Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.5, No.10, 2014


# A Sector Analysis for Rfid Human Implantation: Technical Analyses for Privacy Enhancing Techniques

Muhammad Habib
yahabebi@ymail.com

**Abstract**
Radio Frequency Identification (RFID) has produced a lot of attention in replacing the barcode with microchip. This interdisciplinary research aims to undertake a scoping study of emerged technology serving the security purposes of devices, infrastructures and human utilization. The study aims to address the key areas of widespread RFID implementation, its control over the applied widgets and the effective improvement in the protection measures like owner tracking and cloning. As a part of research an attempt will be taken toward discussion on security framework to improve the model of smart environment eliminating the privacy loopholes. To enhance the real time security structure the Origins of RFID Microchips are essential to be discussed for the application in several sectors like logistics and health care industries. The study will contribute to develop methods and procedures to re-plane the RFID control system, as well as mark other privacy issues which arise in operations.

## INTRODUCTION

Radio Frequency Identification (RFID) technology had humble beginnings in WWII in flying industries, Allied airplanes as well as to track nuclear material and in Australia its being in use by veterinary industry (NLIS) at large scale [1]. Technology then took another jump and currently used in logistics and supply chain management to track the items. Broadly the RFID tags are classified in three categories Active tag, Passive tag and Semi-Passive tags.

The ultimate aim of this research is to contribute to the existing technology of RFID, a microchip having the ability to transmit static identity at the short distance: short distance is due to low power of emitting electromagnetic waves. Extensive research has been done to serve the humanity medically with RFID technology. The prosthetic use of microchips can progress scientifically, assist people to hear better, help the handicaps and possibly can facilitate the paralyzed people to move [2]. The human embedding microchip technology is available which

implant the chips under the controlled application methods though some issues arises in its functional security framework as well as in the control application concerns. The issues include, tracking the person's location at exact coordinates, habitual changes in action at security access point, the privacy concerns as well as the hacking personnel information and access to the secured data illegally. The security problems in the RFID are complex in nature. The undergone research will contribute to steadfast all the significant issue related to the Microchip implementation methodology, its operational measures and all the intensive security issues.

## LITERATURE REVIEW

Radio Frequency Identification (RFID) technology began in World War II with an "Early Identification Friend (IFF) systems where it was possible for Allied fighters and anti-aircraft systems to distinguish their own returning bombers from aircraft sent by the enemy'' [3]. All along with the benefits of the Micro chipping there are also some potential health problems as well. For example the major effects of radio waves can harm in a dangerous way where Non-lionizing Radiation from microwave radio frequency and magnetic fields can also cause of various health issues [4]. Within the medical field there are different ways that RFID can be incorporated. For example RFID chips can be used to track equipment within a hospital. Wristbands with an RFID chip embedded can help hospitals with patient safety requirements. Medical personnel can read the chip to get instant access to the patients' medical history such has medication allergies, medications prescribed and dosage, and specimen results [5].

One example of the Neuro electronic Interface being used is with a paraplegic named John Nagle. "Nagle showed an ability to perform a number of tasks with his mind: control a TV, move a mouse cursor on a screen, and command an artificial hand to open and close grip" [6]. There are limitations at this time for the Neuro-electronic Interface for RFID chip usage in human. The first is the amount of neurons available for the device. The fewer amounts of neurons there are will result the less likely the device work performance. There is health risks associated with the human being implanted with a microchip. Some health issues include "adverse tissue reaction, migration of implanted transponder, electromagnetic interference, electrical hazards, and magnetic resonance imaging incompatibility" [7]. The majority of RFID applications have centered on firms increasing efficiencies in the supplier management process, which ultimately results in lowered costs. However, RFID is also currently being used by logistic service companies in order to enhance the service effectiveness to

 

the customer, thus enhancing the overall value perception. Instead of focusing on efficiencies of supplier relationships for manufacturers, these service firms seek to employ the technology to generate additional value for the customer [8].

## RESEARCH OBJECT IVES

Using the undergone privacy problems in operations, applications and their analysis (Objective 1), previous literature for concepts and ideas regarding RFID data secrecy measures, the set of design implications (Objective 2), the design of security frameworks covering existing threats to transmit information (Objective 3) and identifying categorical RFID implementation areas (Objective 4), it will be explore the possibility of developing a generalized framework in human implantation and its privacy matters that can be applied to the design of RFID systems to support co-located collaborations. However, if we find that the said framework formulation will require substantial extension of the research effort, we may decide to leave it open as a future research endeavor.

