A Secure Health Care Technology Based on BSN Care

Soham S. Kulkarni[1] Swapnil K. Mahajan[2] Vikas R. Mahato[3] Shaninath G. Pawar[4] Swapnalini Pattanaik[5]

[1,2,3,4]Student [5]Assistant Professor

[1,2,3,4,5]Department of Computer Engineering

[1,2,3,4,5]JSPM's Rajarshi Shahu College of Engineering, Tathawade, Pune, India

Abstract— Advances in data and communication technologies have diode to the coming out of net of Things (IoT). Within the latest thing health care atmosphere, the usage of IoT technologies brings convenience of physicians and patients since they're applied to varied medical areas (such as period observation, patient data management, and tending management). The body detector network (BSN) technology is one in every of the core technologies of IoT developments in attention system, where a patient area unit usually monitored employing a collection of small powered and lightweight wireless device nodes. However, development of this new technology in attention applications whereas not considering security makes patient privacy weak. Throughout this text, at first we have a tendency to tend to focus on the most important security desires in BSN based smart attention system. After, we have a tendency to tend to propose a secure IoT based tending system pattern BSN, called BSN-Care, which may with efficiency accomplish those desires.

Key words: Data Privacy, Android, IOT, Security, BSN, Classification, ECG

Nomenclature Table

Sr.No.	Short Form	Description
1	IoT	Internet of Things
2	GPS	Global Positioning System
3	BSN	Body Sensor Network
4	SE	Self-Encryption
5	API	Application Program Interface
6	SQL	Structural Query Language
7	RFID	Radio Frequency Identification
8	SDK	Software Development Kit
9	LPU	Local Processing Unit
10	ECG	Electrocardiograms

I. INTRODUCTION

Internet of Things (IoT) has become one of the foremost powerful communication paradigms of the 21th century. Inside the IoT atmosphere, all objects in our everyday of living become a vicinity of the online because of their communication and computing capabilities (including little controllers, transceivers for digital communication). IoT extends the construct of the online and makes it loads of enveloping. IoT permits not to be faulted interactions among different types of devices like medical detector, observance cameras, home appliances so on. Because of that reason IoT has become loads of productive in several areas like health care system. In health care system, IoT involves many sorts of low value sensors (wearable, implanted, and environment) that modification aged people to consider stylish medical health care services anywhere, any time. Besides, it to boot greatly improves aged peoples quality of life. The body detector network (BSN) technology is one of the leading very important technologies used in IoT-based stylish health care system. It's basically a crowd of low-power and lightweight wireless detector nodes that square measure comfortable monitor the frame functions and around atmosphere. Since BSN nodes square measure familiar collect responsive (life-critical) information and will operate in hostile environments, consequently, they have strict security mechanisms to prevent malicious interaction with the system. The previous couple of decades have witnessed a regular increase in life in many parts of the world leading to a sharp go up inside the variability of aged people. A recent report from world organization foretold that there will be 2 billion (22% of the world population) older people by 2050. To boot, analysis indicates that regarding eighty 9 of the aged people square measure apparently to live severally. However, medical analysis surveys found that concerning eightieth of the aged people older than sixty 5 suffers from a minimum of 1 chronic sickness inflicting many aged people to possess issue in taking care of themselves. Consequently, providing associate honest quality of life for aged people has become a major social challenge at that moment. The speedy increase of knowledge and communication technology is facultative innovative health care solutions and tools that show promise in addressing the aforementioned challenges. Initial we have a tendency to tend to deal with the various security desires in BSN primarily based trendy health care system. Then, we have a leaning to tend to propose a secure IoT primarily based health care system unfair treatment BSN, referred to as BSN-Care, which could guarantee to with efficiency accomplish those desires.

II. RELATED WORK

A. A Secure IoT-based Modern Healthcare System Using Body Sensor Network

1) Author: ProsantaGope, Tzonelih Hwang

The body detector network (BSN) technology is one in every of the core technologies of IoT developments in tending system, wherever a patient may be monitored using a group of tiny-powered and light-weight wireless sensor nodes. However, development of this new technology in tending applications while not considering security makes patient privacy vulnerable. Throughout this article, initially we have a tendency to highlight the major security needs in BSN based mostly stylish tending system. Afterwards, we have a tendency to propose a secure IoT based mostly healthcare system mistreatment BSN, known as BSN-Care, which can efficiently accomplish those needs.

B. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey

1) Author: P. Kumar, and H. Lee,

Healthcare applications are attention about as promising fields for wireless sensing element networks, wherever patients will be monitored unfair treatment wireless medical sensing element networks (WMSNs). Current WMSN health care analysis trends concentrate on patient reliable communication, patient quality, and energy-efficient routing, as some examples. However, deploying new technologies in health care applications while not considering security makes patient privacy in danger. Moreover, the physiological knowledge of a private are extremely sensitive. Therefore, security may be a preponderant demand of health care applications, especially within the case of patient privacy, if the patient has AN uncomfortable illness. This paper discusses the safety and privacy problems in health care application victimisation WMSNs. We highlight some common health care comes victimisation wireless medical sensing element networks, and discuss their security [2].

