Internet of Medical Things (IoMT) using Hybrid Security and Near Field Communication (NFC) Technology

B. Vinoth Kumar
Assistant Professor,
Dept. of Computer Applications
Ayya Nadar Janaki Ammal College, Sivakasi, India

M. Ramaswami
Associate Professor,
Dept. of Computer Applications, Madurai Kamaraj Univerisity, Madurai, India

P. Swathika
Assistant Professor,
Department of CSE,
Kamaraj College of Engg. and Tech., Virudhunagar, India

ABSTRACT
The Internet of Medical Things (IoMT) give a picture of the future where every physical objects will be connected to the internet and be able to identify themselves to other devices. IoMT is a new paradigm of the Internet of Things and it will effect in a large number of applications such as smart living, smart home, healthcare systems, smart manufacturing, environment monitoring, and smart logistics. This paper provides integration, summarizes and surveys some of the security techniques especially Hybrid Security (HS) that can be applied with healthcare applications in IoT environment.

Keywords
Body area network, medical things, hybrid security, hashing.

1. INTRODUCTION
IoT aims to enable things to be connected any place, anything and anytime using any service/network. IoT will create technological revolution in a large number of applications. Internet technology has become ubiquitous within our society which is infiltrating all aspects of our lives, and it is better to call it as necessity rather than convenience. The term IoT was first used by Kevin Ashton, where the physical world is becoming one big information system [1]. Because of the continuing decline in the cost of hardware and network connections used in the IoT, it would be easy to see everything and everyone in our physical world connected to the Internet through wireless network on 24 X 7 basis. Thus, in just over three decades, the percentage of older age people will increase two times from 7% to 14% of the total world population. Although the aging population signifies, a human success story of increased longevity of human life. However, sustained growth of the older population also poses health challenges. As more and more people will be entering an elder age, the risk of developing certain chronic and debilitating diseases is significantly will be higher [2].

2. PROBLEM STATEMENT
As per the reports submitted by the P&S Market Research, there will be a compound annual growth rate (CAGR) of 37.6% in the healthcare Internet of Things industry between the years 2015 and 2020 [3]. They claim that this rise could be attributed to the upper hand of remote monitoring healthcare systems that can detect chronic life-threatening diseases. By this we can assume that IoT has taken the reins and people can enjoy personalized attention for their health requirements; they can tune their devices to remind them of their appointments, calorie count, exercise check, blood pressure variations and so much more. In 2020, it is expected that the number of Internet-connected devices ranges from 26 billion to 50 billion as in. There are many IoT applications, and within those healthcare systems, it is considered one of the most important challenges that our society faces today and will be surveyed with security hybrid techniques in this paper. IoT could fetch many advantages in the field of healthcare, through the use of smart sensors, equipment, detectors, etc. These allow the identification and patient tracking online, the locations of the doctor, and keep track of the medical report of the patient [4].

The medical sensor senses patient sensitive body data and transmits it over the wireless channels which are more susceptible than wired networks. IoT will revolutionize healthcare in terms of security, privacy and investment, if actually it has been trusted by the medical institutions and the human community. Consequently healthcare using wireless sensor networks constitutes an exciting and growing field for scientific investigation. In fact the future of modern healthcare in an aging world will need ubiquitous observation of health with least actual interaction of doctor and patients [5]. In this paper the IoT and healthcare systems are summarized, reviewed and surveyed through the security multifunctional techniques.

3. SECURITY TECHNIQUES: OVERVIEW
In the 21st century, the healthcare industry has seen the drastic improvements due to the involvement of wireless medical sensor networks (WMSNs) in healthcare applications. A few decades ago WSNs were a topic of science/movie fiction for healthcare industries, and now they have become a reality and provide much quality-of-care. As the world's aging population is increasing at an unprecedented rate in both developed and developing countries [6], the dependencies on healthcare system has also increasing. In WMSN network, the mobile phone will help to coordinate the interactions of the things around people and provide real-time access to all types of information, including the people we meet, the places we go and the content that's available there. Some research estimates that the number of connected objects will reach 50 billion by 2020. The IoT promises humans to provide a smart life, highly networked world, which allows for a wide range of interactions with this environment. Techniques for interacting with wireless sensors such as IoT and sensor cloud aim to overcome restricted resources and efficiency. However, deploying new technologies in healthcare applications without considering security often makes patient privacy more vulnerable. The data captured by a set of sensors can be collected, processed according to an application-provided aggregation function, and then perceived as the reading of a single virtual sensor.

