Abstract. In today's world, providing remote healthcare to the aged people or people with chronic diseases is a challenging task. The health risks of this type of patients living alone need continuous monitoring. The intelligent health monitor is likely to be an effective approach to provide healthcare service from remote places, without barging on the privacy of the people. This technology happens to be one of the important applications of cloud based Internet of Things. However, effective implementation of this system needs removal of a variety of security threats and establishment of trust among the participants. In this work, an insight has been presented for the security issues related to Internet of Things environment for remote health monitor. The objective of this work is to propose a novel intelligent and cost-effective framework to assist patients or aged people, who have to live alone and could not afford hospital cost for a long period. The framework is embedded with different modular security solutions in a bottom-up approach to mitigate most of the security risks of IoT environment. The main focus is on to consider interoperability among various security solutions among IoT components with less overhead besides enabling real time decision making effective.

Keywords. Intelligent Health Monitor; Cloud based Internet of Things; Independent Living; Assisted Aged Living; Secure Framework

1 Introduction

The aging population of the world is increasing day by day at an alarming rate. The ratio of elderly versus younger population is also decreasing, signifying lesser number of caretakers for the elderly people at home. Studies have revealed that most of the elderly people prefer to live at their own home rather than in nursing homes or other clinical facilities. Frequent home visits from healthcare agents may increase the cost of caregiving considerably, besides causing disturbance to the people. The concept of Assisted Aged Living (AAL) arises to support elder people with self-management tasks. It provides technical system for aged people who are alone at home and need to be monitored. The concept of assisted living keeps[1] the promises to promote a better and healthier lifestyle for individuals; to enhance security; to prevent social isolation; to support maintaining the multifunctional network around the individual; to support caregivers, and care organizations; to increase the efficiency and productivity of resources in the societies.

Internet of Things (IoT) is a comparatively new domain, which treats heterogeneous entities as “things” and promises to deliver information on an anytime, anywhere basis. This facilitates real time decision making, which is extremely important in case of consideration of the health of aged people. The power of sensors, combined with data storage and other services of clouds, connected to caregivers and other related entities can make the assisted living concept a reality, without involving huge cost. Till now, researchers have been working mainly in the domains of remote healthcare, security of sensor network and cloud, and sensor cloud. IoT brings together all these features, and combines all in a seamless fashion to provide secure, cost-effective solution to the problem of assisted living. It seems to be feasible for a better quality of life of aging society by providing health service at AAL home as opposed to expensive clinical environments. The doctor from a remote location can monitor the health status of the elderly person and is able to provide medical assistance based on the information sent from the assisted living home.
2 Problem Statement

The development of IoT based healthcare application offers many novel challenges, such as, reliable data transmission, fast event detection, timely delivery of data etc. It poses certain challenges such as privacy, reliability, data confidentiality and security. The use of new technologies in healthcare applications without considering security often makes aged person’s privacy vulnerable[2]. The pervasive use of wireless techniques makes it easy for malicious adversaries to launch security attacks. As healthcare systems are designed to assist in medical treatment, security vulnerabilities lead the entire system unreliable, putting elder persons’ lives at risk. Some of the most possible vulnerabilities to this type of healthcare systems include the following. In case of emergencies, false alarms may be generated or real alarms may be suppressed by the system. It is also possible to cause alteration to the health data of a specific person, leading to incorrect diagnosis and treatment. Another concern has been the significant increase of risk to the privacy issues. A Healthcare network shares individual data with healthcare providers at remote places. Unauthorized collection and use of AAL data by potential adversaries can cause life-threatening risks for aged persons, or make their private information available. As the physiological data about an individual are highly vulnerable, so security and privacy become some of the serious concerns for healthcare applications, especially when it comes to adopting IoT techniques. Keeping all these security issues in mind, it has been a challenge to design and implement secure remote health care and monitoring services, with an objective to provide cost effective treatment.

3 Related Work

There is no exact work based on the mentioned topic. Health status monitoring can be done by smart technology [3][4][5] such as under-the-bed sensors for detecting sleep patterns, a medication reminder, an appointment reminder, a toilet bowl sensor to check frequency of its use and health data such as the sugar level in urine. They also include checking of vital signs such as blood pressure, glucose level, body temperature, pulse, weight, cholesterol, medication adherence, and interactions. A significant change in pattern or a significant delay in readings serves as a trigger for an alert. Audible and visual feedback from the measuring device can be very helpful when the user is monitoring his or her health status. One’s caloric intake can be monitored and an audible and visual reminder alerts the person of a recommended consumption level. It includes reminder system announcing upcoming appointments or events and medication. The main role for smart home with healthcare technology is to enhance safety and promote physical activities. The monitoring system should be developed according to the requirement of the user. The system needs to be able to alert the users, as well as caregivers when necessary. The research in the area of IoT and M2M communication from security perspective is still at very early stage. Researchers have been working for quite some time for designing ubiquitous framework for remote healthcare in various scenarios. Most of the researches are directed to the framework focused on wireless body area network (WBAN) which is a main component of IoT. Basic objective of remote health monitor system could not be fulfilled without considering security issues. Lots of works have been done on the security issues of WBAN area[6][7], whereas not much work has been done in the field of IoT environment. There is no single security framework that could claim full protection for a remote health monitor in cloud based IoT environment.