## PROBLEM STATEMENT

The major challenges arises round the globe regarding RFID (Radio Frequency Identification) technology are its data privacy which results location tracking and harmful for secret information to be snatched. In the same way human embedded microchip is also traced during transmitting data from chip to application database which results to locate the person. These issues provide a strong resistance to the technology and its performance capabilities. In context of these issues the research theme designs the privacy framework and the operational methodology which helps the technology to excel and be applicable within and across the domains diversely with steadfast its performance.

## RESEARCH GOALS

G1. Uncertainty control mechanism occurring in RFID data.
G2. How to effectively utilize the RFID for human intensive care purposes? Radical application to respond and transmit data on demand (operational features of Active tags)
G3. Implementation of the proposed novel privacy framework for RFID
G4. What are the countermeasures to conceal the RFID Tag Existence?
G5. How to effectively utilize the time gap when the RFID reader is waiting for the RFID tag to respond to an earlier transmitted command after pre-computation of one or more commands and what technique to apply in such a realistic scenario?

## RESEARCH GAPS

The RFID technology is an emerging area of research and still it is on its initial adoption phases yet facing several research gaps which has to be addressed. The gaps are existed between the performance of RFID systems and its associated issues. Due to various real time uncertainty limitations in such systems, the Faraday Cage (to wrap up the Tag with foil) technique preventing to intercept electromagnetic waves, i.e, ID-Queries, in order to prevent the tag from emitting response to reader. The soft computing practices like fuzzy logic (to map the real-world uncertainty), Complex security schemes (Hash Locking/Kill Commands), Countermeasures to emit extra data (Jamming) techniques are yet to be applied to such systems in order to effectively address the problems in existing RFID systems leading to enhanced privacy and performance.

## RESEARCH DESIGN & METHODOLOGY

The research process for this study will involve distinct phases. First, an extensive literature review will be carried out within innovation-adoption by the target sector and RFID domain. Based on literature, particularly dealing with organizational adoption, an initial research model will be developed. In the secondary research phase, the tentative privacy framework will be designed based on synthesis of existing research. The indicators of 'uncertainty' (data uncertainty, demand uncertainty, and technology uncertainty) are not necessarily correlated among each other; rather they *form* the construct [9].

## TIME FRAME AND RESOURCES

The approximate time required for the completion of research is about 3-4 years which includes the theoretical studies and the experimental work to be prepared. Fifty percent of time will be spent on research and reading relevant material and ten percent of time will be utilized in sorting and marking the research findings and remaining forty percent of time will be spent for writing, formatting and documenting under the potential supervision. There are few experimental resources like RFID tags (Active and Passive), RFID readers and software, which could be sorted out according to the supervision suggestions.

 

**REFERENCES**

[1]. Tonsor, G.T., Schroeder, T.C., 2006. Livestock identification: Lessons for the U.S. Beef Industry from the Australian System. *Journal of International Food & Agribusiness Marketing 18(3/4), 1 03-118.*

[2]. Charles, Techonal J., Manag, 2008. Human Microchip Implantation. *Journal of Technology Management & Innovation 08(3/3)151-1 60.*

[3]. GARFINKEL, S., Holtzman, H. (2005) Understanding RFID Technology. Pg. 15-16. Garfinkel Book [Links]

[4]. COVACIO, S. (2003) Technological Problems Associated with Subcutaneous Microchips for Human Identification (SMHId). *Informing Science.* [Links]

[5]. CASTRO, L, Wamba, S.F. (2007) An Inside LookAt RFID Technology. *Journal of Technology and lnnovation,*Volume 2, Issue I. Pg.4. [Links]

[6]. CHAN, E. (2007) The FDA and the Future of the Brain-Computer Interface: Adapting FDA Device Law to the Challenges of Human-Machine Enhancement. John *Marshall Journal of Computer* & *Information Law Volume* 25 Issue I. Pg. 13, 16, 24. http://works.bepress.com/eric_chan/1/. Retrieved 11-02-07 [Links]

[7]. GAD, L. (2006) Human Microchip Implantation. Wisconsin Legislative Reference Bureau. Pg. 1.www.legis.state.wi.us/lrb. Retrieved 9-28-07. [Links]

[8]. Leea, L.S., Fiedlera, K.D. and Smithb, J.S. (2008), "Radio frequency identification (RFID) implementation in the service sector: A customer-facing diffusion model", *Int. J. Production Economics,* 112, 587–600.

[9]. Teo, H.H., Wei, K.K., Benbasat, I., 2003. Predicting intention to adopt interorganizational linkages: An institutional perspective. MIS Quarterly 27(1), 19-49.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

## CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

**Prospective authors of journals can find the submission instruction on the following page:** http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

## MORE RESOURCES

Book publication information: http://www.iiste.org/book/

### IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar