ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

A Review on Security and Privacy Implications in the Implementation of Internet of Things (IoTs) in E-Health

Dorothy Bundi[1], Masese Nelson[2]

P.G. Student, Department of Computer Science and IT, Kabarak University, Kenya[1]

Lecturer, Department of Computer Science and IT, Kabarak University, *Kenya* [2]

ABSTRACT: Internet of Things (IoT) promises to be a reliable technology for the future in different sectors including health. The health sector is one of the fields which is rapidly adopting IoT solutions with the aim to improve health care services; resulting to security vulnerabilities. This paper uses exploratory method with an objective to review various literature on application of IoTs in e-health based on the latest publications and technologies available in the health sector. In addition analyze the various software platforms available in the field of IoT in e-health. The literature on the security and privacy challenges and threats faced by the IoT in the health industry have also been explored. The results of this paper show that Energy Optimization, Denial of services, Physical attacks, Data manipulation, Trust and Privacy are key threats to the implementation of IoT in the health sector. The mitigation strategies to managing the identified security issues including trust and privacy challenges owing the level of data confidentiality required for healthcare organizations using IoT have been discussed.

KEYWORDS:Internet of Things (IoT), e-health, Security, Privacy, Healthcare Systems

I. INTRODUCTION

Internet of Things (IoTs) according to [1] is a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and involving Internet and network developments. IoTs offer specific object-identification, sensor and connection capability as the basis for the development of independent health services and health applications. These applications are characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability[2].

At the present time, Internet of Things (IoT) links the Internet with sensors and a multitude of devices, mostly using IP-based communications[3]. In healthcare industry,IoT provides options to remote monitoring, early prevention, and medical treatment for institutionalized disabled[4]. For IoT, people or objects can be equipped with sensors, actuators, Radio-Frequency Identification (RFID) tags, etc. Such devices and tags facilitate access by patients' caregivers. For example, RFIDs tags of patients or patients' personal devices (including medical devices) are readable, recognizable, locatable, and controllable via IoT applications[5]

IoT enables a wide range of smart applications and services to cope with challenges that individuals or healthcare sector faces. For example, IoT has dynamic capabilities to connect D2M (Device-to-Machine), O2O (Object-to-Object), P2D (Patient-to-Doctor), P2M (Patient-to- Machine), D2M (Doctor-to-Machine), S2M (Sensor-to-Mobile), M2H (Mobile-to-Human), T2R(Tag-to-Reader). This intelligently connects humans, machines, smart devices, and dynamic systems in order to assure an effective healthcare system[6].

Due to the increasing life expectancy, the group of people who are over the age of 60 is increasing faster than any other age group[7]. This can be considered as a success of public health policies, health services and socioeconomic development. However, it also presents a challenge to the society, which must cope with many more

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

disabled people. According to the World Health Organization (WHO)[8], the world's population of people over the age of 65 will reach 2 billion by 2050. To avoid overwhelming health services, there is a real need to prolong independent living of the disabled people (including the disabled elderly) at their own homes. This not only improves their quality of life, but also reduces costs for their families and the society at large[5]

II. RELATED WORK

The Internet of Things remains a relatively new field of research in different sectors, and its potential use for healthcare is an area still in its infancy[9].In this work, the detailed study of the various IoT enabling technologies and IoT software platforms that aid the recent health care monitoring system has been studied and analyzed for the remote data delivery and security of the data in health management system. Some papers based on different technologies has been discussed their transmission of data and methods and others focused on the security and authentication of the remote data. From the different sensors which are placed in the patient body [10].

A. Various IoT Enabling Technologies

The ehealth IoT system architecture, consisting of three layers (Device Layer, Internet connected gateway and Cloud Layer), allows a connection between a patient and their medical personnel, such as a medical doctor. It provides e-health facilities for continuous monitoring of heart rate, body temperature, blood pressure, blood sugar, electrocardiography, electromyography, skin problems and brain hemorrhage. In the ehealth IoT Architecture, data is collected from the human body via medical sensors[11].The output of the sensors is in electrical form and these signals are processed via Microprocessors or Microcontrollers and then this output is directly forwarded to the User Terminal. The User Terminal is connected to a layer which enables the end users' client or near user device to carry an amount of stored data, called Fog Layer with the help of Communication Protocols[6]. This Fog Layer is connected with the cloud layer. The Cloud Layer is used for Data Storage and Data Processing. The Cloud Layer also makes a backup for the patient data will be the significant territory of concern. IOT worldview will have pass on user's request for the data validation & protocols such that its request can be assess against the policies so that they can give or deny access. Some of the various ehealth IoT enabling technologies include remote Patient Monitoring, telehealth, wearable Devices for the ehealth IoT Solution, and software Platform for the Smartphones(Nandyala& Kim, 2016).