4. SECURITY AND PRIVACY ISSUES

This section discusses: (i) which would be the possible threats to a wireless healthcare application without implementation of proper security; and (ii) privacy issues. Before discussing the security issues in wireless healthcare applications, it is worthwhile to assume the scale of deployment of healthcare applications using WMSNs [7].

5. SECURITY TECHNIQUES: TYPES

Some of the common security techniques [8] that are used in the protection and immunization databases and also in IoT:

1) Access Control: Access control is a security technique which restricts the access to the data on database and its information except for the authorized users. There are two main types of access control: a) Physical access control limits access to rooms, buildings and physical IT assets, and b) Logical access control limits connections to data, system files and computer networks.
2) Hashing: Hashing is used to index and retrieve items in a database by using hash functions and can be defined as the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.
3) Steganography: Steganography is process of hiding/encrypt sensitive information in any type of media. 4) Cryptography: Cryptography is the practice and study of techniques for secure communication in which the ordinary text is converted to cipher text by encryption.
4) Hybrid Cryptography: Hybrid cryptography is a technique using multiple ciphers of different types together (symmetric and asymmetric ciphers), to take benefit of the strengths of each type of cryptography.

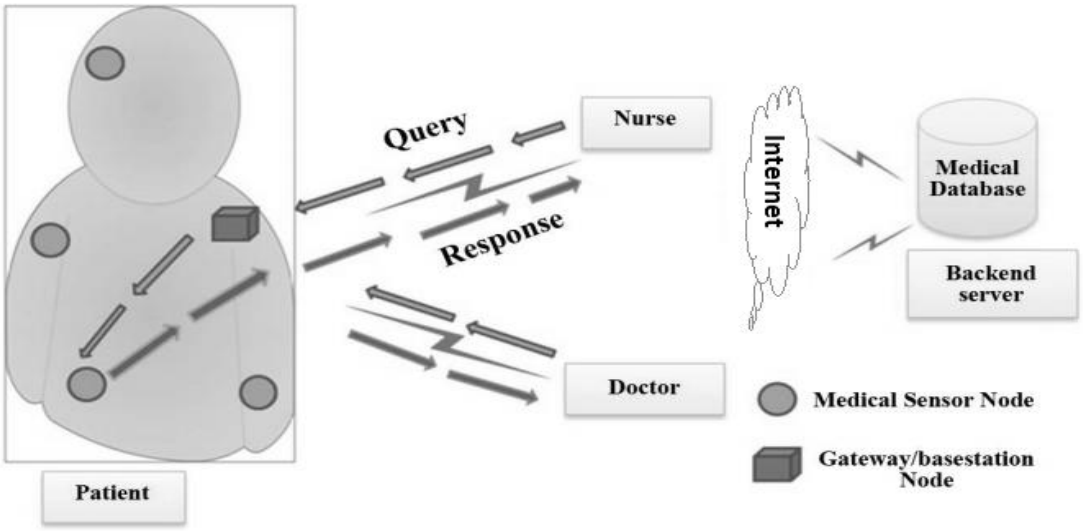

Fig 1: Patient monitoring system

6. SECURITY FOR HEALTHCARE SYSTEMS

Internet of Things (IoT) plays a significant role in a broad range of healthcare applications, from managing chronic diseases at one end of the spectrum to preventing diseases at the other. This requires sensors to gather physiological information and uses gateway devices and the cloud to analyze and store the information and then send the analyzed data wirelessly to healthcare providers for further analysis and decides kind of treatment given to patient. Wireless medical sensors may be wearable, implantable or portable, and integrated on various kinds of wireless communication motes. The wireless medical sensors collecting / generating large amounts of data and it becomes necessary to protect from security attacks [9]. By applying security algorithms/techniques, we can prevent many malicious attacks of data when transmitting to the remote locations over network. Therefore, security is a main requirement of healthcare applications. The success of healthcare application depends mainly on patient security and privacy, for ethical and legal reasons. Body sensors network (BSN) measures motion/acceleration, vital signs, temperature, blood pressure, heart rate and a mobile unit collect, visualizes and records activity data. Body area network (BAN) network on a diabetic patient could be helpful to auto inject insulin though a pump, as soon as their insulin level declines) [10]. Patient-monitoring systems presented in figure 1 with comprehensive patient statistics could be available for remote residential monitoring of patients with chronic diseases such as pulmonary and heart diseases and diabetes.

