Big Data and IoT for U-healthcare Security

Mechelle Grace Zaragoza, Haeng-Kon Kim and Roger Y. Lee

Abstract Big Data is a latest topic of interest by many researchers because of its big potential applied in many areas of science and technology. Big Data is by far captivating strong roots in the healthcare ecosystem, but this healthcare data are becoming more complex, which are challenging to solve using common database management tools or simply the traditional data processing application along with the security systems. On the other hand, IoT remainds you to track your health like fitness devices, calorie meters, heart rate monitors, to name a few up to your fridge reminding you that it is basically running out of water." Big Data and IoT are built on networks and cloud computing of gathering data using sensors but challenges using both especially the security for health care is very vital. IoT and Big Data have the potential to transform the way healthcare providers use sophisticated technologies from their clinical and other data repositories and make informed decisions, but without the right security and encryption solution, Big Data and IoT can mean big problems, especially on healthcare security systems. In this study, we discuss the use and application of IoT and Big Data for u-health care. We have presented this architecture to address the mentioned challenges in this study. Data privacy of patient and user data is a critical requirement. The architecture will access controls to medical device data. The patient should be in control of what is being viewed by whom and will allow him/her to view and set the access control policies, maintaining anonymity and masking of data wherever possible.

Keywords U-health care · IoT · Big Data · Security systems

M.G. Zaragoza · H.-K. Kim (✉)
Catholic University of Daegu, Gyeongsan, South Korea
e-mail: hangkon@cu.ac.kr

M.G. Zaragoza
e-mail: mechellezaragoza@gmail.com

R.Y. Lee
Central Michigan University, Mount Pleasant, USA

R. Lee (ed.), *Computer and Information Science*, Studies in Computational Intelligence 719, DOI 10.1007/978-3-319-60170-0_1

1 Introduction

We live in a communication era where we use the latest technology in everything we do, especially in health care every single day. Numbers of health care-related devices are spreading over to meet the needs of patients or simply for those who are health conscious.

That is one of the main draws of using massive amounts of data, but unfortunately, Big Data and many of the platforms that use it were not designed to address security concerns. If organizations want to ensure their data are secured, they will need to see to it on their own by building those features themselves. If these problems are solved, clinical institutes will be in a better position to truly take advantage of all that Big Data has to offer [1].

2 Background of the Study

As the cost of medical expenses continues to rise, hospitals, clinics, and healthcare institutions can no longer give free hospitalization charges.

The consequence of rising costs increases the penetration of a successful career, which has minimized the provision of unnecessary care, while given the care that is necessary. However, with these even managed situations for patient care, redundant things get to happen, while other effective interventions do not get carried out in part because the number of possible beneficial things to accomplish physicians cannot efficiently keep track of these things. In order to manage this all, an information system must be presented to manage utilization and improve efficiency, quality, and most especially the security of this healthcare system [2].

3 Problem Discussion

IoT is built on networks and cloud computing of gathering data using sensors but challenges using IoT especially the security for health care is very vital. IoT and Big Data have the potential to transform the way healthcare providers use sophisticated technologies from their clinical and other data repositories and make informed decisions, but without the right security and encryption solution, Big Data and IoT can mean big problems especially on healthcare security systems. In this study, we discuss the use and application of IoT and Big Data for u-health care. We have presented this architecture to address the mentioned challenges in this study. Data privacy of patient and user data is a critical requirement. The architecture will access controls to medical device data. The patient should be in control of what is being viewed by whom and will allow him/her to view and set the access control policies, maintaining anonymity and masking of data wherever possible.

