Advantages and Risks of RFID in Business Applications

Vladimir Modrak, Peter Knuth and Jozef Novak-Marcinein
Faculty of Manufacturing Technologies, Technical University of Kosice,
Bayerova 1, 08001 Presov, Slovakia

Abstract: Radio Frequency Identification (RFID) technology in business and industry is rapidly starting to show its growing potential in comparison with other identification technologies. With RFID's expanding role in business applications questions concerning not only gains but also risks are arising. The purpose of this study is to highlight selected areas of this technology that may be critical for its further exploitation in business applications. A comprehensive review approach was used to guide the research process. The relevant literature findings were gathered and sorted into the categories as advantages, disadvantages, readability and privacy security. Differences between RFID and barcode technologies, especially in terms of their use in information management are also discussed in this study. Further, selected critical aspects of RFID development and applications are described. Finally, summative inferences and anticipated expectations of future RFID deployment in business and enterprises are outlined.

Key words: RFID, business, tag, management, bar code, RFID application

INTRODUCTION

RFID (Radio Frequency Identification) technology can be expressed in the most universal manner as wireless identification method, which doesn't need the line of sight to be read or written. It improves communication capabilities of electronic information to be associated with physical items. RFID technology can be basically used in business applications that previously required a bar code or label. The RFID tags are primordially used for identification purposes, such as for employee id/access badges to monitor everyone's whereabouts and credit card account identification. The advantage of RFID tags is that they are small in size and can contain more information than a bar code, which is limited to a single sequence of numbers. On the other hand RFID and barcode technology complement each other because both of them are beneficial in different situations and can be used together in many applications.

RFID devices can be divided into two classes, active and passive. Active tags require a power source, usually a small battery. Passive RFID relies on RF energy transferred from the reader to the tag to generate its own quick response. A passive tag consists of three parts: an antenna, a semiconductor chip attached to the antenna and some form of encapsulation. The main difference between bar code and RFID technologies as stated by Want (2006) is that RFID tags support a larger set of unique IDs than bar codes and can incorporate additional data such as manufacturer, product type and even measure environmental factors such as temperature. Moreover, RFID systems are able to perceive many different tags located in the same area without human assistance. Due to the fact that advantages and risks of RFID are still discussed, this study treats about selected aspects of this technology that may be critical for its further development and applications.

RFID technology advancement: Principles of RFID technology are based on the fundamentals of electromagnetic energy, radio broadcast technology and radar technology. The first active Identification Friend or Foe (IFF) system was developed by the British during world war II. It was radio frequency identification technology for identification of friendly aircrafts. As it has been described by Landt (2001), each aircraft carried a transmitter, which began to broadcast signal back after receiving signals from radar stations on the ground. As further important milestone can be considered the patent on RFID. In the same year, Charles Walton invented access control system based on RFID. The first widespread RFID tag was 1-bit tag (the bit is either on or off) as a part of Electronic Article Surveillance (EAS). EAS could only detect the presence or absence of the tag. In other words if someone doesn't pay, the tag remains on and the readers at the door detects the tag and the alarm sounds to alert un authorized removal. The U.S. government was also supporting research and

Corresponding Author: Vladimír Modrak, Faculty of Manufacturing Technologies, Technical University of Kosice, Bayerova 1, 08001 Presov, Slovakia

development of RFID systems. Los Alamos National Laboratory in New Mexico soon became a leading center for R&D of this technology, as mentioned by Shepard (2005). In this laboratory automated toll payment systems and passive RFID tag to track cows was developed. Both are still using all around the world. Further development lead to use higher frequencies that allowed greater and faster data transfer rates. In 1999 Uniform Code Council, EAN International, Procter and Gamble and Gillette founded an Auto-ID Center project at Massachusetts Institute of Technology for development of RFID standards. The main result of this research was Electronic Product Code (EPC). To other results can be countered air interface protocols (Class 1 and Class 0) and network architecture scheme by linking objects to the internet through the tag. After that Uniform Code Council and EAN International created joint venture EPC global Inc to commercialize EPC technology.

Safety of RFID technology is equally explored as mentioned aspects in its development. To corroborate it by facts the following events can be mentioned. In January 2005 students at John Hopkins University broke encryption of Speed Pass electronic payment and RFID Point of Sale (POS) system. In February 2006 Adi Shamir reported that he could monitor power levels in RFID tag which can be used to compromise Secure Hashing Algorithm-1 (SHA-1) used in some RFID tags (Thornton *et al.*, 2006). However, it is not the reason for a resignation, as a level of risks depends in generally but also in the specific area, on preventive actions. The example supporting this statement offers the situation in privacy protection. In contrast to barcode technology, RFID technology has greater implications on individuals' privacy because RFID tags used in personal identification cards can be read from an abundant distance without that person's knowledge or consent. Therefore, blockers for passport RFID tags in a form of passport jackets containing physical barrier and other countermeasures as unique identifier numbers, encryption and mutual authentication technology has been developed. On the other hand, the more sophisticated protections bring opportunities for potential failures.