i. **Remote Patient Monitoring:** Remote Patient Monitoring Systems are ehealth IoT systems via which patients can be monitored at any place at any point in time. Remote Health Monitoring systems are beneficial for care homes, hospitals, healthcare centers and clinics. They can easily communicate and monitor health problems, in real time. It can potentially help reduce hospital waiting time and treatment time, decrease clinical treatment costs and improve the quality of care for the patients. Remote Health Monitoring Systems can be operated via Android or iOS applications and these applications are then directly connected via the Cloud Layer to the user terminal on smartphones, tablets or smart watches. Medical sensors will send data like oxygen saturation in the blood, heart rate, or pulse rate directly to the user's smart device in the emergency situation [10].

The Remote Monitoring Healthcare System is divided into three tiers: Wearable Sensors, Cloud Layer and User Terminals (such as tablets, smartphones, web portal, smart watches). The first tier in thissystem consisting of Wearable Sensors, is used to collect data like Pulse and Heart Rate, which is transmitted directly to the second tier. There the data is processed and stored in the Cloud Layer[13].The Cloud Layer receives data with the help of various communication modules such as Wi-Fi, Bluetooth or a 2.4 GHz Wireless. In the third tier of the system, hospital or clinical faculties access the data on smartphones or webportal.

The Remote Monitoring Healthcare System uses multiple sensors to acquire health data and provides this real time processed information to the medical doctor as well as patients' smart watch. Based on these results, the medical doctor can provide guidance to patients, for instance: "What to do to recover from the diagnosed disease" or "Which diet is better". The User Terminal consists of four modules of operations: these are: Storage data for the patient or about the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

patient, Management system, Patients view their stored data number of times and Provide treatment advice according to requirements. Every Remote Monitoring Healthcare System has two parameters to make it a Real Time Health Monitoring System [13].

ii. **Telehealth:** Telehealth is a bidirectional audio-video communication between Healthcare Service provider and a patient in their place of residence. Tele-healthcare facilities provide a virtual physical presence of the medical doctor to the Patient's home for the medical treatment and monitoring of the patient and their vital signs[14]. Due to the two-way communication, diseases can be detected by the medical doctors through monitoring their vital signs and providing medical assessments via the Telehealth care system. Telehealth is a bidirectional audio-video communication between Healthcare Service provider and apatient in their place of residence. Tele-healthcare facilities provide a virtual physical presenceof the medical doctor to the Patient's home for the medical treatment and monitoring of the patient and theirvital signs. Due to the two-way communication, diseases can be detected by the medical doctors throughmonitoring their vital signs and providing medical assessments via the Tele-healthcare system[15].

iii. **Telemedicineapplications** consist of three modes: I.e. Save and Forward, Tele-meeting and Video meeting. Save and forward, stores a patient's medical history and diagnosis report in a file with the help ofElectronic Medical Record (EMR). The EMR software sends the report to the medical doctor for advice.Telemedicine can help reduce or bypass the typical problems of waiting-times and travel time, when taking an appointment with a medical consultant [14]. However, this technique is not suitable in case of health problems that require immediate treatment. Tele-meeting is a consultation between different parties' discussions regarding the patient's health through audio via Internet. It is also suitable as a medium for a discussion between patient and doctor about the medical treatment. Video-meetings have so far been found to be themost beneficial and appropriate method for a long-distance medical discussion. It uses both audio andvideo, and requires high bandwidth and the cost of the equipment can be high if they using Radio Frequency(RF) components for audio and video[16].

iv. **Wearable Devices** for Internet of Medical Technology (IoMT) Solutions**:** Wearable Devices are smart devices that can be worn by the user or patient and collect medical data like Heart Rate, Pulse Rate, body Temperature and transmit this data directly to the Cloud Service Provider via Gateway. In a Wearable Device, the sensor and processor should have small in size and power efficient. Wearable devices - such as Smart Glasses, Smart Watch, Smart Shirt, Wireless key tracker, Smart Shoes, Smart Shirts and Pants, Smart Belt and Smart Bracelets-can be beneficial for elderly people, for the monitoring of vital signs during physicals activities [17].

