patient evaluation, and the development of rehabilitation procedures corresponding to the medical investigation. Many factors need to be considered to provide a precise treatment. Computer tools merely rely on the data collected by the sensors and past case studies, while self-learning techniques can adaptively analyze and recommend new treatment options. A few self-learning algorithms [including artificial neural network (ANN), genetic algorithms (GA), ant colony optimization (ACO) and simulated annealing (SA)], are suitable for data analysis and mining. Topology-based and ontology-based heuristic algorithms can help in finding optimal solutions for a large-scale health-care system (Yuehong *et al.*, 2016).

Various distributed computing platforms are being used today for big data analytics. These platforms include Apache Samza, Apache Spark, Hadoop MapReduce, Apache Storm and Flink. Hadoop MapReduce and Apache Spark are the most widely used platforms for massive data storage and analysis (Praveena and Bharathi, 2017). Hadoop is an easy to use open-source tool for handling big data applications. The Hadoop MapReduce framework provides a major distributed computing platform that is capable of storing and processing large amounts of unstructured data sets (Khan and Iqbal, 2017).

MapReduce (Merla and Liang, 2017) is a programming environment that permits parallel and distributed processing on huge amounts of data on large clusters of hardware. Hive (Garg, 2015) is the structured query language (SQL)-like bridges that permit predictable business applications to run SQL queries against a Hadoop cluster. PIG (Jain and Mayrya, 2017) is a tool that makes Hadoop more usable by making MapReduce queries simpler to implement. Wibidata (Moorthy *et al.*, 2014) is a tool that integrates Hadoop with Web analytics to optimize data usage by websites. It is a platform that automatically maps user's queries to Hadoop jobs. Rapidminer (Dwivedi *et al.*, 2016) provides an integrated platform for analytics (both business and predictive), mining of data and machine learning.

3.3 Standardization

Various organizations (such as IEEE, IETF, ITU-T) have contributed to the deployment and standardization of IoT technologies. The standardization of IoT (Stuurman and Kamara, 2016) (Singh *et al.*, 2017) was mostly influenced by the recommendations provided by the Machine-to-Machine European Telecommunications Standards Institute (ETSI) and Internet Engineering Task Force (IETF) Working Groups. All new and emerging ideas should be integrated to form a global solution that helps build standardizations for the future Internet. Based on the results provided by the CERP-IoT project (IERC, 2016), future Internet is an extension of the existing one by integrating general things into wider networks. The standardization will enable the development of IoT-based health-care systems. Table I lists various standardization bodies and some of their recent IoT standards related work.

3.4 Privacy and security

IoT-based systems are useful as long as its users remain safe. In IoT systems, all types of data collection and mining are performed over the Internet. Thus, personal data can be accessed at various stages (during collection, transmission and so on). Patients' safety should be taken into consideration by preventing any form of tracking or illegal identification. The higher the level of autonomy and intelligence of the IoT devices, the harder the protection of identities and privacy becomes. IoT-based applications are also vulnerable because of wireless communication which makes eavesdropping easier. Additionally, IoT devices generally have low energy and low computing power which makes it harder to implement complex algorithms to guarantee security. As big data becomes more ubiquitous in the health-care system, more security challenges will emerge. Rigorous research is needed to ensure privacy, trust, and security throughout the health-care environment.

3.5 Interactive reporting and visualization

Big data applications need to distinguish between analysis and reports (Suyts *et al.*, 2017). Big data applications will not succeed if data are simply written to reports. Applications

Table I. Standards organizations and IoT-related work

Organization	Recent IoT standards work
Institute of Electrical and Electronics Engineers (IEEE) (IEEE, 2019)	Telecommunications and information exchange between systems (IEEE-802.15.4, 2013) Medical device communication (IEEE-1073-10103, 2012) Adoption of Smart Energy Profile 2.0 Application Protocol Standard (IEEE 2030.5, 2013)
Internet Engineering Task Force (IETF) (IETF, 2019)	Energy-efficient features of Internet of Things protocols (Gomez *et al.*, 2018) Securing smart object networks (Sethi *et al.*, 2018)
ITU-T (ITU, 2019)	Reference architectures for smart manufacturing, digital health, and wearable device communications. (ITU-T, 2018)
ETSI (ETSI, 2019)	Reference architectures for smart body area networks and health-care interoperability (ETSI TR 103 394, 2018)
Open Connectivity Foundation (OCF) (OCF, 2019)	Cloud security (OCF-Security, 2019)