MATERIALS AND METHODS

A comprehensive review methodology was used to allow comparisons of advantages and risks of RFID technology across business and industrial applications. Focus of this methodology is based on literature review. Conducted literature research was based on a broad range of sources including journal papers, conference proceedings, industry reports, whitepapers, standards,

press releases and books. Selected explored areas are further verbally analyzed and finally picked aspects are briefly described in the form of the table by focusing on advantages, disadvantages, readability and privacy security of RFID technology.

Critical aspects of RFID development and application: Most practitioners are rather skeptical about the actual utilization of RFID technology taking under considerations more reasons. According to Modrak and Knuth (2009), tag reliability today is considered relatively high by early adopters, at the start of using the tags there was a significant amount of faulty tags. According to the research of the Economist Intelligence Unit by Jacoby and Lofthouse (2006), failure rates in the first generation of RFID tags have been up to 30%. Such relatively high failure rate could not be acceptable, if 100% read rate is essential for successful implementation. Another problem arises due to the fact that tags are read automatically without human interaction. Therefore, theoretically malfunctioned or unreadable tags are not identified by system. This becomes a serious issue for business applications built around RFID if 100% read rates are implicit as part of the core business application design, states (Shutzberg, 2004). Dignan and Nash emphasizes that one of the big reasons why practitioners are less than enthusiastic about these RFID systems is the lack of standards. Standards bodies and academic institutions should harmonize hardware and software standards globally. Until now, most of the standards work has been focused on the US market. China may to be pursuing other standards entirely. Edward Zeng, a member of the China Auto-ID working group, points out that the vast majority of mobile phones in China operate on a GSM standard because Nokia and Ericsson shared their technology more openly than their US-based competitors. In a research study by Hingley *et al.* (2007) has been uncover that in area of supply chain and production management RFID users need to develop not only standardized but also flexible RFID system solutions since they might take into account the context of supply chain power imbalance. This problem comes up when RFID system tracks both ISO tags and EPC tags of varying encoding formats. Then tag decoding tasks can involve significant research. To accomplish this task correctly, developers might work with fairly complex specifications often for multiple tag formats within their application, all of which can add up to a significant amount of new code. Thus, Teskey (2006) thinks that the decoding efforts involved in building a flexible RFID system can be reduced by adopting an RFID middleware platform to perform the decoding tasks automatically, exposing

decoded, meaningful data to applications and business logic through easy-to-use interfaces and development options.

The enormous amount of potentially sensitive data collected by RFID technology makes security a critical aspect in its applications. Therefore, to prevent this risk, the administrative interface, at the lowest level it must be protected by authentication and authorization mechanism. As authentication and authorization protocol can be used so called Secure Socket Layer (SSL) that creates a secure connection between a client and a server, over which any amount of data can be sent securely. However, this protocol is not very commonly used in middleware solutions. Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP), which is designed to transmit individual messages securely.

According to Thiesse (2006), the highest ranked risk by far is the risk of using RFID in order to spy on RFID equipped goods and their owners. In such case consumer privacy is endangered, purchasing anonymity is reduced or eliminated and civil liberties are threatened. Data security of RFID technology depends also on the class and generation of RFID tags. RFID tags are more difficult to replicate, their electronics is more complex than barcodes and barcodes electronics. It was developed new security method uses the concept of random numbers, which are applied to encrypt data sent by the tags so that each message transmitted is unique (Holcomb *et al.*, 2007). Ruefulness, the small sized RFID tag isn't built for that function. Creating smart borders is another application of improving home security together with increasing the security of international shipping containers. According to Adams *et al.* (2006), the contactless IC chip and other RFID technologies are central to the vision of the revolution in border security. RFID attacks can be in general classified into denial of service or relay attacks, sniffing, tracking and spoofing. Techniques like trusted RFID readers or access control mechanism that are located either on a tag like hash locks (Weis *et al.*, 2004), pseudonyms (Juels, 2005) or off the tag are used in order to prevent unauthorized threats and attacks. Off the tag RFID access control mechanisms are for example, Rieback *et al.* (2006) RFID Guardian, RFID Enhancer Proxy (Juels *et al.*, 2005). The Blocker Tag (Juels *et al.*, 2003) and Foe Bud Data privatizer. According to Karjoth and Moskowitz (2005), the easiest way still remains deactivating RFID tag permanently through frying, clipping or as states by Spiekermann and Berthold (2005), killing or temporarily using sleep/wake modes or Faraday cage. In the field of cryptography new low-power algorithms like stream ciphers (Finkenzeller, 2003), block ciphers (Feldhofer *et al.*, 2004), lightweight protocols for authentication (Vajda and Buttyan, 2003) and public key cryptographic primitives have been created.

