

Security Threats and Recommendation in IoT Healthcare

Cansu Eken, Hanım Eken

Computer Science, Ankara University, Turkey, cansueken21@gmail.com
Türksat,Turkey,eken.hanim@gmail.com

Abstract

The Internet of Things (IoT) devices have become popular in recent year. All devices connect network and communicate each other. Therefore all devices become smart. They are used for some systems such as e-Health, e-Energy, e-Home, smart city, smart car etc. IoT device collect data for systems in order to analyze data and give right decision. Thus, attackers attack IoT systems. This paper gives an introduction to IoT healthcare systems and applications, the related security and privacy challenges. This paper tends to analyze the security threats in different layers of the IoT, and give recommendation owing to provide security and privacy.

Keywords: internet of things (IoT), body area network, wearable devices, IoT healthcare systems, security of IoT, privacy, information security

1 Introduction

In recent years, many devices and goods are used in life and these devices and goods communicate with each other. These devices are radio-frequency identification (RFID) tags, mobile phones, mobile devices, sensors, actuators, etc. The term “Internet-of-Things” (IoT) is broadly used to refer to physical objects or “things” connect each other and exchange data on network. The term, internet of things (IoT) was first proposed in 1998 (Weber, 2010).

In the year of 2005, International Telecommunication Union (ITU) released an annual report on “Internet of Things. This report includes the development of information and communication technology and the future of smart devices, communicating with each other (ITU, 2005). Physical objects or “things” become smart by connecting to each other. In later years, physical objects or “things” in every aspect of our lives connect to internet and exchange to data. Therefore, “Internet-of-Things” (IoT) devices are used many sectors.

According to Gartner, Inc., there will be nearly 26 billion devices on the Internet of Things by 2020. Figure 1 presents a list of countries by IoT devices online per 100 inhabitants as published by the OECD in 2015.

Rank	Country	Devices online	Relative size
1	South Korea	37.9	
2	Denmark	32.7	
3	Switzerland	29.0	
4	United States	24.9	
5	Netherlands	24.7	
6	Germany	22.4	
7	Sweden	21.9	
8	Spain	19.9	
9	France	17.6	
10	Portugal	16.2	
11	Belgium	15.6	
12	United Kingdom	13.0	
13	Canada	11.6	
14	Italy	10.2	
15	Brazil	9.2	
16	Japan	8.2	
17	Australia	7.9	
18	Mexico	6.8	
19	Poland	6.3	
20	China	6.2	
21	Colombia	6.1	
22	Russia	4.9	
23	Turkey	2.3	
24	India	0.6	

Figure 1. IoT devices online per 100 in 2015.

In particular, sensors are used many different fields due to the development of sensor technology. Environmental sensing that could use urban planning, electricity, energy management, transportation system and intelligent shopping systems. Biological sensors could use healthcare and medicine systems (Atamli and Martin, 2014).

Table 1. Field of IoT application.

Field of Application	Application
Energy	Smart devices, Energy Management system, Energy Control system
Smart Home	Fire alarm system, Safety control system, Building Automation system
Environmental Monitoring	Air Pollution, Noise Monitoring, Waterways, Industry Monitoring
Green Agriculture	Green Houses, Compost, Irrigation Management, Soil Moisture Management
Retail & Logistics	Supply Chain Control, Intelligent Shopping Applications, Smart Product Management, Item Tracking, Fleet Tracking
Smart Transportation	vehicular communication, smart traffic control, smart parking, electronic toll collection systems
E-Health	Patient monitoring, Doctor tracking, Personnel tracking, Real-time patient health status monitoring, Home health care

IoT devices have important role due to development of healthcare systems. Healthcare quality is improved with IoT devices such as biological sensors.

In addition, IoT devices are used different fields such as media, production, smart home, smart city, transportation, etc. Table 1 demonstrates field of IoT applications.

1.1 Environmental monitoring

Internet of Things is important for environmental analysis and monitoring in order to ensure environmental protection and control. Sensors are used due to measure the air, water, soil pollution. Internet of Things devices diffuse a large geographic area and collect data from large area.

In addition, Internet of Things applications provide that the checks of use of environmental resources. These applications are used to analysis environmental pollution and make right decision about using of environmental resources (Lee and Lee, 2015).