7. IMPLEMENTATION OF THE INTERNET OF MEDICAL THINGS

Simply put, wearable medical devices using Bluetooth Low Energy and NFC are transforming modern healthcare, improving the lives of the elderly, those living with chronic diseases, and those at risk of heart disease or other body ailments. Monitoring solutions are reducing the occurrence of heart disease and diabetes, while automated treatment devices improve quality of life for those with chronic pain or illness. Perhaps most promising of all, by connecting to our smartphones and tablets, the data provided by these wearables can enhance not only the health of the users themselves, but also may help doctors, researchers for better understanding and treat the diseases and ailments that affect the body in time [11].

8. NEAR FIELD COMMUNICATION (NFC) TECHNOLOGY USING MULTIFUNCTIONAL SECURITY

Bluetooth Low Energy, which maintains ubiquitous smartphone support, a usable real-world range of 10 to 30 meters that is perfect for indoor environments, and strong power efficiency, which is key requirement for wireless communications for wearable medical devices. However, near-field communication (NFC) is a strong second-place contender [12]. With lower power usage, and tap-and-go functionality, NFC provides a complementary wireless technology with unbeatable ease of use. Unlike Bluetooth, which lets users move around a room or area while staying connected, NFC requires devices to be within 10 cm, or practically touching, in order to activate. This physical limitation of NFC keeps it from being a direct competitor with Bluetooth, but is also the key to its value as a complementary wireless standard. The close proximity of NFC connections allows for tap-and-go transactions that are quick and easy to initiate. Instead of choosing from a list of nearby devices and entering passcodes, users simply tap the devices together and it automatically triggers an NFC communication sequence [13]. The intuitive nature of NFC is especially attractive for elderly populations, as well as for hospitals where it reduces or eliminates the need to train staff. NFC's maximum bit rate of 424 kb/s is much slower than Bluetooth Low Energy's 1 Mb/s, but NFC interactions can still be quite fast. Two NFC devices can connect, transmit sensor data, and close the connection in a short span of time once the user touching the devices together. With Bluetooth, the same process could involve several seconds, as the user manually selects the correct device to pair with and initiates a sensor reading [14]. Device compatibility is also less of an issue in clinical settings, where compatible devices can be administered by staff. Besides acting as the main wireless transport, NFC has also works well as a simple and secure handover to another longer range or higher bandwidth wireless protocol. NFC handovers are natively supported in the Bluetooth specification as an out-of-band pairing method, and can also be used to setup a Wi-Fi connection. This provides the simplified proximity pairing and authentication of NFC to Bluetooth or Wi-Fi connections. NFC connection handover is especially attractive in clinical settings where there may be dozens of active Bluetooth or Wi-Fi devices [15] in connection range and connecting to the right one is critical which is represented in figure 2.

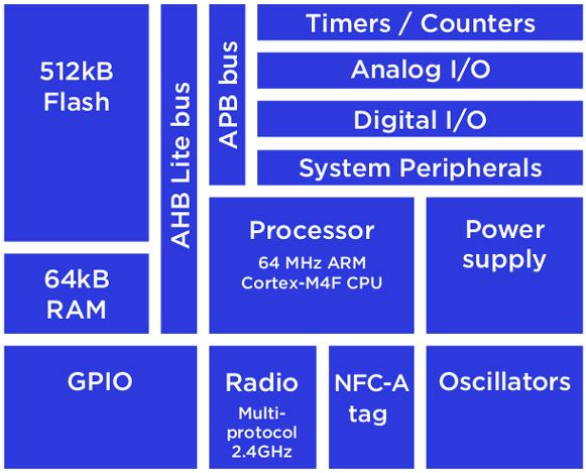

Fig 2: Multifunctional security system using NFC

9. CONCLUSION

IoMT is a new technology that has been more widely used in health care environment which depends on one of the most important technologies, and wireless sensor networks that can be used for connecting the physical world with the logic information world. The open nature of the information/data media has brought risks to the security of the wireless sensor networks and their collected data. In this paper, authors surveyed and discussed some of the security techniques for healthcare application that can be applied in IoT environment and introduced some of security techniques that are used in data security and immunization.