Risks associated with RFID include also harmful electromagnetic radiation. But according to Wyld (2005), there are no concerns about the risks of the health aspect. One can never be sure but this is scientifically proved. For example frequencies 13.56, 915 MHz and 2.45 GHz have been used for many years without any known problems if levels are <1 watt or 4 watt at frequency 13.56 MHz. Overall, most relevant critical aspects are summarized into Table 1.

RESULTS AND DISCUSSION

It is evident that the most RFID applications have been installed in the fields of supply-chain management systems, transport and logistics. Other RFID applications that already have been successfully deployed are shown in Fig. 1. Especially, as perspective area of RFID application appears to be product life cycle traceability, where the generated product data can be read automatically and forwarded to different information systems.

In the supply chain, the biggest advantage that RFID has over bar code is the ability to automatically read large groups of tags eliminating the labor needed to manually scan the large volumes involved in the supply chain.
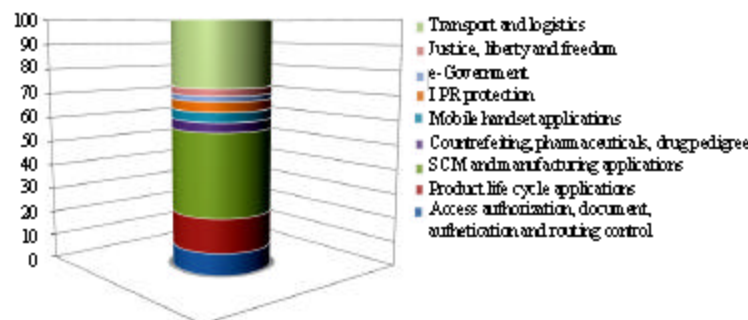

Fig. 1: RFID successful projects by application areas (European research on RFID tags)

Table 1: Picked aspects of RFID in business applications

References	Title	Advantages	Risks (Disadvantages)	Readability	Security (Privacy)
(Myerson, 2007)	RFID in the Supply Chain	Wireless communication, rewritable, automation, better visibility of supply chain, better durability than bar codes	Interference with metals, fluids (for example canned beverages)	Readability can by improved for example by changing metal packages with packages containing less, or no metal	Not mentioned
(Auto-ID Center, 2004)	Technology guide	Automatic identification, automatic data capture, doesn't require line-of-sight, near perfect supply chain visibility	Costs, compatibility, interference with metal and liquids	Readability can be improved by design and appropriate selection of application frequency	Not mentioned
Karygiannis *et al.* (2007)	Guidelines for Securing Radio Frequency Identification (RFID) Systems	Increased efficiency, lower costs	Potential business process risks, unauthorized access risks business intelligence risks, privacy risks, externality risk hazards of electromagnetic radiation	Not mentioned	Unauthorized access of competitors can potentially harm the interests of the organization implementing the RFID system
(Berisso, 2007)	RFID in the Extreme Cold Chain	All tested EPC Class 1, Gen 2 RFID tags are able to withstand cold temperatures	Not mentioned	Very important in achieving1 00% readability is tag placement, antenna configuration and reader setting	Not mentioned
(Baudin and Rao, 2005)	RFID applications in manufacturing	RFID eliminates need of extra labor in compare with barcodes, enhanced warehouse management	Costs of RFID tags, lack of consensus standards, privacy and security concerns	60 % readability was achieved by 12/2004 in Wal-Mart with UHF Gen 1, Class 0 and 1 tags	legislative restrictions of RFID use and related information about customers (security concerns) can slow down RFID deployment by keeping higher costs
(Michael and Mc Cathie, 2005)	The pros and cons of RFID in supply chain management	Non-line of sight technology, labor reduction, enhanced visibility, asset tracking and returnable items, possible item-level tracking, improved inventory management, cost savings	Cost of technology, software and equipment upgrades, privacy concerns	After modifications and trials San Francisco International Airport have achieved 99,5% reliability	RFID can provide anti- theft features for securing the goods
(Soleymani and Zahedani, 2006)	RFID Privacy and Security for ID cards and E-Passports	Physical environment becomes more interactive and supportive by tagging items with chips together with service-enriched backend infrastructure	Privacy concerns, security concerns, possible attacks and fraud concerns	Not mentioned	Encryption, access control and other techniques can be very difficult to implement properly and are unlikely to succeed properly in real world mass applications
(Laran RFID, 2005)	A basic introduction to RFID technology and its use in the supply chain	Reduced inventory and shrinkage, in store and warehouse labor expenses reduction, out-of stock items reduction, anti-counterfeit, improved visibility and automation	Industrial sabotage, industrial espionage, counterfeiting	Not mentioned	Secure tags are pricey, security of data involves not only storage, but also how data is created and transferred