1.2 Infrastructure management

Urban and rural infrastructure management is important for countries. Therefore, every country has applications due to monitor and control dam, road, bridge, railway tracks, subway, and other critical infrastructure (Jayavardhana et al., 2013). Internet of Things (IoT) devices can be used to monitor and operate events or changes in structural conditions that can compromise safety and increase risk.

Furthermore, Internet of Things (IoT) applications are used for providing access to ships transition from bridge, measure and control the density of road vehicles, check dams' occupancy rate etc. They have big role to coordinate between different service providers and users in critical infrastructure in order to ensure cost effective and time schedule maintenance and repair. Usages of IoT devices provide improving the quality of service like incident management and emergency response (Michael et al., 2014).

1.3 Building, home automation and energy management

Devices has become smart with connect internet. So, systems used in buildings and houses began to be automated. People have become control devices in their home remotely. These smart devices are television, heater, air conditioning, and fridge in the home. Smart buildings include Fire alarm system, Safety control system, Building Automation system, Energy Management system, Energy Control system, Central, Control and monitoring system, Contact communication systems, Centralized information sharing service (Shrouf and Miragliotta, 2015).

Home automation systems, like other building automation systems, are typically used to control lighting, heating, ventilation, air conditioning, appliances, communication systems, entertainment and home security devices to improve convenience, comfort, energy efficiency, and security.

1.4 Transportation

IoT devices are important for transportation. They are used for control transport system. Application of the IoT extends to all aspects of transportation systems. All smart system is communicating each other in order to provide high quality transportation services. Smart transportation services are smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance (Alvi et al., 2015).

1.5 Medical and healthcare systems

The developments of health technology are presenting new opportunities and facilities in order to improve healthcare sectors. In these days, healthcare system use sensors, mobile devices. Internet of Things (IoT) devices are used all parts of healthcare systems. Figure 2 shows sensors in the healthcare.

They are used for remote health monitoring and emergency notification systems. Monitoring system can enable patient monitoring for chronic issues, checkups, blood pressure and heart rate monitors and unnecessary appointments (Lubecke et al., 2014)

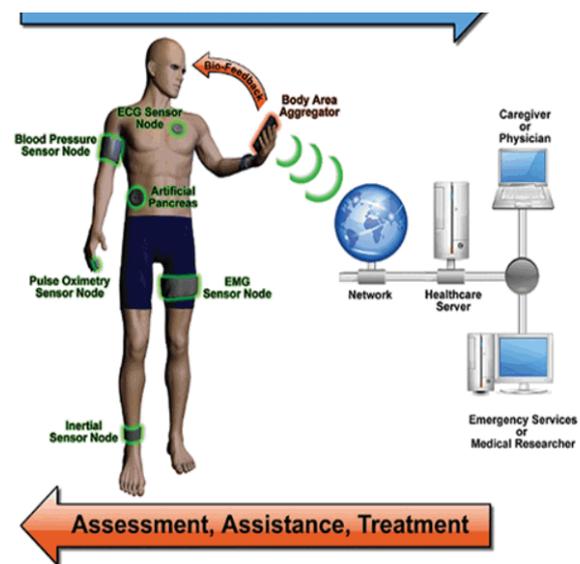


Figure 2. Sensors in the healthcare.

2 Related Work

There are many articles covering security of Internet of Things (IoT) devices in healthcare systems. Nguyen et al. (2015) define the security requirement for highly interconnected network of heterogeneous devices in Internet of Things (IoT). Kai et al. (2013) propound security and privacy methods for Health Internet of Things in order to protect patients' healthcare data. Neisse et al. (2015) propose a Model based Security Toolkit due to the control and protection of user data from Internet of Things (IoT).

Hamdi and Abie (2014) propose a game based model for security eHealth applications in the Internet of Things (IoT). They use security effectiveness and energyefficiency methods for evaluating security strategies.

3 Threats of IoT Health Applications

IoT devices are important for health applications. IoT devices collect measurable and analyzable healthcare data in order to facilitate the work healthcare applications. Therefore, security of IoT healthcare applications is important for healthcare systems. IoT devices are threatened by many security vulnerabilities. I give details about these vulnerabilities in this part of article.