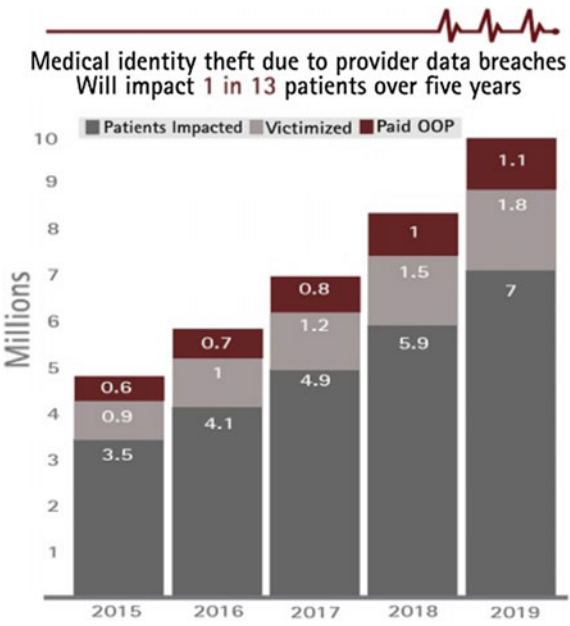

Fig. 1 Average cyber-attacks report from Accenture

3.1 Security Threats

Figure 1 explains that cyber-attacks in the next 5 years will cost US health systems $305 billion in cumulative lifetime revenue. As Accenture approximates that one in 13 patients—roughly 25 million people—will have personal information, like their social security or financial records, stolen from technology systems in the next 5 years. "What most health systems don't realize is that many patients will suffer personal financial loss as a result of cyber-attacks on medical information," by Kaveh Safavi, CHICAGO; Oct. 14, 2015—[3].

4 Understanding Health Care

In order to understand what health care really is, let us see the history of prior to 1960 of unrelated events rather than a modernized organized effort. Healthcare systems across the globe are focusing on policy in improving the quality of health care delivered. In contrast, let us first see the healthcare quality improvement in earlier time periods from a series of unrelated incidents and its developments.

Table 1 represents the chronological history of health care [4].

Table 1 History of healthcare quality

Chronological summary of key tipping points, individuals by year			
Year(s)	Key tipping points	Key individuals responsible	Country of origin
1854	Quality improvement documentation	Nightingale	England
1861	Sanitary commissions	Barton	USA
1862, 1918	Improvisation and innovation	Pasteur, Blue	France, USA
1879	Sterilization	Chamberland	France
1895, 1956, 1960	Technology	Rontgen, Safar, Laerdal	Germany, USA, France, Norway
1910	Education	Flexner	USA
1881–1955	Pharmaceuticals	Pasteur, von Behring, Kitasato, Descombey, Salk, Kendrick, Eldering Pittman, Fleming	France, Germany Japan, USA, England
1883–1945	Healthcare financing	Bismark, Beveridge, Kaiser	Germany, England, USA
1908	The role of industry and mass production	Ford	USA

4.1 Obama Healthcare Law

4.1.1 Why Do We Need to Care

In November 1, 2016, the enrollment started for this Obama Health Care Reform Bill. This was the former President Barack Obama's reforms in the healthcare industry as this expands the Medicaid and Medicare providing the most affordable insurance to low-to-middle income Americans. The bill is called Obama Care, which includes many provisions that focus on expanding quality, affordable healthcare coverage helping millions of Americans. Obama's plan for healthcare reform outlined what would be in the current Obama healthcare law [5].

But as of now, Americans are already seeing the results: a historic expansion of health care, with costs now growing at the slowest rate in 50 years. Healthcare reform changed the course of history in America. It has been a goal for presidents and progressive leaders since the days of Teddy Roosevelt. Today, finally, no American can be discriminated against because of a preexisting condition. This is how important health care is. As one of the most powerful countries needs improvement to its health care, we believe that we could still improve a lot of things to make health care more beneficial in the community [6].

4.1.2 US to HER Security

As Electronic health record security is concerned, data distribution and its extremely sensitive nature of healthcare information must be protected. The implementation of a very effective security and privacy control must be considered as personal healthcare records are almost digitized. According to guidance issued by the US Department of Health and Human Services in December 2008, the US government is providing incentives to its people to get all healthcare providers using EHR by 2015 in which protected by reasonable administrative, technical, and physical safeguards. It is expected that the adoption of electronic health records will allow up to $100 billion to be saved in healthcare expenditure over a 10-year period, according to research group RAND [7].

