RFID BASED TELEMEDICINE SYSTEM

Gunjan Baghel[1], Shweta[2], Yabrin Amin[3], Vivek Singh[4]

[1,2,3]UG, Students of Department of ECE, AIMT, Greater Noida ,(India).
[4] Assistant Professor, Department of ECE, AIMT, Greater Noida, (India)

ABSTRACT

Radio Frequency Identification (RFID) has potential for application in the new field of telemedicine, as the use of radio waves offers advantages over traditional optical technology such as bar codes. Radio waves are not limited by line of sight, they can penetrate objects and communicate in a wireless fashion. However, the same advantage is also the inherent weakness, as radio waves are susceptible to attack. Ongoing efforts have identified forward secure chain hashing as a viable security protocol for RFID authentication. Today's typical RFID communications take place with the "host-reader-tag" arrangement where the computational requirements are performed by a back end server system which holds all the intelligence and houses all records for an entire facility. One server can easily utilize multiple readers, but a compromise of this single system could have serious ramifications. Why not make a smaller system that is more robust and tolerant of intrusion. This can be achieved by implementing a stand alone reader that relies only on itself. We propose a server-less system that can accomplish the same results. Because our enhanced reader does not require a server to perform its function, if any readers are breached it only impacts that specific reader, not the entire server. By eliminating the resource heavy server device, we can yield a more robust overall system. We have selected a forward secure protocol to implement on an embedded platform that will be able to authenticate a tag without the resources of a back end server.

Keywords: RFID Components, Telemedicine System, RFID based Telemedicine System.

I. INTRODUCTION

Many people have experienced the commercial use of encrypted RFID in today's commerce, such as the toll collection system *"EZPass"* or the *"SpeedPass"* payment system by Exxon-Mobil. *SpeedPass*uses the Digital Signature Transponder (DST) manufactured by Texas Instruments (TI). DST is a cryptographically enabled passive RFID device using a block cipher to implement a challenge-response authentication scheme. Despite using a cipher text to exchange data with the reader, the fact remains that the data interaction was performed on an open broadcast rendering the unprotected tag vulnerable to any compatible reader. This authentication protocol was defeated in 2005 [5] with a TI evaluation kit.

The operational premise of RFID is based on wireless transmissions over open radio waves, which is also the appeal for unauthorized access by an adversary. Acknowledging the possibility of attack, we shall consider the wireless exchange as compromised and include it in the development parameters. These parameters also consider tag anonymity, the ability to prevent tag tracking, low cost of computational resources, and means to keep previous information secure going forward. We explore previous works that have successfully addressed these criteria. The work in [6] proposes a matrix algorithm which is adaptable to the embedded platform, but passive tags lack the ability to operate a timer as

specified, while [3] proposes an XOR scheme sharing random keys in a common list which require frequent overwriting of the complete list has failed to maintain security when not updated by the users. 1

In [1], [21], Ohkuno et al. state the criterion for a secure system includes indistinguishability, non- tracking, low-cost and forward-secure protocol. They propose the use of a one way function to circumvent the adversary tampering and implement a protocol that ensures the users privacy using a hash scheme. This method satisfies the low cost requirement and is adaptable to RFID use. Luo et al. build upon [1] by adding on mutual authentication protocol [2]. This work describes how to make the tag output non-constant using a randomized key thereby securing the data interaction between the reader and tag. Though the work is sound, [2] needs to synchronize the reader and tag using a PRNG, which is cost prohibitive for implementation on a low cost tag, therefore, was not considered for our implementation.

Of the work researched, [1] has the best approach for our proposed thesis. We will implement an embedded system using an 8bit microcontroller as an alternative to the traditional back end server that can be as effective in the RFID information exchange while limiting the potential of wide scale data breach. The work in this thesis will contribute to the security concerns stated by providing a lower cost alternative to the back end server setup that is able to keep information previously sent from being revealed in the future.