3.1 Energy Optimization

Sensors are significant devices for healthcare systems. Measurable and analyzable healthcare data are gathered very easily with the development of sensor technology. In recent years, wearable devices are very popular for healthcare systems. Wearable devices could collect many healthcare data without disturbing patients. However, energy consuming is important problem for wearable devices. Because wearable devices are small and they are used to collect data form people body. They collect healthcare data from body continuously. Battery is not enough to collect and send health data to healthcare applications. In addition, battery of wearable devices is necessary to be constantly charge. These are serious problems for IoT devices in healthcare systems (Decuir, 2015).

3.2 Privacy

Privacy has many definitions in the literature. Privacy is important topic for information security at healthcare system in the world. Hence, many international organizations define privacy. The Organization for Economic Cooperation and Development (OECD) defines it as "any information relating to an identified or identifiable individual (data subject)" (Chen and Zhao, 2012).

Healthcare data are collected from IoT devices. These devices gather data by remote access mechanisms which have some challenging about privacy and security. Data collected by the sensor is transmitted to the database or cloud over internet. In addition, IoT devices connect internet and communicate with each other from the Internet. Security vulnerabilities on Internet and IoT devices are threatened health data. Additionally, healthcare data are collected from different health units. Health data is shared by various health units. Every unit must provide privacy of data. Because healthcare data includes essential significant information. All the world's attackers all the world's attackers want to capture health data. Thereof, privacy of data must be protected (Thilakanathan et al., 2013).

3.3 Trust

Trust management is important for IoT devices and applications due to provide security and privacy of data. Because all devices connect network and send data to applications. Therefore, devices on the internet must be trusted due to ensure privacy and security. Attackers could connect device IoT applications in order to manipulate data (Skarmeta et al., 2014).

Data collection trust is serious issue because of huge volumes of data are collected from devices. Big data is used by IoT health application owing to make right decision about patients and improve quality of healthcare. Moreover, IoT health care services include data process, analysis and mining. Attackers could be damaged big data with create damage or malicious input of IoT devices. Hence, researchers study about challenges of trust management in IoT. Trust management in IoT must implement network layer and application layer (Abomhara and Køien, 2004).

3.4 Denial-of-service attacks (DoS)

Denial-of-service attacks (DoS) are to make IoT devices and IoT applications cannot provide service. IoT devices connect network and transfer data and communicate with each other. IoT applications need to connect to network and receive data from these devices. Denial-of-service attacks (DoS) dangerous attacks for IoT applications because of machine or network resource. IoT devices have low memory capabilities and limited bandwidth, battery, and disk space. Hence, they are affected from Denial-of-service attacks (DoS) easily (Abomhara and Køien, 2004).

3.5 Physical attacks

Physical security is serious issue for IoT devices because of gathering data from of unprotected

environment. Further, IoT devices are small devices and they are integrated TVs, cars, air conditioning, ovens etc. Therefore, these devices could be stolen easily or changed configured settings. Attackers can change data sent by IoT devices. IoT devices are exposed many physical attacks such as a secret stealing, software manipulation, and hardware tampering.

3.6 Data Manipulation

Data is important IoT healthcare applications. Data is used all steps of healthcare systems. Thus, attacks are against to data security and privacy. Attacks are stealing data, data manipulation and damaging data. Health data is important and sensitive data for all country in the world because of including personally identifiable data. Data is used multiple paths in the IoT. These are IoT devices (data generator, data receiver, and aggregation point), the internet (multi-directional data transport), the cloud (data stored), the machine (application services, big data repositories, analytic) (Bing et al., 2011)

Attackers steal health data for malicious use and they damage victims. They steal data when data is generated and transported by IoT devices. Attackers manipulate or change data in order to redirect victims what attackers want. Doctors could give wrong decision about diagnosis and treatment because of data manipulation. In addition data loss is serious problem for IoT health application.

4 Security Solution of IoT Health Applications

Security is important IoT health applications because of sensitive health data privacy. This section classifies security solution in order to protect data from attacks. Figure 3 represents data security in IoT healthcare applications.



Figure 3. Data security in IoT healthcare applications.

Access Control is important step in protecting IoT healthcare applications and health data. Well-designed access control must be implemented IoT healthcare applications and devices. IoT devices collect health data from patients and transfer health data to healthcare databases. Hence, IoT healthcare applications must have strong access management in order to ensure healthcare data security and privacy. Through access control systems, an organization can restrict and monitor the use of critical data, and protect privacy and security (Rush Carskadden, 2013).