III. THE IOT IN E-HEALTH SOFTWARE PLATFORMS

According to [18] some of the commonly used IoT healthcare platforms are from Google, Apple and Sumsung which are google fit, health kit, and SAMI respectively. However, all the three are offering theservices differently from each other, since the IoT has no specific standard specification that can be adopted by all the companies that are developing the IoT supported applications and platforms.

One of the limitations in the wider spread of IoTs in eHealth solutions is the fact that the existing portable or home-usable medical devices work only with software provided by the device's supplier; any attempt to re-use and integrate such devices in different applications fails because communication protocols are not openly available, or the device interfaces are proprietary solutions[19]. The lack of standardization and openness regarding protocols is counterproductive not only for the end-users or integrators but also for the suppliers. This can be solved through a standardization effort, a limited number of industrial network protocols and specially adapted Ethernet interfaces assure compatibility between different devices and distributed automation applications [20].

This paper adopts an IoT platform model which has 5 component of the IoT Platform for healthcare as one of the suitable self-management model for chronic disease such as hypertension, diabetes and obesity. The 5 components of the adopted IoT platform comprises of the medical sensor, virtual medical sensor, Mobile application, the software platform and its software manager [21]. The first element which is a medical sensor device is used to measure and send the medical data, and the second element is a virtual medical sensor which is a software sensor

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

which has an intelligent diagnosis algorithm and mashup data from various physical medical sensors and server. And the next component is a mobile application that is used for browsing medical data about patient or user from medical IoT device as well as using it for self-management purposes. The last component is an IoT software platform and its manager that enables all the components to communicate with each other by using unified API[1].

IV. THREATS OF IOT HEALTH APPLICATIONS

IoT devices are important for various 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. Despite the IoT benefits to the health sector, IoT devices are threatened by many security vulnerabilities and these include:

i. **Energy Optimization:** Sensors are significant devices for healthcare systems. Measurable and analyzable healthcare data aregathered very easily with the development of sensor [22] technology [23]. 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 [24].

ii. **Privacy**:Privacy has many definitions in the existing literature as defined by many authors. Privacy isimportant topic for information security at healthcaresystem in the world. Hence, many internationalorganizations define privacy. The Organization forEconomic Cooperation and Development (OECD) definesit as “any information relating to an identified oridentifiable individual. Healthcare data are collected from IoT devices [22].These devices gather data by remote accessmechanisms which have some challenging aboutprivacy and security. Data collected by the sensor istransmitted to the database or cloud over internet. Inaddition, IoT devices connect internet andcommunicate with each other from the Internet.Security vulnerabilities on Internet and IoT devices arethreatened health data[19]. Additionally, healthcare dataare collected from different health units. Health data isshared by various health units. Every unit must provideprivacy of data. Because healthcare data includesessential significant information. All the world'sattackers all the world's attackers want to capturehealth data. Thereof, privacy of data must be protected [25].

iii. **Trust**:Trust management is important for IoT devices andapplications due to provide security and privacy ofdata. Because all devices connect network and senddata to applications. Therefore, devices on the internetmust be trusted due to ensure privacy and security[2].Attackers could connect device IoT applications inorder to manipulate data.Data collection trust is serious issue because of hugevolumes of data are collected from devices. Big data isused by IoT health application owing to make rightdecision about patients and improve quality of healthcare [13]. Moreover, IoT health care services includedata process, analysis and mining. Attackers could bedamaged big data with create damage or maliciousinput of IoT devices. Hence, researchers study aboutchallenges of trust management in IoT. Trustmanagement in IoT must implement network layer and application layer[2].

iv. **Denial-of-service attacks (DoS)**:Denial-of-service attacks (DoS) are to make IoTdevices and IoT applications cannot provide service.IoT devices connect network and transfer data andcommunicate with each other. IoT applications need toconnect to network and receive data from thesedevices. Denial-of-service attacks (DoS) dangerous attacks for IoT applications because of machine ornetwork resource. IoT devices have low memorycapabilities and limited bandwidth, battery, and diskspace. Hence, they are affected from Denial-of-service attacks (DoS) easily[22].