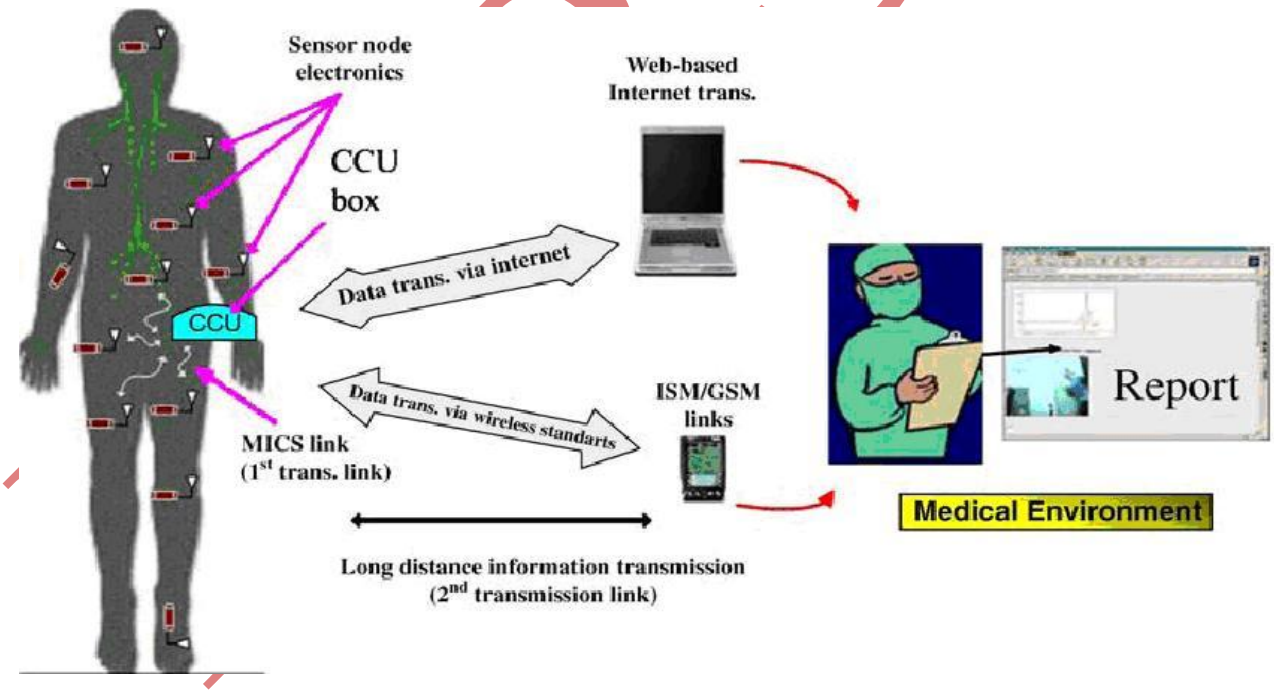

Figure1: Overview of RFID Based Telemedicine System

II. TELEMEDICINE

Telemedicine is the use of communication technology for the delivery of medical consultation or procedures at a distance. The appeal of telemedicine is that has the ability to bring primary and specialty medical care into remote areas. The potential to help patients who live hours from basic medical care services, and would otherwise not be able to get to

a medical facility, is enormous; it enables the patient to directly access quality medical professionals without leaving their communities. Telemedicine is not only restricted to patient use, medical specialists in off-site locations would be able to provide consulting services to onsite staff.

One example of the applications for telemedicine is an assisted living facility. The assisted living facility would benefit from promoting and offering virtual office visits with medical professionals from the facility. This is good for the living facilities ability to attract residents and increases the potential number of care sessions the resident could receive without actually leaving the facility. There is no need for the patient to be transported to the care giver and eliminates the logistics involved for the transportation. The virtual visit can also reduce the stress for the patient. Perhaps the patient has a condition that they wish to keep private as not to burden family members or they simply want to keep their affairs to themselves. Or perhaps the care giver at the living facility is a general practitioner or physicians assistant and needs to consult with a specialist; this ability would greatly increases the care available to the residents.

III. RADIO FREQUENCY IDENTIFICATION

RFID has been in existence since WWII but was too costly to be considered for widespread use in industry. In recent years the acronym has become more commonplace and come forward to be an acceptable means of identification technology. As important technology eventually does, RFID has found its way in to commerce and is being integrated into many areas in various forms. One may be using RFID in daily activities and not be aware of it. Libraries are using the technology for checkouts, shipping centers are using the technology for package tracking or work environments use RFID in the employee identification badges that grant building access to its personnel or perhaps a major credit card is embedded with a RFID device that does not need to be swiped to make a transaction.

In basic terms, RFID is a means to identify of one or more objects with the use of radio frequency waves. To make use of RFID technology there are three essential components required, these systems are discussed further.