4 Proposed Work

To visualize this concept in real life, use of IoT is the best option that involves heterogeneous network and thus an integration of all techniques is needed[8]. To handle large volume of health related data cloud based IoT framework has been considered[9].

Security of AAL framework in IoT environment should address the following main issues[10].

- Preservation of privacy for heterogeneous sets of objects.
- Decentralized authentication and trust model.
- Energy efficient security solutions.
In the proposed framework, involved entities are Ubiquitous sensor network or body area network, WPAN or 6LoWPAN area, Smart phone applications, Gateway or middleware, Internet, Cloud environment. Basic concept is to consider existing security policies for each entity in the framework as a base and then modify it according to the requirement for interoperability. Bottom up approach integrates the following modules to provide seamless solution. The security levels are – Data owner level, WBAN-WPAN level, 6LoWPAN level, Smart Phone level, 6LoWPAN gateway level, Internet level, Cloud computing level. However, technical implementation of integration of all security levels is very much complex. The main concerns for these technologies are cyber security, privacy issues, costs, lack of human intervention etc. Smart Home with monitoring system is open to security vulnerabilities due to the network interconnection of different systems. Work is on to solve this problem to provide benefits to the society.

Fig. 1. IoT based Assisted Aged Living Framework

The working procedure of proposed framework of intelligent health monitor for assisted aged living (AAL) is given below. The proposed IoT framework consists of six layers - Sensing layer, Data collection layer, Transport layer, Processing layer, Application layer, Transaction layer. Bio-sensors are attached to the human body for sensing biological parameters such as heart rate, blood pressure, glucose level, sweat condition, body temperature, etc. Actuator captures the event and sends it to the digital band on human wrist acting as sink node. The sink node in turn connects to smart phone via Bluetooth for sending packets. Other sensing or smart nodes capture events from daily activities of aged people and send it to the smart phone via Bluetooth. Smart phone application listens for Bluetooth connection. Read packets received from sensor or sink nodes and read system time while Bluetooth is connected. Sensor nodes go to low power sleep mode when it has nothing to do. Smart phone adds timestamp to packets and aggregates the packets as per the requirements. Then packets are sent to the nearest physical gateway which basically acts as middleware to provide homogeneous transmission among heterogeneous networks. Data packets are transmitted towards intelligent health monitor server site. Server site uses cloud environment to provide better service in cost-effective way. Therefore server site becomes cloud customer for using third party service on pay-per-use basis. There are several public clouds such as context service provider cloud, aged persons profile provider cloud, social service provider cloud to provide better service to the aged people. There is one application namely context management system (CMS) that uses context aggregator to integrate all the information to develop context model. It can analyze basic behavioral pattern of aged people to determine whether emergency situation occurs or not. This application considers sensing data along with senior’s
position with respect to X, Y, and Z coordinates; his/her location in terms of mapped region (at which place inside the intelligent home); his/her current activity to determine the importance of the event. Context model decision goes to health monitor server site. If emergency situation occurs then alert goes towards healthcare agent to provide immediate action. For minor events warning goes towards aged person. Otherwise healthcare agent can directly access patient’s data according to their access privilege regularly for routine check-up via biometric authentication enabled user interface.

5 Conclusion

In proposed framework entities should agree on a secure trust model at the initialization phase and all should provide authentication proof before their operations. It has been seen that sensing data should be transmitted towards smart phone in a secure manner within WPAN. Then data are aggregated according to the requirements and transmitted towards client side gateway using Bluetooth security concept. The gateway transmits the packets towards healthcare server site using effective encryption mechanism and traditional security mechanism over public network. Healthcare server site provides encrypted data to cloud provider in a secure manner. Data owner or healthcare provider can retrieve data only after giving suitable authentication proof. In general, minor alert can be generated by CMS and transmitted towards home site and healthcare site. During emergency, major alert is generated and transmitted towards healthcare site for immediate actions.

In-home health monitoring could help an increased portion of the growing elderly population to live safely and independently in their own homes. Trust Management is a key area for smart environments because of the user centric nature of these systems. At present, work is on to implement and analyze novel security mechanism at all layers of the proposed framework. Our plan is to design a prototype of secure and intelligent smart home framework that would provide assurance towards independent and safe living of the old populations worldwide.

References