5 Internet of Things for Medical Devices (IoT-MD)

The number of increasing sensors used by medical devices, remote, and continuous monitoring of a patient's health is becoming promising. This network of sensors, actuators, and other mobile communication devices, referred to as the Internet of Things for Medical Devices (IoT-MD), is composed to revolutionize the functioning of the healthcare industry.

IoT-MD simply provides a setting in which patient's vital parameters get transmitted by some medical devices through an access point going to a secure cloud-based platform as a storage medium, aggregated and analyzed.

This cloud-based platform is simply the storage of millions of patients and performs analysis in real time, ultimately promoting an evidence-based medicine system [8].

5.1 IoT

How IoT is fast approaching and speeding up its usage in the future?

Figure 2 projects the evolution of interconnected devices in the near future. The existence of IoT is to basically enable all things to be "smart" in a way that things should be connected anytime, anyplace, with anything, and anyone ideally using any path/network and any service. These objects make themselves recognizable to other devices intended to it, and they obtain intelligence by making or enabling context-related decisions. It will serve as a communication device to transmit information about them [9].

As of now, saying that securing properly Internet of Things is a little late but as the IoT increases in diversity and complexity, solutions in resolving these issues

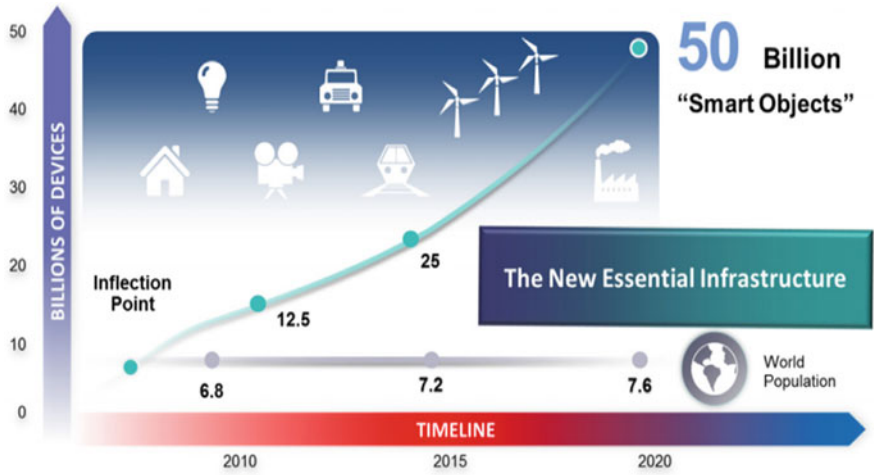

Fig. 2 Interconnected devices and the future of evolution (Cisco 2011)

may not as difficult as we think it is. Technology is growing and progressing that security experts are barely keeping up as it is. The main problem about this increasing number of interconnected devices is mainly the security unless major advances are made to adopt a "security first" idea, as the Internet of Things may always be a risky attempt [10].

6 How Big Is Big Data Is It?

6.1 The 3Vs of Big Data

Big Data has 3 specific areas: Volume, Variety, and Velocity. This is like dealing with massive amounts of data, from all kinds of sources, in all kinds of forms. Traditional BI relies on the so-called structured data which is usually arranged in columns and rows, with every field corresponding to some known source. Big Data is often completely unstructured, as it needs to have a developer to create some kind of mechanism for interpreting the information.

Velocity is defined as the extra capacity you get with distributed processing can also dramatically accelerate computing. Velocity as described in the 3v's of Big Data is the extra capacity you get with distributed processing as velocity is the measure of how fast data is coming in [11].

Figure 3 displays the concept of Big Data was first defined in 2001 by Doug Laney, who specified 3Vs for Big Data: Volume, Velocity, and Variety in his paper titled "3D Data Management: Controlling Data Volume, Velocity and Variety." Shows the 3Vs to describe and explain Big Data in today's era [12] (Figs. 3 and 4).