Challenges	Solutions
Big data analysis	Use of efficient data analysis tools and intelligent learning algorithms such as ANN, genetic algorithms GA, ACO and SA
Standardization of protocols	Creation of standards for IoT such as those created by the IETF and ETSI
Security and privacy	Implementation of lightweight cryptographic algorithms that can be implemented on resource-constrained IoT devices connected via low-energy networks Protection of data during capture, storage, and transit Develop password enforcement policies, secure pairing protocols, and secure transmission mechanisms Design of new and improved key sharing mechanisms for implementing symmetric key encryption
Effective information reporting	Statistical reporting methods should be adopted instead of using traditional reporting techniques

Table II. Digital health-care adoption: challenges and solutions

need to derive valuable insights from a bulk of data and only mention specific highlights (intelliPaat, 2019). It is also necessary to train algorithms to generate precise insights based on available data without which the credibility of the report comes into question. Reports can be made appealing and useful by including graphs and statistical information. Applications should also focus on developing visualizations that would make it easy to derive insights from a report and allow easy identification of trends and challenges in a health-care segment.

As discussed above, there are several challenges that still need to be addressed before digital health care can be widely adopted. Table II summarizes some of these challenges together with possible solutions.

4. Conclusion

We are currently witnessing rapid advances in information communication technologies. It is a well-known fact that the implementation and deployment of these technologies in the health-care sector bring about significant benefits (affordable health care, cost-efficient health services, and many others) to all health-care stakeholders. In this work, we discussed some of the major impediments that are slowing down digital health-care adoption nationally and internationally along with some possible solutions to enable faster digital health-care deployment. While the health-care sector is increasingly interested in leveraging IoT and big data technologies to become more efficient, there are several challenges that need to be addressed before digital health care can become a widespread reality.

Note

1. *In this paper we will use the terms digital health, connected health and smart health interchangeably.

References

Agha, L. (2015), "The effects of health information technology on the costs and quality of medical care", *Journal of Health Economics*, Vol. 34, pp. 19-30, available at: www.sciencedirect.com/science/article/pii/S0167629613001720

Anagnostopoulos, I., Zeadally, S. and Exposito, E. (2016), "Handling big data: research challenges and future directions", *Journal of Supercomputing*, Vol. 72 No. 4, pp. 1494-1516.

BroadbandCommission (2017), "Digital health: a call for government leadership and cooperation between ICT and health", available at: www.broadbandcommission.org/Documents/publications/WorkingGroupHealthReport-2017.pdf (accessed August 2019).

Broda (2007), *Managing Trust in e-Health with Federated Identity Management*, eHealth Workshop, Konolfingen.

Burke, J. (2015), "Is that data valid? Getting accurate financial data in healthcare", *Health Catalyst*, available at: www.healthcatalyst.com/financial-data-in-healthcare-edw (accessed August 2019).

catCert (2017), "Identity and capability management in eHealth: the CATCert approach", available at: www.projectliberty.org/liberty/content/download/3691/24338/file/071011%20I%20Alamillo%20CATCert%20v1r0%20case%20study.pdf (accessed August 2019).

Chaudhury, S., Paul, D., Mukherjee, R. and Haldar, S. (2017), "Internet of thing based HealthCare monitoring system", *The 8th IEEE Annual Conference on Industrial Automation and Electromechanical Engineering, Bangkok*.

Cisco (2019), "Making connected health a reality", Cisco Systems, available at: www.cisco.com/c/dam/en_us/solutions/industries/docs/healthcare/connected_health_brochure.pdf (accessed August 2019).

Claunch, D. and McMillan, M. (2013), "Determining the right level for your IT security investment", *Healthcare Financial Management*, Vol. 67 No. 5, pp. 100-104.

CMS (2019), "National health expenditure data", Centers for Medicare and Medicaid Services, available at: www.cms.gov/ (accessed August 2019).

Das, A.K., Zeadally, S. and He, D. (2018), "Taxonomy and analysis of security protocols for internet of things", *Future Generation Computer Systems*, Vol. 89, pp. 110-125.

