International Journal of Computer Applications Technology and Research
Volume 4– Issue 8, 614 - 617, 2015, ISSN: 2319–8656

Review of the Introduction and Use of RFID

Fariba Ghorbany Beram
Sama Technical and Vocational Training College Islamic Azad University, Shoushtar Branch, Shoushtar, Iran

Mojtaba Khayat
Sama Technical and Vocational Training College Islamic Azad University, Shoushtar Branch, Shoushtar, Iran

Sajjad Ghorbany Beram
Sama Technical and Vocational Training College Islamic Azad University, Shoushtar Branch, Shoushtar, Iran

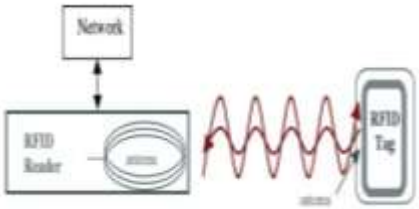
Abstract: We live in an age where technology is an integral part of human daily life. The aim of the technology is secure, accurate, correct use of time for mankind and nature brings it may also have disadvantages and challenges. In this paper we describe the RFID technology. Today, this technology in hospitals, shops, airports, tracking birds are used. It can be used in hospital intensive care unit for monitoring and remote patient care, which causes it to print patients and physicians are not required to comply with very close distance, the result of which can cause safety Patients and physicians should be. The security technology implementation is a challenge. This paper introduces the applications, the challenges we have this technology.

Keywords: Radio Frequency identification; tag; network; challenge

1. INTRODUCTION

Radio Frequency identification (RFID) is the popular wireless induction system [1-7]. RFID tags were initially developed as very small electronic hardware components having as their main function to broadcast a unique identifying number upon request. The simplest types of RFID tags are passive devices that not have an internal power source and are incapable of autonomous activity. They are powered by the reader's radio waves, with their antenna doubling as a source of inductive power. While admittedly a new technology, the low-cost and high convenience value of RFID tags gives them the potential for massive deployment, for business automation applications and as smart, mass-market, embedded devices that support ubiquitous applications. However, current RFID protocols are designed to optimize performance, with lesser attention paid to resilience and security. Consequently, most RFID systems are inherently insecure. The general design of a simple RFID system is displayed through the following figure:

Figure 1: Diagram describing operation of the RFID system.



2. RFID TECHNOLOGY

A typical deployment of an RFID system involves three types of legitimate entities, namely tags, readers and back-end servers. The tags are attached to, or embedded in, objects to be identified. They consist of a transponder and an RF coupling element. The coupling element has an antenna coil to capture RF power, clock pulses and data from the RFID reader. The readers typically contain a transceiver, a control unit, and a coupling element, to interrogate tags. They implement a radio interface to the tags and also a high level interface to a backend server that processes captured data. The back-servers are trusted entities that maintain a database containing the information needed to identify tags, including their identification numbers. Since the integrity of an RFID system is entirely dependent on the proper behavior of the server, it is assumed that the server is physically secure and not attackable. It is certainly legitimate to consider privacy mechanisms that reduce the trust on the back-end server—for instance, to mitigate the ability of the server to collect user-behavior information, or to make the server function auditable[8]. In this paper, however, we shall not investigate such privacy attacks. Here we shall consider the servers to be entirely trusted following:

- Signal strength limited to a required

distance;

- Radio frequency unable to work in certain

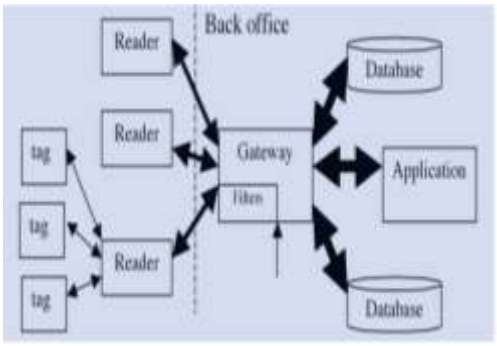
geographical areas;

- Electromagnetic field prone to interruption from solar and electrical storms.

The medical and healthcare sectors are using this technology as a means to keep track of medical equipment and the delivery of pharmaceuticals that proved to be costly in the past when it came to tracking them down. But now this technology is being applied as a means of protecting online medical information systems from those who are involved in perpetrating the criminal activity of medical identity theft. Because the identity of every individual is centred around recognising specific features, personality, knowledge and traits that define who we are requires having the

implementation of a robust identity management system that can be used in determining our individual specific features and characteristics through the provision of unique identifiers in recognising us[9,10]. A general RFID architecture is depicted in Figure 2.

