Grenze International Journal of Engineering and Technology, June Issue

Major Security Models and Privacy Issues in India Surrounding IoT Healthcare Sector: A Study

Divya Sharma[1], Urvashi Sangwan[2] and Harshita[3]
[1-3]Manav Rachna International Institute of Research and Studies, Faridabad, India
Email: divya2957@gmail.com, urvashi.baswana84@gmail.com, harshita9121@gmail.com

***Abstract*—The privacy and security issues in these IoT applications are discussed, along with the IoT-based solutions known in the literature. Finally, the article identifies the privacy and security requirements for IoT applications. This article is a survey on privacy and security models in IoT health applications for disabled users. First, it includes definitions of privacy and security terms and discusses their relationship. Next, present an overview of IoT, including architecture and components. People are more likely to use the Internet of things. The growing population of the elderly and the increase in chronic diseases generate the need for the health sector to find ways to provide services at the patient's ease. Many people in India don't have access to adequate medical services because the health of these people suffers. Today the government is taking many initiatives to support and help people living in rural areas. This document proposes a model of IoT equipped electronic governance healthcare structure that helps meet critical health requirements. This article main focussed on major security models and privacy issues surrounding IOT healthcare sector in India.**

***Index Terms*— IoT, RFID, CIA-AANN, EPC, EDI, GPS.**

I. INTRODUCTION

Today “the Internet of Things (IoT) connects the Internet with sensors and a multitude of devices, primarily using IP-based communications. In the healthcare sector, IoT offers options for remote monitoring, early prevention and medical care for institutionalized disabled people. For IoT, people or objects can be equipped with sensors, actuators, radio frequency identification (RFID) tags, etc. These devices and tags facilitate access for healthcare professionals. For example, patient RFID tags or patient personal devices (including medical devices) are readable, recognizable, localizable and controllable through IoT applications [1].” IoT enables a wide range of smart applications and services to address the challenges people or the healthcare sector faces [2]. “For example, the IoT has dynamic capabilities to connect D2M (machine to device), O2O (object to object), P2D (patient to doctor), P2M (patient to machine), D2M (machine to doctor).), S2M (from sensor to mobile), M2H (from mobile to human), T2R (from tag to reader). This intelligently connects humans, machines, smart devices and dynamic systems to ensure an effective health system [3]. This not only improves their quality of life, but also reduces costs for their families and society in general.”

In a country like India, “where social and economic inequality exists, health is an important concern. People living in rural areas do not even know basic and primary health services. Villages make up a large part of the Indian economy and do not have the main medical facilities. According to the 2011 census, 68.84% of India's total population lives in villages, but the condition of health and medical services has not met expectations and

Grenze ID: 01.GIJET.10.2.592

requirements.”.
In India, “where it comes to geographical and population inequalities, it is difficult to provide medical services to everyone anywhere, but the use of IoT has made it possible. IoT can be implemented in any sector, be it environmental, manufacturing or framework. IoT has helped to reduce human efforts to provide various services to people.”

II. Objective of the Study

- To presenting the concept of privacy and security solutions for these IoT applications; and its relationships.
- To proposed IOT solutions for healthcare for the disabled and its related model of IoT equipped hospital**.**

III. Definitions of Privacy and Security

Privacy: “Ensuring privacy requires that individuals retain the right to control what information is collected about them, who stores it, which is used, how it is used and for what purpose it is used. Figure 1 shows the main privacy services1 and the properties defined by [4]:

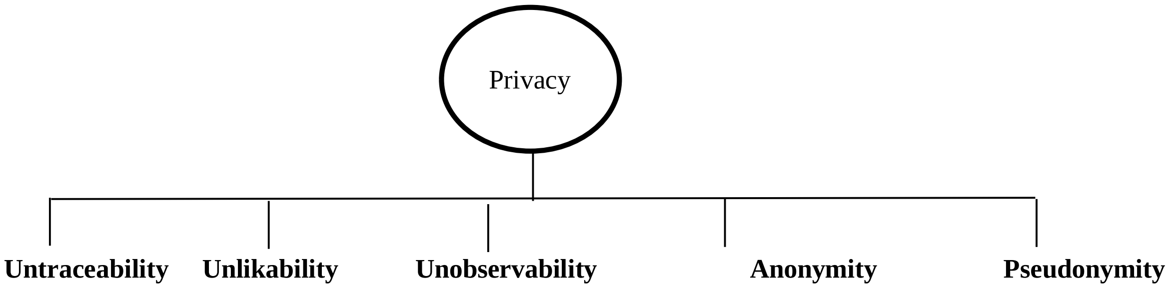

Figure1. Privacy Services

a) *Untraceability:* making it difficult for an opponent to identify that the same subject has performed a certain series of actions.
b) *Unlinkability:* hides information about the relationship between any element, such as topics, messages, actions, etc.
c) *Unobservability*: hide the fact that a message has been sent (instead of hiding the identity of the sender of the message).
d) *Anonymity*: hides information about who performed a certain action or who is described by a specific data set.
e) *Pseudonymity:* use of pseudonyms instead of using real identifiers.