Dimitrov, D.V. (2016), "Medical internet of things and big data in healthcare", *Healthcare Informatics Research*, Vol. 22 No. 3, pp. 156-163, available at: www. ncbi.nlm.nih.gov/pmc/articles/PMC4981575/

Dwivedi, S., Kasliwal, P. and Soni, S. (2016), "Comprehensive study of data analytics tools (RapidMiner, Weka, R tool, Knime)", *IEEE Symposium on Colossal Data Analysis and Networking (CDAN), Indore*.

eHealth (2019), "Cookbook identity and authorization management", available at: www.ehealth.fgov.be/ehealthplatform/nl/search?q=i.am%20overview&filter=&doctype%5BCookbook%5D=on&page=1&filter%5Bbase_services%5D=on

eMarketer (2017), "Wearables still far from mass adoption", available at: www.emarketer.com/content/wearables-still-far-from-mass-adoption (accessed August 2019).

ETSI TR 103 394 (2018), "Smart body area networks (SmartBAN); system description", available at: www.etsi.org/committee/1413-smartban (accessed August 2019).

ETSI (2019), "European telecommunications standards institute", available at: www.etsi.org/ (accessed August 2019).

Firouzi, F., Farahani, B., Ibrahim, M. and Chakrabarty, K. (2018), "From EDA to IoT eHealth: promise, challenges, and solutions", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 37 No. 12, pp. 2965-2978.

Garg, V. (2015), "Optimization of multiple queries for big data with Apache Hadoop/Hive", *IEEE International Conference on Computational Intelligence and Communication Networks, Jabalpur*.

Gawanmeh, A. (2016), "Open issues in reliability, safety, and efficiency of connected health", *First IEEE Conference on Connected Health: Applications, Systems and Engineering Technologies, Washington, DC*.

Gleeson, D. and Friel, S. (2013), "Emerging threats to public health from regional trade agreements", *The Lancet*, Vol. 381 No. 9876, pp. 1507-1509.

Gomez, C., Tian, H., Cao, Z. and Kovatsch, M. (2018), "Energy-efficient features of internet of things protocols", IETF draft, available at: https://tools.ietf.org/id/draft-ietf-lwig-energy-efficient-08.html (accessed August 2019).

Gopi, P. and Hwang, T. (2016), "BSN-care: a secure IoT-based modern healthcare system using body sensor network", *IEEE Sensors Journal*, Vol. 16 No. 5, pp. 1368-1376.

Grood, C., Raissi, A., Kwon, Y. and Santana, M.J. (2016), "Adoption of e-health technology by physicians: a scoping review", *Journal of Multi-Disciplinary Health*, Vol. 9, p. 335, available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC4975159/

Haluza, D. and Jungwirth, D. (2014), "ICT and the future of healthcare: aspects of doctor-patient communication", *International Journal of Technology Assessment in Health Care*, Vol. 30 No. 3.

HealthAffairs (2019), "National health expenditure projections, 2018–27: economic and demographic trends drive spending and enrollment growth", available at: www.healthaffairs.org/doi/full/10.1377/hlthaff.2018.05499 (accessed August 2019).

Hipaa (2019), "Health information privacy", available at: www.hhs.gov/hipaa/index.html (accessed August 2019).

IEEE 2030.5 (2013), "Adoption of smart energy profile 2.0 application protocol standard", available at: https://standards.ieee.org/standard/2030_5-2013.html (accessed August 2019).

IEEE (2019), "The world's largest technical professional organization for the advancement of technology", available at: www.ieee.org/ (accessed August 2019).

IEEE-1073-10103 (2012), "Health informatics–point-of-care medical device communication", available at: https://standards.ieee.org/standard/11073-10103-2012.html (accessed August 2019).

IEEE-802.15.4 (2013), "IEEE standard for local and metropolitan area networks – part 15.4: Low-Rate wireless personal area networks (LR-WPANs)", https://standards.ieee.org/standard/802_15_4j-2013.html (accessed August 2019).

IERC (2016), "IoT European Research Center", available at: www.internet-of-things-research.eu/ (accessed August 2019).

IETF (2019), "Internet engineering task force", available at: www.ietf.org/ (accessed August 2019).

IHS (2015), "The connected patient", available at: https://cdn.ihs.com/www/pdf/Technology-White-Paper-The-Connected-Patient.pdf (accessed August 2019).

intelliPaat (2019), "What is data analytics", available at: https://intellipaat.com/blog/what-is-data-analytics/ (accessed August 2019).

iScoop (2018), "Healthcare in digital transformation: digital and connected healthcare", available at: www.i-scoop.eu/digital-transformation/healthcare-industry/ (accessed August 2019).

iSheriff (2015), "The new heathcare crisis: cybercrime, patient records and information security", White Paper.