Improving visibility in the supply chain systems gives managers better visibility, which enables identification of bottlenecks and elimination of loss in unplanned operations. Potential benefits of RFID implementation in the supply chain management are counterfeit and fraud reduction, improved efficiency, labor cost reduction, stock shrinkage, stocking management improvements and improved customer satisfaction.

Talking about reliability of automatic identification technology, an attention might be focused on the ability of readers to identify codes from tags at the first time. The possible interferences of bar codes make optical barriers such as objects placed between bar code and reader or dirt. Also, they are unreadable under extreme atmospheric conditions such as steam or when vertical damage occurs. Bar code readers are sensitive to dirt, dust or other foreign object obstructing the lens too. But 2-D bar codes can be read even if part of the tag is destroyed. Passive RFID tags can interference with environments or fields and various materials such as liquids and metals that affect

transmission of radio frequency. Active tags are less susceptible to interference. Despite this, they can be read under extremer weather conditions than bar codes. On the other hand bar codes that could not be read and easily entered manually.

Understandably, there is no universal solution for implementation of RFID at all. It is always necessary to fit RFID system to meet company needs. And because there are numerous types of RFID tags the selection of proper RFID tag system is essential. It is better to start with smaller project and obviously in detail defined problem rather than to fail. But there are a lot of similar solutions that have a typed character. For instance, in income logistics it is often difficult to know what good are on which truck without first unloading the truck. It makes it impossible to direct the truck to the right drop off or parking yard location.

RFID tags can be placed on truck trailers and RFID readers placed at entry and exit points of yards allowing information systems to log the incoming and outgoing data in real-time. Then the incoming trucks can be directed to the most efficient unloading location. The same approach can be applied to forklift drivers at warehouses. The effective RFID-based warehouses management systems have significantly reduced number of pallets and eliminated trucks waiting to the minimum.

Opportunities enabled by RFID are expected apart from abovementioned effects in simplification of business processes. Many manufacturing organizations have processes, where a product, asset, document or even a person is touched by many different people at different times.

It causes limited view of information that can introduce inefficiencies in the overall process when information about other steps is needed to execute the current step. Accordingly, common MES/ERP systems can not have an access to detailed information and they have no idea of what is really happening to material flow on the shop floor. When all data that information systems operate with are fed to them by intermediary subject, information on material flow is time dependent so it is already outdated when inserted into the information system by human operator according to Modrak and Moskvie (2006).

Application of RFID technology for tracking and traceability of material flow will impact the whole performance of information systems in terms of information validity and practically eliminate time dependence of amount and quality of information available for ERP/MES systems.

CONCLUSION

A major problem of today's RFID is a lack of greater motivation to adopt this technology in business application more widely, than in the present. It is mainly resulted from the global crisis and also from the lack of information and feeling that one can not see the code stored in the chip, which makes bar-code technology more human friendly, as noticed by Modrak and Knuth (2009). Mentioned future development of RFID technology will allow better management of in-house and supply chain processes with greater accuracy and provide unprecedented visibility to the material flows.

As regards to readability of RFID tags it is difficult to attain perfect read accuracy in business and other applications. Each of specific objects of identification can influence the readability of the RFID tag in a different way. Kawakita *et al.* (2005) state that in cases where RFID tags must be carried by individuals, some improvement in readability rates might be gained by using signs instructing people to keep electronic devices away from their RFID tags as they pass through the gate readers. They add that even then it would be difficult to reach a readability rate of 100%.

Security and privacy related to RFID technology become increasingly important. According to Maghiros *et al.* (2007), exploration in Europe showed that by respondent's view, RFID breeds relevant privacy threats. Data security of RFID technology depends equally on technical and legislative aspects. In spite of a progress in improving of protection methods, privacy security that is related to RFID presents serious concern of people everywhere.

If RFID technology is to succeed in today's competition, it must be economically passable. Although, RFID already found its place in many industry and business fields it is arguable if its short-term return of investment justifies initial cost of implementation. There are more studies on this issue with positive results (Moskvie and Modrak, 2007).