Security: Providing security requires that you avoid access to information or other objects by unauthorized users, as well as protect from unauthorized alteration or destruction of our information. The classic definition of security is combined with confidentiality, integrity and availability, called (with its acronym) the triad of the CIA. The ISO 7498-24 standard extends the definition of safety, as shown in Figure 2, to the following requirements that can be used by the abbreviation CIA-AANN (cf. [5]):

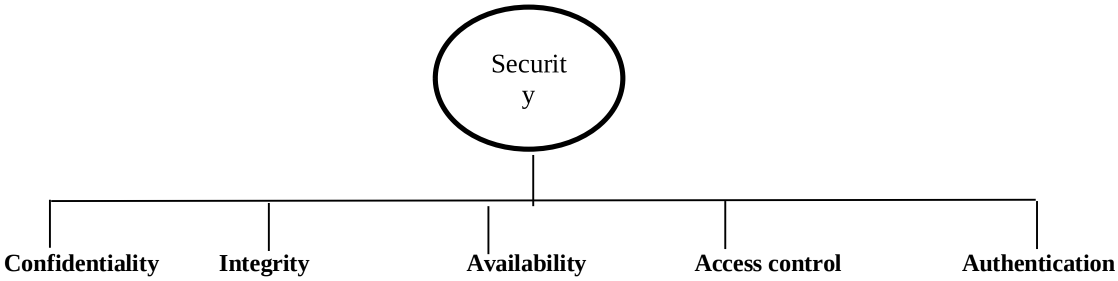

Figure 2. Security Services

a) *Confidentiality:* information is not made available or disclosed to unauthorized persons, entities or processes.

b) *Integrity*: the data have not been altered or destroyed in an unauthorized way.
c) *Availability:* a system is operational and functional at any time (it is not idle).
d) *Access control:* users only access the resources and services to which they have the right of access and qualified users do not have access to the services they legitimately expect to receive.
e) Authentication*:* confirmation that an entity is the one claimed and the source of the data received is the one claimed.

IV. Relationship between Privacy and Security

The Privacy and security are different. However, in the field of health, the relationship between these two concepts is data protection. We show the mutual relationship between security and privacy in Figure 3; that is, confidentiality is at the intersection of privacy and security."

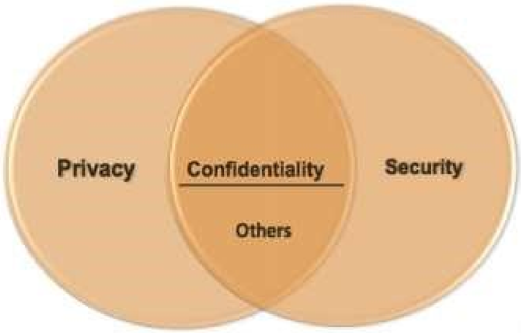

Figure 3. Mutual Relationship between Privacy and Securit

V. Overview of Internet of Things (IoT)

A. IoT Architecture

IoT architecture is made up of several layers, starting with the edge technology layer at the bottom and the application layer at the top, as shown in Figure 4 [6, 7]. The lower two levels contribute to data acquisition, while the upper two levels are responsible for the use of data in applications.