v. **Physical attacks**:Physical security is serious issue for IoT devicesbecause of gathering data from of unprotected devices and they are integrated TVs, cars, air conditioning,ovens etc. Therefore, these devicescould be stolen easily or changed configuredsettings. Attackers can change data sent by IoTdevices. IoT devices are exposed many physicalattacks such as a secret stealing, softwaremanipulation, and hardware tampering[26].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

vi. **Data Manipulation**:Data is important IoT healthcare applications. Data isused all steps of healthcare systems. Thus, attacks areagainst to data security and privacy. Attacks arestealing data, data manipulation and damaging data.Health data is important and sensitive data for allcountry in the world because of including personallyidentifiable data. Data is used multiple paths in the IoT.These are IoT devices (data generator, data receiver, and aggregation point), the internet (multi-directionaldata transport), the cloud (data stored), the machine(application services, big data repositories, analytic)Attackers steal health data for malicious use and theydamage victims. They steal data when data is generatedand 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[27].

V. SECURITY SOLUTION OF IOT HEALTH APPLICATIONS

Security is important for IoT health applications because of the sensitivity of health data which require to be handled and managed with the highest level of privacy.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 andmonitor the use of critical data, and protect privacy and security[28].

In addition, employers in healthcare institutions 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.

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 protectingphysical attacks. In this way, IoT health devices keepon 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 [4].

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[29].

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 [5].

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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

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. 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 toemployees regularly[30].

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 andevent management (SIEM) must have auditing toensure 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 passivedefense because of becoming aware of critical security event after the occurrence of the event. Auditing help people to response to unwanted-event quickly[31].

V. METHODS

This paper uses exploratory research design with an objective to review various literature on application of IoTs in e-health based on the latest publications and technologies available in the health sector. This research design was guided by the following research questions:

1. How does the Internet of Things (IoTs) technology influence service delivery in e-health?
2. What are the security and privacy challenges and threats faced by the IoT in the e-health industry?

The researcher conducted the advanced search for the relevant publications from the electronic libraries and databases using the query string(s) defined below:

(Internet of Things OR "IoTs") AND (healthcare OR ehealth OR e-health OR health* OR *health*)

The table below shows the results from some of the 10 electronic databases and electronic libraries that were searched by the author.

Table 1: Electronic Databases and Electronic Libraries

S.No.	Database /Library Name	Number of Results	Number of results suitable after detailed screening
1.	IEEE Xplore	17	10
2.	Google Scholar	105	12
3.	PubMed – NCBI	30	5
4.	Elsevier Science Direct	18	8
5.	Mendeley	103	7
6.	PNAS	23	2
7.	Springer link	55	1
8.	Web of Science (WoS)	10	2
9.	Medline EBSCO	20	4
10.	ACM Digital Library	6	1

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

VI. RESULTS

Cisco Systems estimates that IoT will consist of 50 billion devices connected to the Internet by 2020 and it is predictable that many physical objects, like computers, sensor actuators, will be distributed with unique addresses and the ability to transfer data, from the common daily activities to restricted medical records, in a secure way [32].
The IoT is a critical part of health business processes and strategies going forward. Based on an IDC study of 2300 executives in 15 countries, 48 percent of those surveyed have already deployed IoT solutions, and 58 percent said that the IoT is strategic to their business strategy [33].
According to CISCO report of 2016 [34] the security solutions for the security challenges and threats are as summarized in the table below.

Table 2: Summary of IoT Threats Defense

SOLUTION	CAPABILITIES	PRODUCTS	HEALTHCARE OUTCOMES
IOT THREAT DEFENSE	• **Segmentation**– extensible, scalable protection against external attacks and compromised IoT devices **Secure Remote Access** – highly secure access, visibility and control to trusted third parties • **Visibility and Analysis** – Analysis of internal and external traffic to detect and block threats • **Security Services** – expert guidance to assess risk, design solutions and respond to incidents	• Cisco Identity Services Engine (ISE) • Stealth watch • Cisco Umbrella • Cisco Next Generation Firewalls • Cisco Any Connect • Cisco Advisory Services • Cisco AMP • Cisco CTA	• Comprehensive threat protection from healthcare facility to the cloud • Authorise access to restricted areas • Inventory tracking with automated stock control • Mitigate medical device vulnerabilities and threats, such as Ransomware • Facilitate compliance with policy driven controls, so as to protect data privacy governance • Anytime anywhere workforce with secure access to apps, devices and collaboration solutions • Improve healthcare security and strengthen ransomware protection.

The table below shows the summary of Security Vulnerabilities, Threats/Attack Types, and Security Requirements/Solution Categories for IoT Components.