C. Medical Monitoring Application for Wearable Computing

1) Author: Dejan Rakovic Thomos Martin And Emil Jovanov

In this paper we discuss system design issues, present a survey and sensors and introduce two taxonomies of medical monitoring applications for wearable computing [3].

D. Untracable Sensor Movement in Distributed IoTInfrastructure

1) Author: ProsantaGope, Tzonelih Hwang

In this paper we tend to concentrate on the privacy of the device movement during a distributed IoT infrastructure. During this regard, initially we tend to propose a distributed IoT system design. Then, we tend to style a light-weight anonymous authentication theme, which may guarantee numerous security problems associated with privacy of the device node like obscurity, intractability, replay attacks, DoS attacks, etc. so as to style the light-weight authentication framework for IoT, we are going to use the light-weight crypto logic primitives just like the hash perform and bitwise exclusive-OR, wherever these crypto logic primitives cause less machine overhead and fairly a lot of less execution time as compared to different crypto logic primitives like uneven encryption/decryption, modulo operation etc.[4].

E. Transactional Confidentiality in Sensor Networks

1) Author: Samper Pai, Sergio Bermudez, and Stephen B. Wicker

The association for Standardization (ISO) defines confidentiality because the assurance that information is accessible solely to those approved to own access. Confidentiality is provided through policies and practices that make sure that info flows solely to approve people. In a very network, confidentiality requires the event of rules governing access to transactional knowledge (that is, the knowledge gathered through generation, transmission, and routing of information messages inside the network) and technical measures that enforce those rules and prevent adversary from violating them. In several cases, conserving network confidentiality could be a beginning in conserving the privacy of a detector network's users and deplorers, and, where individuals are gift within the network area, their privacy and safety further [5].

F. Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)

1) Author: Jason W.P. Ng, Benny P.L. Lo, Oliver Wells, Morris Sloman, Nick Peters, AraDarzi, Chris Toumazou, and Guang-Zhong Yang

Body device network (BSN) is associate degree helpful technology for providing present attention watching. Even with the technological developments of sensing and watching devices, problems associated with system integration, sensor efficiency, low-power device interface electronic equipment design, wireless links and signal process area unit major technical challenges. The aim of this paper is to address problems associated with victimisation wearable or implantable sensors for distributed mobile watching. A proposed system design, together with ainitialexpression prototype, is delineated [6].

III. EXISTING SYSTEM

The last few decades have witnessed a delicate increase in life in many parts of the world leading to a quick rise among the vary of previous of us. A recent report from alignment predicted that there will be a try of billion (22% of the world population) older of us by 2050. In addition, analysis indicates that concerning eighty 9 of the aged of us square measure probably to live severally. However, medical analysis surveys found that concerning eightieth of the aged of us older than sixty 5 suffers from a minimum of 1 chronic health problem inflicting many aged of us to possess issue in taking care of themselves. Consequently, providing associate degree honest quality of life for aged of us has become a big social challenge at that moment. The speedy proliferation of information and communication technologies is facultative innovative health care solutions and tools. In existing system security issues were a heavy disadvantage. Thanks to this lack of security, some patient's necessary data lost. It finally ends up within the weakness of the patient's privacy. To beat this disadvantage, some projected techniques square measure handled to require care of the data security.

A. DISADVANTAGES

1) System security issues
2) Digital Divide among Patients
3) Lack of Information Control
4) Safety and privacy

IV. PROPOSED SYSTEM

The body device network (BSN) technology is one in every of the core technologies of IoT developments in care system, wherever a patient are often monitored employing a assortment of tiny-powered and light-weight wireless device nodes. However, development of this new technology in care applications while not considering security makes patient privacy vulnerable. Here initially we tend to highlight the key security needs in BSN based mostly trendy care system. After, we tend to propose a secure IoT based mostly care

1054

system victimisation BSN, referred to as BSN-Care, which may expeditiously accomplish those needs. We tend to gift a listing of security parameters that area unit needed to be self-addressed in any IoT based mostly care system victimisation BSN. We tend to gift our BSN-Care system and after, we tend to conjointly therefore show the way to enforce security in our BSN-Care model to realize all the imperative security properties.
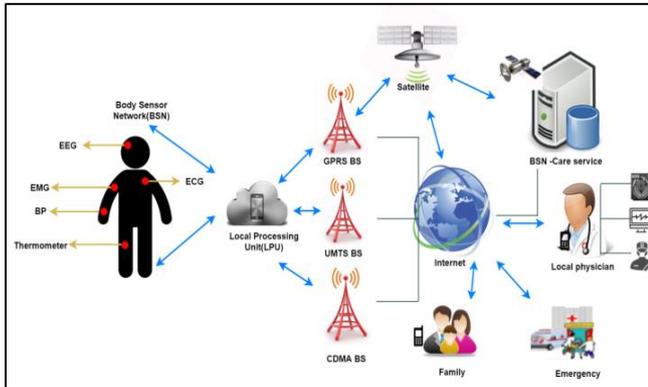