ITU (2019), "ITU telecommunication standardization sector", available at: www.itu.int/en/ITU-T/Pages/default.aspx (accessed August 2019).

ITU-T (2018), "Series Y: global information infrastructure, internet protocol, aspects, next-generation networks, internet of things and smart cities", available at: www.itu.int (accessed August 2019).

Jain, P. and Mayrya, J.P. (2017), "Comparative analysis using hive and pig on consumers data", *International Journal of Computer Science and Information Technologies*, Vol. 8, No. 2, pp. 285-291.

Johri, P., Singh, T., Das, S. and Anand, S. (2017), "Vitality of big data analytics in healthcare department", *IEEE International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)*, *Dubai*.

Khan, M. and Iqbal, N. (2017), "Computational performance analysis of cluster-based technologies for big data analytics", *The IEEE International Conference on Internet of Things (iThings)*, *IEEE, Exeter*, pp. 280-286.

Loiselle, C.G. and Ahmed, S. (2017), "Is connected health contributing to a healthier population?", *Journal of Medical Internet Research*, Vol. 19 No. 11, p. e386.

Merla, P. and Liang, Y. (2017), "Data analysis using Hadoop MapReduce environment", *IEEE International Conference on Big Data*, *Boston, MA*.

Mohammed, D., Mriani, R. and Mohammed, S. (2015), "Cybersecurity challenges and compliance issues within the US healthcare sector", *International Journal of Business and Social Research*, Vol. 5 No. 2, pp. 55-66.

Moorthy, M., Baby, R. and Senthamaraiselvi, S. (2014), "An analysis for big data and its technologies", *International Journal of Computer Science Engineering and Technology*, Vol. 4 No. 12.

Nambiar, A.R., Reddy, N. and Dutta, D. (2017), "Connected health: opportunities and challenges", *IEEE International Conference on Big Data*, *IEEE*, *Boston, MA*, pp. 1658-1662.

Oasis (2005), "Security and privacy considerations for the OASIS security assertion markup language (SAML) V2.0", OASIS Standard.

OCF (2019), "Open connectivity foundation", available at: https://openconnectivity.org/ (accessed August 2019).

OCF-Security (2019), "Cloud security specification", available at: https://openconnectivity.org/draftspecs/Essen/CR%202871%20-%20OCF_Cloud_Security_Specification.pdf (accessed August 2019).

Olaronke, I. and Oluwaseun, O. (2016), "Big data in healthcare: prospects, challenges and resolutions", *Future Technologies Conference*, *IEEE*, *San Francisco, CA*, pp. 1152-1157.

Peterson, P.G. (2019), "Growing healthcare costs in the US", Peter G. Peterson Foundation, available at: www.pgpf.org/chart-archive/0056_health-care-costs-proj (accessed August 2019).

Pettypiece, S. (2015), "Rising cyber attacks costing health system $6 billion annually", available at: www.bloomberg.com/news/articles/2015-05-07/rising-cyberattacks-costing-health-system-6-billion-annually (accessed August 2019).

Poyner, I.K. and Sherratt, R.S. (2018), "Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people", *IET Living in the Internet of Things: Cybersecurity of the IoT*, *London*.

Praveena, M.A. and Bharathi, B. (2017), "A survey paper on big data analytics", *IEEE International Conference on Information, Communication, and Embedded Systems*, *Chennai*.

Saiz, C.P., Markina, I.C., Yarza, A.A., López, M.R. and Eizaguirre, L.E. (2014), "Disclosure of health information: a challenge of trust between the various sectors involved", *Revista Latina de Comunicacíon Social*, Vol. 69, p. 125.

SAML (2019), "SAML", available at: http://saml.xml.org (accessed August 2019).

Sethi, M., Arkko, J. and Back, H.M. (2018), "Practical considerations and implementation experiences in securing smart object networks", IETF RFC, available at: https://tools.ietf.org/html/rfc8387 (accessed August 2019).

Sharma, S., Tripathi, M.M. and Mishra, V.M. (2017), "Survey paper on sensors for body area network in health care", *The IEEE International Conference in Emerging Trends in Computing and Communication Technologies (ICETCCT)*.

Shibboleth (2019), available at. www.internet2.edu/products-services/trust-identity/shibboleth/ Accessed: August 2019.