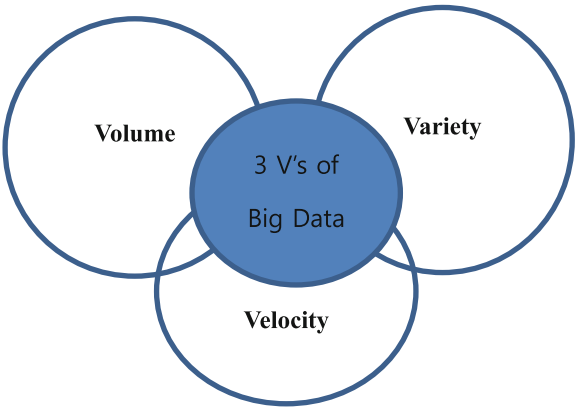

Fig. 3 **a** Volume: Massive amount of data generated at an unprecedented pace, **b** Velocity: the speed at which the data are created, transformed, stored, analyzed, and visualized, **c** Variety: various types of data in structured, unstructured, and semi-structured formats

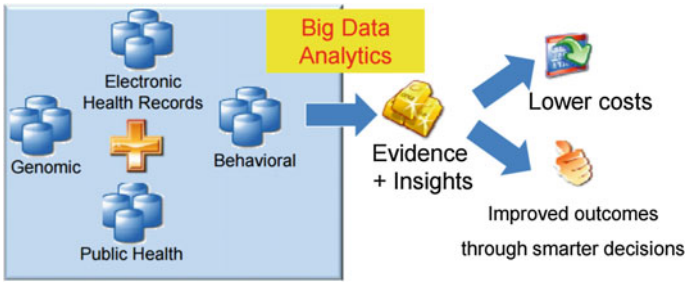

Fig. 4 Overall goals of big data (analytics) in healthcare

In a broader view, it takes advantage of the amounts of data and provides right intervention to the right patient at the right time. It could also be a personalized care to the patient, benefiting the overall components of a healthcare system such as provider, payer, patient, and management [13].

6.2 Challenges and Opportunities in Big Data

Major concern is the privacy issue. We know some computer programs that could readily erase all the details stored and being transported into a larger databases, but stakeholders should be aware about the potential threats these data might become public in the future. Big Data adaptation has the potential to transform health care [14].

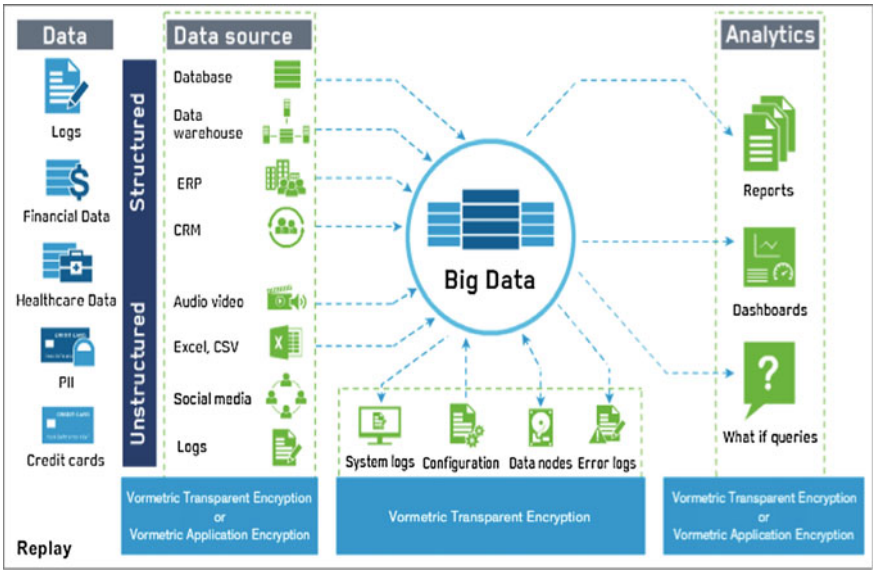

Fig. 5 Securing Big Data environments with vormetric

6.3 Big Data Analytics

As discussed before, Big Data is a collection of large and complex data sets which are hard to process using common database management tools or traditional data processing applications.