10. REFERENCES

[1] B. Elisa, "Data Secusity and Privacy – Concepts, Approaches and Research Directions", IEEE Annual Computer Software and Applications Conference, pp. 400-405, 2016.

[2] S. M. Riazul Islam, Daehan Kwak and MD. Humaun Kabir, "The Internet of Things for Health Care: A Comprehensive Survey", IEEE Journals and Magazines, pp. 678-708, 2015.

[3] Wei Zhao; Chaowei Wang; Yorie Nakahira "Medical Applications on Internet of Things", IET International Conference on Communication Technology and Application, pp. 660-665, 2011.

[4] Nava A. Shaked, "Avatars and virtual agents – relationship interfaces for the elderly", Healthcare Technology Letters, Vol. 4, pp. 83-87, 2016.

[5] Lei Clifton, David A. Clifton, Marco A. F. Pimentel, Peter J. Watkinson and Lionel Tarassenko, "Predictive Monitoring of Mobile Patients by Combining Clinical Observations With Data From Wearable Sensors", IEEE Journal of Biomedical and Health Informatics, Vol. 18, pp. 722-730, 2014.

[6] Taiyang Wu; Fan Wu; Jean-Michel Redouté; Mehmet Rasit Yuce, "An Autonomous Wireless Body Area Network Implementation Towards IoT Connected Healthcare Applications", IEEE Journals & Magazines, Vol. 5, pp. 11413-11422, 2017.

[7] Ding Ding; Mauro Conti; Agusti Solanas , "A smart health application and its related privacy issues", 2016 Smart City Security and Privacy Workshop (SCSP-W), pp. 1-5, 2016.

[8] B. Vinoth Kumar, M. Ramaswami and P. Swathika, "Data Security on Patient Monitoring for Future Healthcare Application", International Journal of Computer Applications, Vol.163, No. 6, pp. 20-23, 2017.

[9] Jiho. P, Yong-Gyu. L and Gilwon. Y, "Implementation of Security Algorithms for u-Health Monitoring System", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:6, No:5, 2012.

[10] B. Vinoth Kumar, M. Ramaswami, P. Swathika and P. Abinaya, "IPv6 based patient monitoring architecture for future healthcare application", International Journal of Computer Science and Information Security, Vol.14,No. 10, pp. 278-284, October 2016.

[11] Ankur Limaye and Tosiron Adegbija, "A Workload Characterization for the Internet of Medical Things (IoMT)", 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 302-307, 2017.

[12] Alessandro Leone, Gabriele Rescio and Pietro Siciliano, "An open NFC-based platform for vital signs monitoring", 2015 XVIII AISEM Annual Conference, pp. 1-4, 2015.

[13] Guoqiang Sun, Fan Yu, Xingyun Lei, Yan Wang and Hongpu Hu, "Research on Mobile Intelligent Medical Information System Based on the Internet of Things Technology", 2016 8th International Conference on Information Technology in Medicine and Education (ITME), Pages: 260–266, 2016.

[14] Antonio J. Jara, Pablo López, David Fern'ndez; Benito Úbeda, Miguel A. Zamora and Antonio F. G. Skarmeta," Interaction of Patients with Breathing Problems through NFC in Ambient Assisted Living Environments", 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp.892–897, 2012.

[15] Davide Brunell, Elisabetta Farella, Davide Giovanelli, Bojan Milosevic and Ivan Minakov, "Design Considerations for Wireless Acquisition of Multichannel sEMG Signals in Prosthetic Hand Control", IEEE Sensors Journal, Vol. 16, No. 23, pp. 8338-8347, 2016