Shodan (2019), available at: www.shodan.io/ (accessed August 2019).

Singh, V.P., Dwarakanath, V.T., Haribabu, P. and Babu, N.S.C. (2017), "IoT standardization efforts — an analysis", *IEEE International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, *Bangalore*.

Sonune, S., Kalbande, D., Yeole, A. and Oak, S. (2017), "Issues in IoT healthcare platforms: a critical study and review", *IEEE International Conference on Intelligent Computing and Control (I2C2)*, *Coimbatore*.

Strauss, A.T., Martinez, D.A., Garcia-Arce, A., Taylor, S., Mateja, C., Fabri, P.J. and Zayas-Castro, J.L. (2015), "A user needs assessment to inform health information exchange design and implementation", *BMC Medical Informatics and Decision Making*, Vol. 15 No. 1, pp. 1-11, available at: http://dx.doi.org/10.1186/s12911-015-0207-x

Stuurman, K. and Kamara, I. (2016), "IoT standardization – the approach in the field of data protection as a model for ensuring compliance of IoT applications?", *4th IEEE International Conference on Future Internet of Things and Cloud Workshops*, *Vienna*.

Suyts, V.P., Shadrin, A.S. and Leonov, P.Y. (2017), "The analysis of big data and the accuracy of financial reports", *5th International Conference on Future Internet of Things and Cloud Workshops, Prague*.

Szerejko, J.D. (2015), "Reading between the lines of electronic health records: the health information technology for economic and clinical health act and its implications for health care fraud and information security", *Connecticut Law Review*, Vol. 47 No. 4.

Tse, D., Chow, C.K., Ly, T.P., Tong, C.Y. and Tam, K.W. (2018), "The challenges of big data governance in healthcare", *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, New York, NY*.

Uddin, M.S., Alam, J.B. and Banu, S. (2017), "Real time patient monitoring system based on internet of things", *4th IEEE International Conference on Advances in Electrical Engineering, Dhaka*.

US DHHS (2019), "US department of health and human services, breach portal: notice to the secretary of HHS breach of unsecured protected health information", available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed August 2019).

WHO (2018), "Global health and aging", World Health Organization, 2011, available at: www.who.int/ (accessed August 2018).

Williams, C., Mostashari, F., Mertz, K., Hogin, E. and Atwal, P. (2012), "From the office of the national coordinator: the strategy for advancing the exchange of health information", *Health Affairs*, Vol. 31 No. 3, pp. 527-536, available at: http://content.healthaffairs.org/content/31/3/527.abstract

Williams, P.A. and McCauley, V. (2016), "Always connected: the security challenges of the healthcare internet of things", *3rd IEEE World Forum on the Internet of Things, Reston, VA*.

Yang, Z., Zhou, Q., Lei, L., Zheng, K. and Xiang, W. (2016), "An IoT-cloud based wearable ECG monitoring system for smart healthcare", *Journal of Medical Systems*, Vol. 40 No. 12, p. 286.

Yuehong, Y.I.N., Zeng, Y., Chen, X. and Fan, Y. (2016), "The internet of things in healthcare: an overview", *Journal of Industrial Information Integration*, Vol. 1, pp. 3-13.

Zagan, I., Gaitan, V.G., Petrariu, A.I. and Brezulianu, A. (2017), "Healthcare IoT m-green CARDIO remote cardiac monitoring system – concept, theory of operation and implementation", *Advances in Electrical and Computer Engineering Journal*, Vol. 17 No. 2, pp. 23-31.

Zeadally, S. and Bello, O. (2019), "Harnessing the power of internet of things based connectivity to improve healthcare", *Internet of Things*, p. 100074, available at: https://doi.org/10.1016/j.iot.2019.100074

Zeadally, S., Isaac, J.T. and Baig, Z. (2016), "Security attacks and solutions in electronic health (E-health) systems", *Journal of Medical Systems*, Vol. 40 No. 12, p. 263.

Zilani, K.A., Yeasmin, R., Zubair, K.A., Sammir, M.R. and Sabrin, S. (2018), "R^{3}HMS, an IoT based approach for patient health monitoring", *IEEE International Conference on Computer, Communication, Chemical, Material and Electronic Engineering, Rajshahi*.

Further reading

Cloudera (2019), "Platfora", available at: www.cloudera.com/partners/solutions/platfora.html (accessed August 2019).

Corresponding author

Sherali Zeadally can be contacted at: szeadally@uky.edu