Figure 2: A general RFID architecture



2.1 Classification of technologies

around RFID We identify three classes to order the relation

between RFID and network technologies:

• Enabling technology

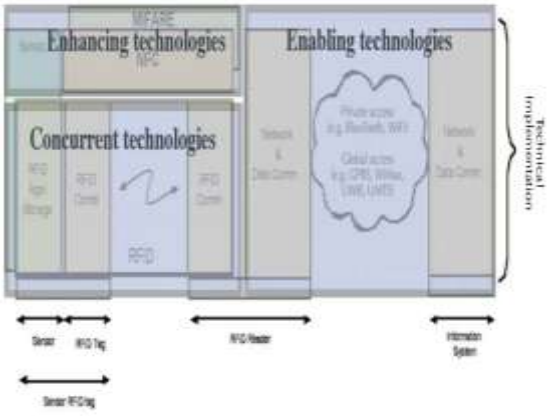
• Enhancing technology

• Concurrent technology

In Figure 3 these classes are mapped onto

the RFID will be used to characterize the different technologies.

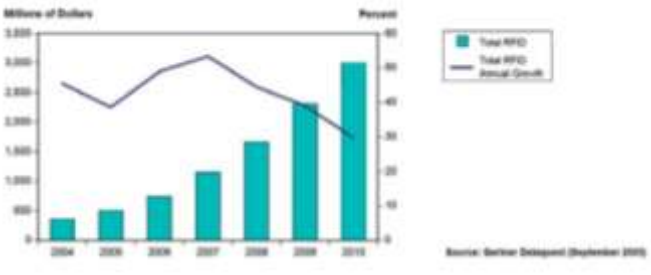
Figure 3: Classification of technologies around RFID



3. APPLICATIONS

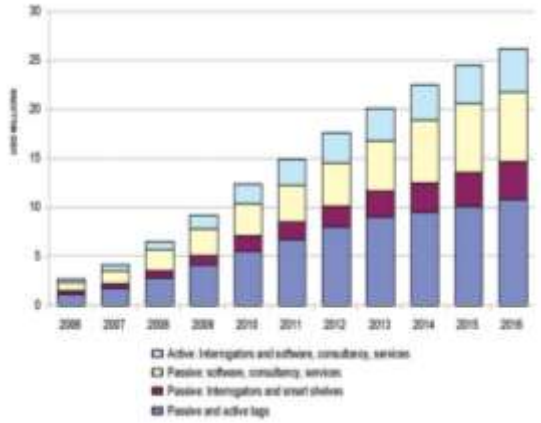
The deployment of a pervasive RFID-based infrastructure in an everyday environment holds the promise of enabling new classes of applications that go beyond tracking and monitoring. Such a system could, for example, support logging and analysis of individual tag movements over time, allowing a user to ask questions such as ”how often do I get interrupted in my office on an average day?”. Current and historical data on groups of tags could also be used to identify and analyze aggregate phenomena such as the impact of seminars on improving communication between researchers. Real-time streams of tag reads could be used in “find my object” applications, reminding services [11,12], and to actuate devices. Enabling these classes of application, however, presents a significant challenge to the system design. First, the system must be able to consistently and accurately read tags and it must do so at a granularity sufficient for the intended applications. The system must support archiving and retrieval of tag reads and real-time reporting of new reads. To enable the monitoring of large spaces with a possibly large number of tags, the system must scale to handle highvolume streams of tag reads. Finally, because such a system will manage large amounts of (potentially sensitive) personal data from multiple users, it must be secure and support an appropriate privacy model. In the following section, we present our preliminary system architecture and discuss how these application requirements affected its design. As an example Gartner (Gartner, 2005b) claims that the RFID market will experience an annual growth rate somewhere between 30% and 50% in the years 2004-2010 ending up at 3 billion USD in 2010 (see Figure 5-7). They say this refers to “the use of RFID technologies within a supply chain environment to improve the visibility, management and security of cargo shipments or supply chain assets, such as conveyances or valuable mobile assets. The applications and hardware that are used outside of the above environment were excluded. These would include consumer uses, such as contactless smart cards.”

Figure 4: RFID, worldwide size and growth, 2004-2010



The IDTechEx report provides some more data as depicted in Figure 5.