Fig. 2: System Architecture

A. Advantages
1) Decreased Costs
2) Improved Outcomes of Treatment
3) Improved Disease Management
4) Reduced Error
5) Enhanced Patient Experience
6) Enhanced Management of Drugs

V. TECHNOLOGY USED

A. Android
Android could be a total set of code for mobile devices like pill computers, notebooks, sensible phones, electronic book readers, set-top boxes etc. It contains a Linux-based software, middleware and key mobile applications. It will be thought of as mobile software. However it's not secret to mobile exclusively. It's presently utilized in varied devices like mobiles, tablets, televisions etc.

B. SqLite
SQLite is RDBMS. SQLite is Associate in nursing in-process library that implements a self-contained, server less, zero configurations, transactional. It written in ANSI-C and provides easy and easy-to-use API. In distinction to several direction systems, SQLite isn't a client-server info engine. The ASCII text file for SQLite is publically domain. SQLite is ACID-complaint (Atomic, Consistent, Isolated and Durable), permitting safe access from multiple processes or threads. It's not a standalone method like various databases; you'll link it statically or dynamically as per your demand together with your application. It will access its storage files directly. A whole SQLite info is hold on in a very single cross-platform computer file. It's terribly tiny and lightweight weight, but 400KB absolutely designed. It's out there on OS (Linux, OS-X, Android) and Windows (Win32, Win RT, WinCE).

C. MySql
MySQL is open source relational database management system (RDBMS) which is freely available and makes use of Structured Query Language. It was widely used open source client server RDBMS. It is one of the best RDBMS being used for developing web-based software applications. MySQL is developed, marketed, and supported by MySQL AB, which is Swedish company. It makes use of a standard form of the well-known SQL data language. It has become popular because of its features. MySQL is released under an open-source license. So you need not require paying. It is capable of handling a large subset of functionality of the most expensive as well as powerful database packages. It is scalable and it has the ability to handle almost any amount of data. It is a secure database. It includes solid data security layers which protect sensitive data from intruders. It supports the several development interfaces like JDBD, ODBC ad scripting (PHP and Perl). It can be executed under a number of operating system.

VI. PURPOSE

1) Security is one of the most imperative aspects of any system.
2) Various security threats to these systems. So implement key security requirements in IoT based healthcare system using BSN.

VII. SCOPE

1) IoT based devices is mostly used now a days
2) Provide solution without extra hardware requirement
3) To develop an Android application that is cost efficient
4) To efficiently use of resources
5) To make system easy to handle and accurate

VIII. CONCLUSION AND FUTURE SCOPE

In this Paper, initially we've got explain the protection and therefore the privacy problems in health care applications exploitation body device network (BSN). Afterward, we tend to found that even supposing most of the favoured BSN primarily based analysis comes acknowledge the problem of the protection, however they fail to introduce robust security services that would be preserve patient privacy. Finally, we tend to projected a secure IoT primarily based health care system operation BSN, referred to as BSN-Care, which may expeditiously achieve various security needs of the BSN primarily based health care system.

IX. CONTRIBUTION

- Family members having notification about patient Health day by day.
- And also doctor having notification about patient health like (Patient is normal or not any other changes occurred after treatment is also regularly check using smart devices).
- Patient Information Security and Patient Healthcare are smartly managed.

– IoT is most popular now a days so here satellite is available that maintain all record regarding to healthcare appliances.

REFERENCES

[1] ProsantaGope, Tzonelih Hwang "BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network"– 2015.

[2] P. Kumar, and H. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey." Sensors (Basel, Switzerland) 12.1 (2012): pp. 55–91.

[3] Dejan Rakovic Thomos Martin and Emil Jovanov "Medical Monitoring Application for Wearable Computing" Jul– 2003.

[4] ProsantaGope, Tzonelih Hwang "Untraceable Sensor Movement in Distributed IoTInfrastructure" -2015

[5] SamperPai, Sergio Bermudez, and Stephen B. Wicker "Transactional Confidentiality in Sensor Networks"jul/Aug 2008.

[6] Jason W.P. Ng, Benny P.L. Lo, Oliver Wells, Morris Sloman, Nick Peters, AraDarzi, Chris Toumazou, and Guang-Zhong Yang"Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)" – 2010.