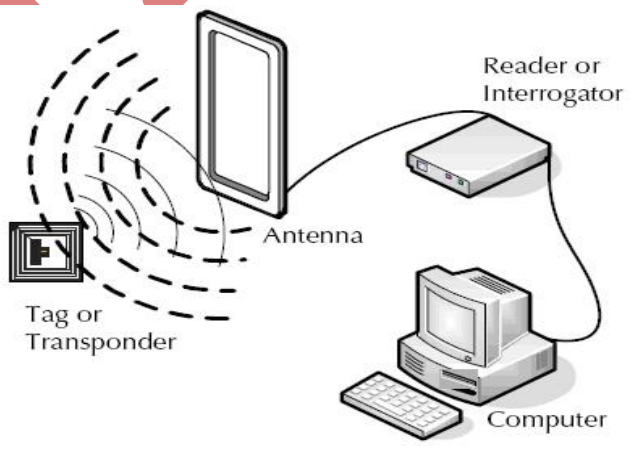

Figure 2: Working Diagram of RFID tags.

IV. SYSTEM DESIGN

From the several options and possible configurations we have shown, we have decided to employ a system that uses a wireless radio. The interface to the radio is simple a DB9 connection and the radios do not require the additional overhead of specific software for the internet or cell phone device. Also, the microcontroller we have selected does not have an encryption engine; this decision was made because of the frequency hopping operation of our chosen radio and inventory on hand.

Figure3: Reader Module

V. ABOUT KEIL uVISION 3

Keil Software to provide you with software development tools for 8051 based microcontrollers. With the Keil tools, you can generate embedded applications for virtually every 8051 derivative. The supported microcontrollers are listed in the µVision Device Database™. The Keil Software 8051 development tools are designed for the professional software developer, but any level of programmer can use them to get the most out of the 8051 microcontroller architecture. Keil software converts the C-codes into the Intel Hex code.

VI. BENEFITS TO PATIENTS-

- Access to specialized healthcare services to underserved rural , semi urban and remote areas.
- Reduce burden of morbidity.
- Reduce travel expenses.
- Early detection of disease.
- Reduce visits to specialityhospitals.
- Early diagnosis and treatment.

VII. CONCLUSION

Now here we will be attach all component those are give above with the Specific value connect through the given circuit diagram and in this manner Our RFID BASED TELEMEDICINE SYSTEM project will be complete. TELEMEDICINE ; One small step for IT , a giant leap for healthcare."

REFRENCES

[1] M. Ohkubu, K. Suzuki and S. Kinoshita, “Cryptographic approach to “Privacy-Friendly” tags”, Nippon Telegraph and Telephone Company, 2003.

[2] Z. Luo, T. Chan, J. Li, E. Wong, W. Cheung, V. Ng, W. Fok, “Experimental Analysis of an RFID Security Protocol”, IEEE International Conference on E-Business Engineering, IEEE ICEBE 2006, Shanghai, Oct 2006.

[3] Vyas, A.; Ahamed, S.I.; Haque, M.M.; Jayanthi, M.V.S., “A Robust lightweight solution for RFID security”, Advanced Information Networking and Applications Workshops, 2007, AINAW apos;07. 21st International Conference, Vol 2, May 2007.

[4] S. Weis, “Security and privacy in radio-frequency identification devices”, Master Thesis, Massachusetts Institute of Technology (MIT), 2003.

[5] S. Bono, M. Green, A. Stubblefield, A. Rubin, A. Juels, M. Szydlo. "Security Analysis of a Cryptographically-Enabled RFID Device".In Proceedings of the USENIX Security Symposium, August 2005.

[6] S. Karthikeyan, M. Nesterenko, “RFID security without extensive cryptography”, In Proceedings of the 3rd ACM workshop on SASN, New York, NY USA, 2005, pp 63-67 ACM Press, 2005.

[7] National Institute for Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180, Government Printing Office, Washington, D.C., 1993.

[8] National Institute for Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-3, Government Printing Office, Washington, D.C., 2008.

[9] Rivest, R., "The MD5 Message-Digest Algorithm," RFC-1321, MIT LCS and RSA Data Security, Inc., April 1992.

[10] http://matrix.inesc-id.pt/~pff/tfc04/md5-cast.pdf

[11] http://www.ti.com/rfid/docs/manuals/pdfSpecs/RI-TH1-CB1A.pdf

[12] Mollin, R. A. *An Introduction to Cryptography*. 1st Ed., CRC Press, Inc. 2000.

[13] http://www.lavalink.com/fileadmin/newsletters/link_06.04.pdf