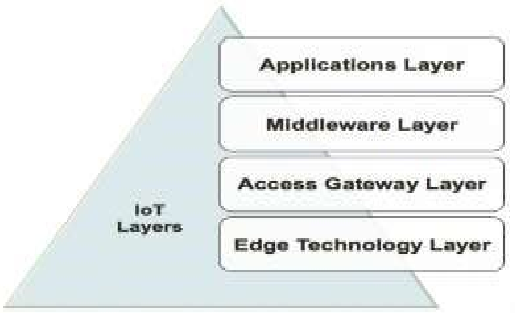

Figure 4. Layered Architecture of IoT

The functions of the levels (from bottom to top) are as follows:

1. Edge "technology level (also known as perception level): this is a hardware level that includes data collection components, such as wireless sensor networks (WSN), RFID systems, cameras, intelligent terminals, electronic data interfaces (EDI), global positioning systems (GPS). These hardware components provide the identification and storage of information (e.g. via RFID tags), information gathering (e.g. via sensor networks), information processing (e.g. via integrated on-board processors), communications, control and performance (e.g. by robot)."
2. Gateway layer "(also known as network layer or transport layer): this layer is responsible for data management, including data transmission, message routing and message publishing and subscription. Sends the information received from the edge layer to the middleware layer, using communication technologies such as Wi-Fi, Li-Fi, Ethernet, GSM, WSN and WiMax [6,7]."

3. Middleware level: “it is a software platform that provides abstraction to the applications of things. In addition, it offers numerous services such as device detection and management, data filtering, data aggregation, semantic data analysis, access control and information detection (using the electronic product code (EPC) or the object naming service (ONS).”
4. Application level: this higher level. “This is responsible for delivering several applications to different IoT users. It consists of two substrates:”
   a) “Sublayer for data management: provides directory services, quality of service (QoS), cloud computing technologies, data processing, machine-to-machine services (M2M), etc.”
   b) Application “service substrate: it is responsible for the interface with end users and business applications running on the IoT application level.”

B. IoT Components

The “IoT involves several components that work together to implement the IoT concept. The main IoT components are described below, described in Table 1.” The “IoT component of physical objects Physical objects (also known as physical devices): collecting, identifying and monitoring information on disabled users in their environments. This includes devices that monitor the vital signs of the disabled (blood pressure, heart rate, glucose, daily life). Physical devices are connected to the Internet and transform disability information obtained in the physical world into data for the digital world.”

TABLE I. IOT LAYERS AND COMPONENTS

IOT Layers	IOT Components	Tasks	Used Technologies
Application Layer	Applications	Provide the distribution with data and assistance	Smart Home technologies, Robotics, cloud computing
Middleware Layer	Access Control Data Management	Enable communication between applications and things.	MQTT, EPC, CNS, REST, Lightweight.
Access Gateway	Communication Technologies	Wireless WAN, training information over the internet through a device or gateway.	Wireless WAN, 2G, 3G, Long term evaluation(LTE)
Edge Technology Layer	Physical Objects	Identify and provide data about distributed layers in their environments.	RSID sensors, actuators.

The “IoT component of communication technologies The most common types of networks for IoT healthcare applications for the disabled are personal area networks (PAN), local area networks (LAN) and wide area networks (WAN). Each type of network involves a number of wireless technologies, as shown in the Layer row of the access gateway of Table 1.

C. The Applications IoT Component

The “IoT component of applications is responsible for formatting and organizing the data flow for specific applications [8]. It provides attention and assistance to users through intelligent technologies, such as smart home technology. Intelligent health systems that introduce new interconnections between the natural habitat of disabled people, their bodies and the Internet in order to produce and manage participatory medical knowledge. By replacing the wireless sensors inside the home, in clothing and personal objects, it is possible to monitor, in order to preserve privacy, the macroscopic behavior of the person, as well as compile statistics, identify precursors of dangerous behavioral anomalies and finally to activate alarms o request remote actions through appropriate assistance procedures.”

VI. IOT SOLUTIONS FOR HEALTHCARE FOR THE DISABLED AND ITS MODEL

Due to population growth and aging, expenditure on health services is growing rapidly, which is restricting access for some people with disabilities. The lack of specialized medical professionals, health workers and disabled facilities is particularly serious in rural areas [8]. This forces disabled people to seek health services in large hospitals or other high-cost healthcare institutions. The IoT is an opportunity to extend disabled-friendly health services in an affordable and cost-effective way. Risks of Exposure to Patient Privacy A Personal Health Register (PHR) is an "individual electronic health information register that meets nationally recognized interoperability standards. PHR can be extracted from multiple sources while it is managed, shared and controlled by the individual "[9]. PHRs are reported directly to the electronic health center and the main problem of privacy and security is maintaining the confidentiality of patients' PHRs.”