In addition, employers in healthcare should have the awareness of information security owing to provide security of IoT healthcare applications and health data. Information security awareness training should be given to healthcare staff members. Furthermore, employees should receive all training about access control of priority for ensuring data security, privacy, and patient rights.

Access management in IoT healthcare applications protects to misuse healthcare data and perform malicious attacks on the users' healthcare data.

IoT health devices are tiny and integrated other systems. IoT health devices collect data from various environments. Hence, physical security is significant topic for IoT health devices. IoT health devices should be secure against physical threats (Shen and Liu, 2011).

Physical security of IoT health devices and health data involves protection against environmental threats, accidents, physical sabotage, and theft. IoT health devices should have replacement devices for protecting physical attacks. In this way, IoT health devices keep on collecting and transferring data. Countermeasures should be taken to decrease the damage and recover from attacks, accidents and disaster quickly.

Network security is important issue for IoT health devices and applications. All IoT devices connect to network and communicate each other over network. Therefore, network is required in all steps in the IoT health applications'. Some technologies are WiFi, Bluetooth, Zigbee, RFID etc. Especially, wireless body area network (WBAN) is used to data collect from wearable devices.

Firewalls, IPS, IDS, ingress/egress filtering structures, internet protocol security (IPsec), secure Sockets Layer/Transport Layer Security (SSL/TSL) should be used in order to ensure network security. HTTPS is used for application to encrypt to message (Sadeghi et al., 2015; Xingmei et al., 2013). Data privacy is major issue for IoT health devices and applications because of the ubiquitous character of the IoT environment. IoT health devices connected each other and send data. Strong encryption algorithm is used for data. Data must be encrypted and sent IoT application over a secure network. RFID technology is used for IoT devices to send data. However, RFID has

some security vulnerabilities such as reverse engineering, eavesdropping, man-in-the-middle attack, spoofing etc. When data is sent by RFID technology, some security measures are taken owing to provide privacy protection (Xingmei and Jing, 2013).

Besides, IoT health application should have strong access control management and trust management services due to ensure data security and privacy. Health data is collected from IoT health devices then share various health units. Healthcare data is used accurate assessment and right decision about patient treatment and diagnosis. IoT healthcare application must have “need-to-know” principle for authorization management (Weinberg et al., 2015).

Policies, standards and guidelines could be developed, documented, and implemented. Further, many standards about security of healthcare are published by international organizations. These documents are used for on account of providing security and privacy. Each employee and department should have enough information about procedures, guidelines, and standards related to data security and privacy. They could be reviewed and update regularly and change according to the needs of the healthcare sector (Weinberg et al., 2015). Trainings should be prepared owing to improve information security awareness of healthcare staff. These trainings give details about fundamental security and risk IoT healthcare applications and emphasize about privacy of health data. These trainings could be provided to employees regularly (Weinberg et al., 2015).

All IoT healthcare devices, IoT healthcare applications and network components’ log must be collected with central log management systems. Logs are monitored, analyzed and evaluated so as to prevent unwanted events to healthcare systems. Besides, central log management or security information and event management (SIEM) must have auditing to ensure security. Undesirable events must be reported security team quickly to interfere unwanted events. Central log management or security information and event management (SIEM) must have strong authentication and authorization to monitor the audit log. The log should be checked continuously.

Unfortunately, auditing is a passive defense because of becoming aware of critical security event after the occurrence of the event. Auditing help people to response to unwanted-event quickly.

5 Conclusions

IoT devices are very important for systems. Today, many systems have become smart with IoT devices. These systems include big data. IoT devices collect data for these systems. Data is sensitive because of including personal information. Hence, these systems

have many threats about data security and privacy. Security recommendation could be used to mitigate the security threats.

This paper presents detail about IoT healthcare applications and security threats in IoT application. In addition, this paper gives security solution in order to mitigate security threats.