As Fig. 5, shows vormetric solutions for Big Data security enable organizations to make use of the benefits of Big Data analytics [15].

7 Discussion

Healthcare data is becoming more complex. Big data analytics have the potential to transform the way healthcare providers use sophisticated technologies to gain insight from their clinical and other data repositories and make informed decisions.

In the future, we will appreciate the widespread implementation and use of Big Data analytics across the healthcare organization, with that several challenges that were mentioned must be addressed. Big Data analytics became too mainstream by this time [16].

Figure 6 shows how a typical IoT hospital revolutionizes as technology and time progress in the field of medicine. Hospitals have started the process of paper-based

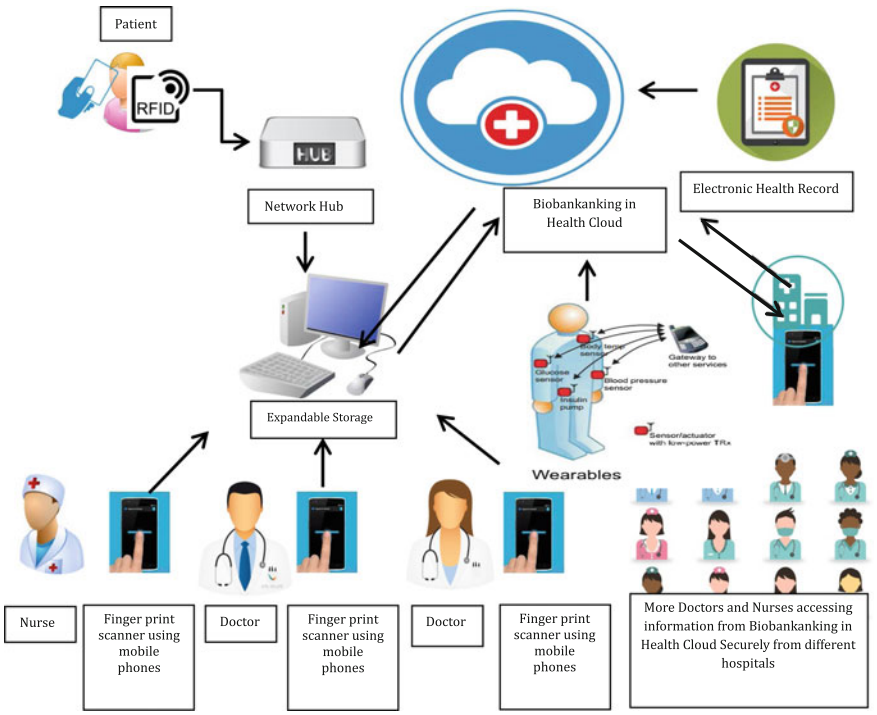

Fig. 6 A proposed secured Internet of Things (IoT) in a single hospital connected to more hospitals in accessing patients' data based on (HIR) Healthcare Informatics Research

medical records to EHR from a traditional writing of a patient's health record. A patient diagnosed with diabetes will have its ID provided to be scanned by the RFID scanner that is connected to the secure biobanking health cloud which stores the (EHR) electronic records of the patient. The mobile app (specific health app for hospital records) will ensure that doctors or the nurses could only see ad retrieve the records stored in biobanking. To do his, the program will have to ensure the doctor's data are already stored in the program as well as the time inputted and in the near future, the records being collected in a specific field provided for example (patient name, birth date, or diagnosis). This proposed architecture is possible, though IoT and Big Data. This will ensure that the most sensitive data being disseminated are safe. That those who can only access are the authorized persons listed on the system.