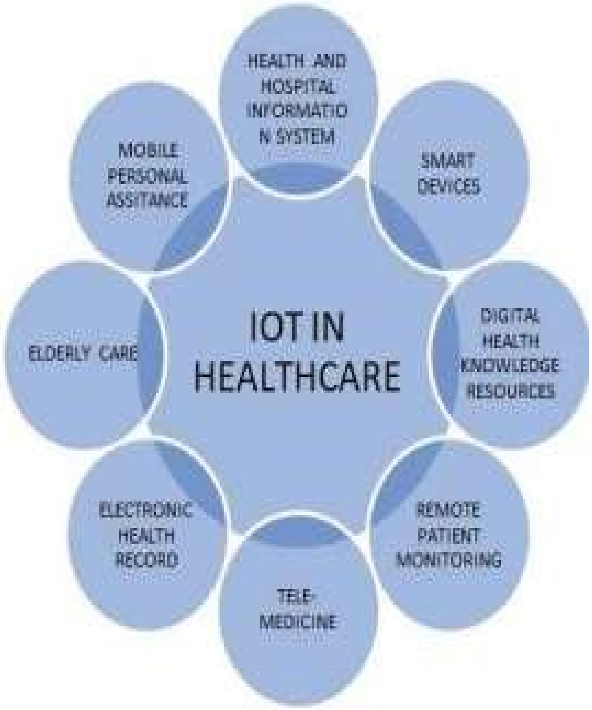

Figure 5. IoT in healthcare

A. Threats of Cyber-Attacks on Privacy

Cyber-attacks can “inject fake data into a system, causing critical damage to IoT applications. It is essential to provide the appropriate level of protection against cyber-attacks in smart home applications for the disabled. However, the limited nature of the resources of many of the IoT devices present in a smart home environment does not allow the implementation of standard security solutions.” E. Listening and confidentiality of data

In general, “patient health data, including those with disabilities, are kept under legal confidentiality obligations and made available only to authorized healthcare professionals. It is important to avoid stealing data from memory or spying on it as it flows through wireless links. For example, a popular insulin management system and IoT-based disabled glucose monitoring use wireless communication links, which are often used to launch attacks on privacy.” F. Proposed Model of IoT equipped Hospital.

While reading “the research conducted by numerous IoT researchers in the health sector and in many other sectors[10], an idea was trapped in the head and presented as a model. This document proposes a model of hospital facility equipped with IoT that projects the most advanced state-of-the-art medical care center that supports all GCSKs. Figure 5 illustrates a bottom-up approach, in which there were 3 levels: village levels, gram taluka level and state level. The village level refers to the rural area where adequate medical facilities and services are not available. The Garam Taluka level is made up of GCSK which helps a minimum of 10 villages. Anyone with a problem contact the doctor present at GCSK. The doctor collects all the data relating to the patient and his problem, stores them on a smart card and maintains a

database. Here, the patient receives the basic services of primary health care and treatment with the help of Swasthya slate. If the doctor present at GCSK is unable to cure the disease, he receives assistance from the state-level senior doctor through a video conference.

Patient care management: “the architecture of the model hospital structure equipped with IoT is shown in Figure 6. All the technologies used are connected via the Internet. Data collected via sensors and other technologies are sent to doctors, as well as medical assistants, who monitor the patient and the environment. The doctor, after analyzing the information received, sends comments. Doctors use the Android application on their smartphone to monitor the patient. If any unusual change in the patient's health is observed, the doctor receives an alert and visits the patient for a checkup. All data is uploaded and stored in cloud storage from where senior doctors can monitor patients (Figure 6).