Table 3: Summary of Security Vulnerabilities, Threats and Security Solutions

IoT Components	Vulnerabilities	Threats/Attack Types	Security Requirements/ Solution Categories
Physical Objects	• Devices of this layer have limited calculation, communication and storage resources • Nodes are distributed in distant location; adversary can easily accesses the devices and performs	• Physical attacks • Integrating RFID • Integrating WSNs • DoS/DDoS • Unauthorized data access and access control	• Evaluate suspicious nodes' behavior can reduce the influence of malicious nodes • Encryption/ Cryptographic techniques • Access control • Authorization

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

	damages and illegal actions such as extract security information, keys, reprogram the device, etc.		• Identification • Authentication
Communication Technologies	• IoT is a dynamic network infrastructure • Low power • Lossy network • The challenges of selection security technique for each element • Defense capability of the network varies in different networks	• Wireless PAN/LAN communications • Wireless WAN communications • Secure IoT communication protocols in constrained resources environment • Secure transmitted data	• Communication security: the proposed security protocols ensure the smoothness transitions connections among different edge networks • Confidentiality service can be ensured through encryption/ decryption • Strong authentication • Backup solution: the ability of providing fast backup solution when network fails • Enhanced the security of IoT communication protocols • Authorized access • Availability
Applications	• Cloud computing • Data exposure • Web application security issues • Secure communication	• Data access • Data protection • PHRs Attacks • Malicious insider attack • Sharing data in multiple environments • Real-time information processing • Big data • Sharing the same sensed data by several applications • DoS • XSS attack • CSRF attack • SQL Injection	• Implementing the separation between information content and information source/ data isolation • Encryption/ decryption mechanisms • Secure data access • Confidentiality of data • Secure sensitive data • Backup plan • Scheduling techniques • Assuring identification • Proposing traditional distributed database technology • Assuring authentication • Firewall and antivirus • Intrusion detection • Enhanced communication protocols security

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

VII. CONCLUSION

IoT devices are very important for systems. Today, many systems have become smart with IoT devices. IoT devices are used to enable remote health monitoring and emergency notification systems. This can range from blood pressure and heart rate monitors to specialized implants, such as pacemakers. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. A smart bed also adjusts itself to apply appropriate pressure and support without manual intervention. End-to-end health monitoring IoT platforms are coming into use for diagnostic purposes as well, such as the prenatal diagnosis of birth defects.

These IoT health systems include big data and other sensors. IoT devices collect data for these systems. Patient's data is sensitive because of including personal information and other diagnostic data. Hence, these systems have many threats about data security and privacy. Security strategies that could be used to mitigate the security threats are provided.

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. Future work could be done to evaluate the security issues of post-implementation of IoTs in health sector.