References

- M. Abomhara and G. M. Køien. Security and Privacy in the Internet of Things: Current Status and Open Issues, 2004.
- S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood. Internet of multimedia things: Vision and challenges, 2015.
- A. W. Atamli and A. Martin, Threat-based Security Analysis for the Internet of Things, IEEE, 2014.
- C. Bing, D. Yuebo, J. Bo, Z. Xiang, and Z. Lijuan. The RFID-based Electronic Identity Security Platform of the Internet of Things, 2011 International Conference on Mechatronic Science, Electric Engineering and Computer Jilin, China, August 19-22, 2011.
- D. Chen and H. Zhao. Data security and privacy protection issues in cloud computing, International conference on computer science and electronics, engineering, 2012.
- J. Decuir. The Story of the Internet of Things, IEEE Consumer Electronics Magazine, 2015.
- M. Hamdi and H. Abie. Game-Based Adaptive Security in the Internet of Things for eHealth, IEEE, Communication and Information Systems Security Symposium, 2014.
- G. Jayavardhana, B.Rajkumar, M. Slaven, and P. Marimuthu. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 2013.
- K. Kai, P. Zhi-bo, and W. Cong. Security and privacy mechanism for healthinternet of things, 20(Suppl. 2): 64–68, www.sciencedirect.com/science/journal/10058885 <http://jcuapt.xsw.bupt.cn>, December 2013.
- I. Lee and K. Lee. The Internet of Things (IoT): Applications, investments, and challenges for enterprises, Elsevier, 2015.
- O. B. Lubecke, X. Gao, E. Yavari, M. Baboli, A. Singh, and V. M. Lubecke. E-Healthcare: Remote Monitoring, Privacy, and Security, 2014, IEEE, page 1351-1360, 2014.
- C. Michael, L. Markus, and R. Roger. The Internet of Things, McKinsey Quarterly, McKinsey & Company, Retrieved 10 July 2014.

- R. Neisse, G. Steri, I. N. Fovino, and G. Baldini. SecKit: A Model-based Security Toolkit for the Internet of Things 2015.
- K. T. Nguyen, M. Laurent, and N. Oualha. Survey on secure communication protocols for the Internet of Things, 2015.
- R. Sadeghi, C. Wachsmann., and M. Waidner, Security and Privacy Challenges In Industrial Internet of Things, 2015.
- A. Santos, J. Macedo, A. Costa, and M. J. Nicolau. Internet of Things and Smart Objects for M-Health Monitoring and Control, CENTERIS 2014 - Conference on ENTERprise Information Systems / ProjMAN 2014 – International Conference on Project MANagement / HCIST 2014 - International Conference on Health and Social Care Information Systems and Technologies, 2014.
- Michael J. Rush Carskadden, Threat Implications of the Internet of Things, 5th International Conference on Cyber Conflict, Tallinn, 2013.
- M. Shane, V. Nicola, S. Martin, and L. Anne. The Internet of Everything for Cities: Connecting People, Process, Data, and Things To Improve the ‘Livability’ of Cities and Communities, Cisco Systems, 2014.
- G. Shen and B. Liu. The visions, technologies, applications and security issues Of Internet of Things, 978-1-4244-8694-6/11/, IEEE, 2011.
- F. Shrouf and G. Miragliotta. Energy management based on Internet of Things: practices and framework for adoption in production management, Journal of Cleaner Production, 2015.
- S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini. Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, 2015.
- A. F. Skarmeta, J. L. Hernández-Ramos, and M. V. Moreno. A decentralized approach for Security and Privacy challenges in the Internet of Things, IEEE World Forum on Internet of Things (WF-IoT), 2014.
- D. Thilakanathan, S. Chen, S. Nepal and R. and A. Calvo. Secure and controlled sharing of data in distributed computing, IEEE 16th International Conference on Computational Science and Engineering, 2013.
- R. H. Weber., Internet of things – new security and privacy challenges, Computer Law & Security Review, 2010.
- B. D. Weinberg, G. R. Milne, Y. G. Andonova, and F. M.Hajjat. Internet of Things: Convenience vs. privacy and secrecy, Business Horizons, 2015.
- International Telecommunication Union. ITU Internet Reports, the Internet of Things, 2005.
- <http://www.ibmdatahub.com/blog/privacy-and-internet-things>, access date: 27.01..2016.
- <http://www.iso.org/iso/home/search.htm?qt=health+privacy&sort=> , access date: 27.01..2016.
- X. Xiaohui, Study on Security Problems and Key Technologies of the Internet of Things, 2012.
- X. Xingmei, Z. Jing, and W. He, Research on the Basic Characteristics, the Key Technologies, the Network Architecture and Security Problems of the Internet of Things, 2013 3rd International Conference on Computer Science and Network Technology, IEEE, 2013.