This may seem very basic, as we try to expand the cloud capacity to store the needed information to be distributed, this will create more advances and privacy-wise useful in the field of medicine [17].

8 Conclusion and Future Works

Health care paved its way to be more successful as technology proved its existence to make our lives as laid-back as possible, but the advantages depict that there would always be a disadvantages.

Information security and privacy in the healthcare sector are both critical issues they need to be addressed. As to keeping and securing the records of the patients, one should consider the other goal of u-heathcare systems. That is to not only provide the best treatment a patient should deserve, but the overall treatment of the patient including their hospital records. To solve these issues, the proposed secured Internet of Things (IoT) in a single hospital connected to more hospitals in accessing patients' data based on (HIR) Healthcare Informatics Research and its attributes, we have presented this architecture to address the mentioned challenges in this study. Data privacy of patient and user data is a critical requirement. The architecture will access controls to medical device data. The patient should be in control of what is being viewed by whom and will allow him/her to view and set the access control policies, maintaining anonymity and masking of data wherever possible. In future work, we intend to elaborate the information security (a proposed secured Internet of Things (IoT) in a single hospital) in order to make it useful as a tool in providing security and privacy of health data to a more secured and efficient health care.

Acknowledgements This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the C-ITRC (Convergence Information Technology Research Center) support program (IITP-2016-H8601-15-1007) supervised by the IITP (Institute for Information & Communication Technology Promotion).

This research was supported by the International Research & Development Program of the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and Future Planning (Grant Number: K 2014075112).

References

1. Buckley, J.: 7 Big Data Security Concerns. Qubole, 7 May 2015
2. Bates, D.W., Kuperman, G.J., Wang, S., Gandhi, T., Kittler, A., Volk, L., Spurr, C., Khorasani, R., Tanasijevic, M., Middleton, B.: Ten commandments for effective clinical decision support: making the practice of evidence-based medicine a reality. J. Am. Med. Inf. Assoc. **10**(6), 523–530 (2003)
3. Cyberattacks Will Cost U.S. Health Systems $305 Billion Over Five Years, Accenture Forecasts, 14 Oct 2015
4. Sheingold, B.H., Hahn, J.A.: The history of healthcare quality: the first 100 years 1860–1960. Int. J. Afr. Nurs. Sci. **1**, 18–22 (2014)
5. ObamaCare Facts: Facts on the Affordable Care Act. http://obamacarefacts.com/obama-health-care-bill/
6. Health care reform is helping millions of Americans get better health care. That's worth fighting for. https://www.barackobama.com/obamacare/
7. Howarth, F.: Security challenges in the US healthcare sector, Bloor Research, A white paper, December 2010

8. Khanna, A., Misra, P.: The Internet of Things for Medical Devices—Prospects, Challenges and the Way Forward, A white paper
9. Vermesan, O., Friess, P.: Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems
10. Ar. Amster: Internet of Things: Big Data and Data Security Problems, 27 Apr 2016
11. Junk, D.: Big Data vs Traditional Approaches to Enterprise Reporting. http://blog.apterainc.com/business-intelligence/big-data-vs-traditional-approaches-to-enterprise-reporting. Accessed 18 Sept 2015
12. Shan, T.: Big Data 3Vs, Leading by Game-Changing Cloud, Big Data and IoT Innovations, 10 Oct 2013
13. Sun, J., Reddy, C.K.: Big Data Analytics for Healthcare. https://www.siam.org/meetings/sdm13/sun.pdf
14. Kayyali, B., Knott, D., Kuiken, S.V.: The big-data revolution in US health care: accelerating value and innovation
15. BIG DATA SECURITY Vormetric Data Security Use Cases. https://www.vormetric.com/data-security-solutions/use-cases/big-data-security
16. Raghupathi, W., Raghupathi, V.: Big data analytics in healthcare: promise and potential. J. Health Inf. Sci. Syst.
17. Dimitrov, D.V.: Medical internet of things and big data in healthcare. Health Inf. Res. **22**(3), 156–163 (2016)