Figure 5: Total RFID market projections 2006-2016



4. PRIVACY CHALLENGES

Pervasive RFID-based deployments raise privacy concerns because they can enable the tracking of people and personal objects by parties that would otherwise be unable or unauthorized to do so. These concerns involve: the physical security of the communication between tags and readers, the security of the data stored in and processed by the system, and controlled access to the data. In this study, we focused on the latter problem and studied in-situ many of the privacy concerns experienced by the participants. Chief among the participants' concerns was the perceived ease with which one's activities could be inferred from the data (e.g., time of day, direction of movement, and set of tags seen). We were able to validate this concern by writing a simple script that could detect lunch breaks with better than 75% accuracy for three of the participants, showing that participant P1 took 29 minute lunch breaks on average, P2 took about 32 minutes, and P3 took the longest (40 minute) breaks. Similarly, it was easy to infer potentially more sensitive information such as when and how many times a participant used the restroom in a day. Our initial approach to addressing these privacy concerns was to allow display and deletion of one's personal data via the web interface. The limitation of this approach is that a user can still see another's data before that data is deleted. A more appropriate option would be for users to specify high-level rules that describe which TREs should be accessible to which users and which TREs should be dropped automatically (e.g., all trips from my office to the restroom shorter than 2 minutes)[13]. For example, a query on a colleague's location could return approximate information (e.g., 4th floor) by default, or more exact information (e.g., room 490) only a few times per day. We are currently exploring the suitability of such techniques for various applications. Finally, to protect the privacy of non-participants, each Node Server automatically discards any tag reads for a tag that is not registered in our database[14].

5. CONCLUSION

In this paper, we motivated the benefits of RFID. As mentioned, this technology has many applications is. Studies show that in the near future this technology will be increasingly used and welcomed. By examining the current challenges in the technology and resolving the problems with reliability Khatrbyshtr can use this technology.

6. REFERENCES

[1] Ajay Malik, "RTLS for Dummies," publishing by Wiley publishing. Inc., USA, Indianapolis, Indiana, (2009) ISBN: 978-0-470-39868-5.

[2] J. Zhou, and J. Shi "RFID localization algorithms and applications a review," The International Journal of Intelligent Manufacturing, Vol. 20 (6), Springer Netherlands, pp. 695-707, 2008.

[3] R. Want, "An Introduction to RFID Technology," IEEE Pervasive Computing, Vol. 5, pp. 25-33, 2006.

[4] G. Barber, and E. Tsibertzopoulos, "An Analysis of Using EPCglobal class-1 generation-2 RFID Technology for Wireless Asset Management," IEEE Military Communications Conference (MILCOM 2005), Vol. 1, pp. 245-251, October 2005.

[5] K. Ahsan, H. Shah, and Paul Kingston, "RFID Applications: An Introductory and Exploratory Study," IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 1, No. 3, January 2010.

[6] Benjamin D. Braaten, and Robert P. Scheeler, "Design of Passive UHF RFID Tag Antennas Using Metamaterial-Based Structures and Techniques," Radio Frequency Identification Fundamentals and Applications, Design Methods and Solutions, Book edited by: Cristina Turcu, pp. 324, February 2010,ISBN 9789537619725.

[7] Daniel M. Dobkin, "The RF in RFID: Passive UHF RFID in Practice," Chapter 3: Radio Basics for UHF RFID, (2007), ISBN: 9780750682091.

[8] Smith, J. R. RFID-based techniques for human-activity detection. Communications of the ACM, 48(9), Sept. 2005.

[9] Songini, M. L. Wal-Mart details its RFID journey. ComputerWorld, Mar. 2006.

[10] Stanford, V. Pervasive computing goes the last hundred feet with RFID systems. IEEE Pervasive Computing, 2(2), Apr. 2003.

[11] Sweeney, L. k-anonymity: A model for protecting privacy. IJUFKS, 10(5):557–570, Oct. 2002.

[18] Want, R. The magic of RFID. ACM Queue, 2(7), Oct. 2004.

[12] Want, R. et. al. An overview of the PARCTAB ubiquitous computing experiment. IEEE Personal Communications, 2(6):28–33, Dec 1995.

[13] Want, R. et. al. Bridging physical and virtual worlds with electronic tags. In CHI, pages 370–377, 1999.

[14] E. Wu, Y. Diao, and S. Rizvi. High-performance complex event processing over streams. In Proc. of the 2006 SIGMOD Conf., June 2006