REFERENCES

[1] M. A. Azzawi, R. Hassan, and H. A. A. Bakar, "A Review on Internet of Things (IoT) in Healthcare," *Int. J. Comput. Appl. (0975 8887)*, vol. 113, no. 1, pp. 1–7, 2015.
[2] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 88, 2018.
[3] S. V. Nath, "IoT architecture," *Internet Things Data Anal. Handb.*, pp. 239–249, 2017.
[4] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "600 =0.8," pp. 1–7, 2018.
[5] S. Sivagami, D. Revathy, and L. Nithyabharathi, "SMART HEALTH CARE SYSTEM IMPLEMENTED USING IoT," *Int. J. Contemp. Res. Comput. Sci. Technol.*, vol. 2, no. 3, pp. 641–646, 2016.
[6] Mir Sajjad HussainTalpur, "The Appliance Pervasive of Internet of Things in Healthcare Systems," *Int. J. Comput. Sci. Issues*, vol. 10, no. 1, pp. 419–424, 2013.
[7] M. Ianculescu, A. Stanciu, O. Bica, and V. Florian, "Shaping a Person-Centric eHealth System for an Age-Friendly Community. A Case Study," vol. 1, pp. 252–258, 2016.
[8] WHO | eHealth, "WHO | eHealth," *Who*. 2017.
[9] M. S. C. Kala and R. S. A. A. Raj, "A Vision of Internet of Things based Health Care : Applications , Challenges and Opportunities," *Int. J. Adv. Eng. Res.*, pp. 658–661, 2018.
[10] E. Sowmiya, L. Malathi, and A. Thamarai Selvi, "A study on security issues in healthcare applications using medical wireless sensor network and IoT," *IIOAB J.*, vol. 7, no. 9Special Issue, pp. 575–583, 2016.
[11] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," *Security and Communication Networks*, vol. 2018. 2018.
[12] C. S. Nandyala and H. K. Kim, "From cloud to fog and IoT-based real-time U-healthcare monitoring for smart homes and hospitals," *Int. J. Smart Home*, vol. 10, no. 2, pp. 187–196, 2016.
[13] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors (Switzerland)*, vol. 19, no. 2, 2019.
[14] S. S. Al-Majeed, I. S. Al-Mejibli, and J. Karam, "Home telehealth by Internet of Things (IoT)," *Can. Conf. Electr. Comput. Eng.*, vol. 2015-June, no. June, pp. 609–613, 2015.
[15] Darrell M. West, "How 5G technology enables the health internet of things," *Cent. Technol. Innov. Brookings*, no. July 2016, pp. 1–20, 2016.
[16] K. Lazarev, "Internet of Things for personal healthcare. Study of eHealth sector. Smart wearable design," no. December, p. 91, 2016.
[17] A. H. NguA, Po-Teng TsengA, Manvick PaliwalA, Christopher CarpenterA, and Walker Stipe, "Smartwatch-Based IoT Fall Detection Application," *Open J. Internet Things*, vol. 4, no. 1, pp. 87–98, 2018.
[18] B. M. Lee, "Design Requirements for IoT Healthcare Model using an Open IoT Platform," vol. 66, pp. 69–72, 2014.
[19] N. Terry, "Will the Internet of Things Transform Healthcare?," *Vand. J. Ent. Tech. L.*, vol. 19, pp. 327–327, 2016.
[20] K. Gautam, V. Puri, J. G Tromp, C. Van Le, and N. G. Nguyen, "Internet of Things and Healthcare Technologies: A Valuable Synergy from Design to Implementation," *Int. J. Mach. Learn. Networked Collab. Eng.*, vol. 2, no. 3, pp. 128–142, 2018.
[21] M. Maksimović, "Improving computing issues in internet of things driven e-health systems," *CEUR Workshop Proc.*, vol. 1852, pp. 14–17, 2017.
[22] F. I. Khan and S. Hameed, "Understanding Security Requirements and Challenges in Internet of Things (IoTs): A Review," pp. 1–18, 2018.
[23] A. S. Shah, H. Nasir, M. Fayaz, A. Lajis, and A. Shah, "A review on energy consumption optimization techniques in IoT based smart building environments," *Inf.*, vol. 10, no. 3, 2019.
[24] E. Sheikhi, G. P. Cimellaro, and S. P. Mahin, "Adaptive energy consumption optimization using IoT-based wireless sensor networks and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

structural health monitoring systems," *8th Eur. Work. Struct. Heal. Monit. EWSHM 2016*, vol. 1, 2016.

[25] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, pp. 648–651, 2012.

[26] H. Mora, D. Gil, R. M. Terol, J. Azorín, and J. Szymanski, "An IoT-based computational framework for healthcare monitoring in mobile environments," *Sensors (Switzerland)*, vol. 17, no. 10, 2017.

[27] S. Bhattacharjee, M. Salimitari, M. Chatterjee, K. Kwiat, and C. Kamhoua, "Preserving Data Integrity in IoT Networks Under Opportunistic Data Manipulation," *Proc. - 2017 IEEE 15th Int. Conf. Dependable, Auton. Secur. Comput. 2017 IEEE 15th Int. Conf. Pervasive Intell. Comput. 2017 IEEE 3rd Int. Conf. Big Data Intell. Compu*, vol. 2018-Janua, pp. 446–453, 2018.

[28] I. Ali, S. Sabir, and Z. Ullah, "Internet of Things Security , Device Authentication and Access Control : A Review," vol. 14, no. 8, pp. 456–466, 2016.

[29] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 464–467.

[30] A. Armando, "Access Control : Policies , Models , and Mechanisms," 2019.

[31] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, Jun. 2013.

[32] Cisco, "Cisco 2016 Annual Security Report," *Cisco Annu. Rep.*, pp. 1–87, 2016.

[33] M. Kraeling and M. C. Brogioli, "Internet of Things," *Softw. Eng. Embed. Syst.*, pp. 465–499, 2019.

[34] B. Y. C. I. C. Analysts, "Security priorities for IoT and connected healthcare," pp. 1–6, 2018.