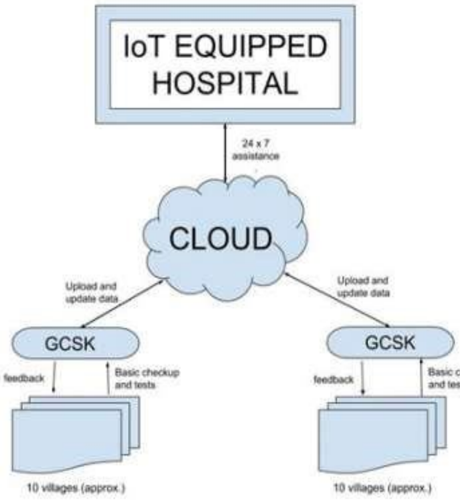

Figure 6. A bottom-up approaches

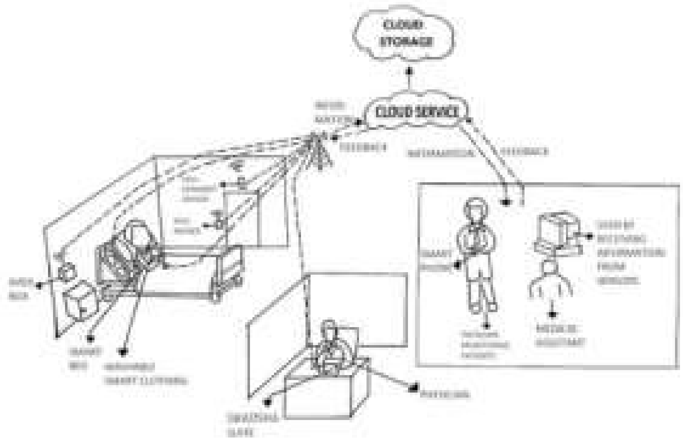

Figure 7. An architecture of the model framework of IoT equipped hospital

VII. CONCLUSION

The health sector has focused more on the use of IoT. There are several regions of India that face problems like blocking roads for a certain period of time every day, transportation problems, etc. The structure of the proposed model for a hospital equipped with IoT will be of great help during this period, as it can provide immediate help and has 24 × 7 connectivity with the hospital in the state region via the Internet. The Indian economy is based on villages, but villagers simply have availability and knowledge of medical facilities and services. The government must take the initiative to provide the villagers with medical facilities and services in the best possible way."

The diversity of "IoT components make security problems in IoT applications more difficult for disabled users. Therefore, identifying and addressing these security concerns is a key issue in the development of these IoT applications. The minimum security requirements for applications can be summarized in confidentiality, integrity and availability (CIA). Several research papers address the security challenges for IoT architecture. This article examines the security issues for the following IoT components, which are described in the table: physical objects, communication technologies and applications."

This article is about "IoT, its layered architecture and its role in the healthcare sector. It describes privacy and security services and proposes to consider confidentiality as the intersection of privacy and security. The articulation presents IoT components in the context of IoT architecture and mainly from the point of view of security and privacy. The article describes the range of IoT healthcare applications for the disabled along with their classification. Analyze privacy and security issues in IoT health applications for the disabled and review IoT-based solutions known in the literature."

REFERENCES

[1] R. Tesoriero, J.A. Guled, M.D. Lozano, and V.M.R., Penichet,“Tracking Autonomous Entities using RFID Technology ,” IEEE Trans. on Consumer Electronics, vol. 55 (2), May 2009, pp. 650-655.

[2] D. Giusto, A. Iera, G. Morabito, and L.Atzori,“An Overview of Privacy and Security Issues in the Internet of Things, “The Internet of Things, 1st Ed., Springer, New York, 2010, pp. 389-395.

[3] P. Yang, W. Wu, M. Moniri, and C.C. Chibelushi,“Efficient Objects Localization Using Sparsely Distributed Passive RFID Tags,” IEEE Trans. on Industrial, vol. 60(12), Dec. 2013, pp.1-11.

[4] L. Buttyan, and J. P. Hubaux,“ Privacy protection,” in Security and cooperation in wireless networks: Thwarting malicious and selfish behavior in the age of ubiquitous computing. New York: Cambridge University Press, 2008, pp. 237-254.

[5] B. Bhargava, , C. Farkas, , L. Lilien, , and F. Makedon. Trust, Privacy, and Security: Summary of a Workshop Breakout Session, the National Science Foundation Information and Data Management (IDM) Workshop held in Seattle, Washington. Sep. 14–16, 2003. Technical Report 2003-34.

[6] G. Santucci, “From Internet to Data to Internet of Things,” Proceedings of the Int. Conf. on Future Trends of the Internet, J. Wireless Personal Communications, vol. 58(1), May 2011, pp. 49-69.

[7] L. Atzori, A. Lera, and G. Morabito,“The Internet of Things: A Survey,” Computer Networks, vol. 54(15), Catania, Italy, 2010, pp.1-17

[8] D. Chen, G. Chang, L. Jin, X. Ren, J. Li, and F. Li,“A Novel Secure Architecture for the Internet of Things,” IEEE 5th Int. Conf. on Genetic and Evolutionary Computing, Xiamen, China, Aug. 2011, pp.311-314.

[9] J.S. Khan, V. Aulakh, and A. Bosworth,“ What It Takes: Characteristics of the Ideal Personal Health Record,” Health Aff (Millwood), vol. 28(2), pp. 369-376.

[10] Alpana Kakkar, Naveen Kumar and Sahil Kakkar. “Healthcare reaching rural area-A technology change management process.” IJSWS, Vol. 12, No. 1, 2015, pp. 117-21.M.V.S.S.