It is beyond doubt that RFID technology brings asignificant shift to the business workplace. Adoption of RFID in both consumer and business markets will drive greater business volumes thanks to fulfillment customer needs on higher level. The impact that RFID will have on business operations and support infrastructure definitely calls attention to IT specialist to start aggressively planning for RFID. Customer's application development will need further targeted communication to increase awareness and balanced view on RFID technology.

ACKNOWLEDGEMENT

REFERENCES

Adam, N.R., V. Atluri, R. Koslowski, R. Grossman, V.P. Janeja and J. Warner, 2006. Secure interoperation for effective data mining in border control and homeland security applications. Proceedings of the 2006 International Conference on Digital Government Research, May 21-24, San Diego, California, pp: 124-125.

Auto-ID Center, 2004. Technology Guide. Massachusetts Institute of Technology, Massachusetts, USA.

Baudin, M. and A. Rao, 2005. RFID applications in manufacturing. White Paper Draft, California, USA. http://www.mmt-inst.com/RFID%20applications%20in%20manufacturing%20_Draft%207_.pdf.

Berisso, K., 2007. RFID in the Extreme Cold Chain. Center for Automatic Identification, Ohio, USA., pp: 1-5.

Feldhofer, M., S. Dominikus and J. Wolkerstorfer, 2004. Strong authentication for RFID systems using the AES algorithm. Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, Aug. 11-13, Springer, Heidelberg, pp: 357-370.

Finkenzeller, K., 2003. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. 2nd Edn., Wiley, USA., pp: 446.

Hingley, M., S. Taylor and C. Ellis, 2007. Radio frequency identification tagging: Supplier attitudes to implementation in the grocery retail sector. Int. J. Retail Distribut. Manage., 35: 803-820.

Holcomb, D.E., W.P. Burleson and K. Fu, 2007. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. Proceedings of the Conference on RFID Security. Malaga, Spain, July 11-13.

Jacoby, D. and G. Lofthouse, 2006. RFID comes of Age. A Report Sponsored by The North of England Inward Investment Agency. Briefing Paper, The Economist Intelligence Unit. March 2006. http://www.rfidproductnews.com/whitepapers/files/RFID_Comes_Of_Age.pdf.

Juels, A., 2005. Minimalist Cryptography for Low-Cost RFID Tags. In: Security in Communication Networks, Blundo, C. and S. Cimato (Eds.). LNCS. 3352, Springer-Verlag, Berlin, Heidelberg, ISBN: 978-3-540-24301-4, pp: 149-164.

Juels, A., P. Syverson and D. Bailey, 2005. High power proxies for enhancing RFID privacy and utility. Proceedings of the 5th Workshop on Privacy Enhancing Technologies, May 30- Jun. 1, Dubrovnik, Croatia, pp: 210-226.

Juels, A., R. Rivest and M. Szydlo, 2003. The blocker tag: Selective blocking of RFID tags for consumer privacy. Proceedings of the 10th ACM Conference on Computer and Communications Security, Oct. 27-30, ACM Press, New York, USA., pp: 103-111.

Karjoth, G. and P. Moskowitz, 2005. Disabling RFID tags with visible confirmation: Clipped tags are silenced. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES 2005), Nov. 7-7, ACM Press, Alexandria, pp: 27-30.

Karygiannis, T., B. Eydt, G. Barber, L. Bunn and T. Phillips, 2007. Guidelines for securing radio frequency identification (RFID) systems. Natl. Inst. Stand. Technol., 800-98: 1-154.

Kawakita, Y., Y. Uo, O. Nakamura and J. Murai, 2005. Use of RFID at large-scale events. Iatss Res., 29: 31-39.

Landt, J., 2001. Shrouds of time: The history of RFID. The Association for Automatic Identification and Data Capture Technologies, Pittsburgh, PA, USA.

LaranRFID, 2005. A basic introduction to RFID technology and its use in the supply chain. White Paper, Laran RFID, USA.

Maghiros, I., P. Rotter and M.V. Lieshout, 2007. RFID technologies: Emerging issues, challenges and policy options. Tech. Report 22770 EN, European Commission Joint Research Centre's Inst. for Prospective Technological Studies. http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1476.

Michael, K. and L. Mc-Cathie, 2005. The pros and cons of RFID in supply chain management. Proceedings of the International Conference on Mobile Business, July 11-13, USA., pp: 623-629.

Modrák, V. and P. Knuth, 2009. Security and Reliability of RFID Technology in Supply Chain Management. In: Encyclopedia of Information Science and Technology, Pour, M. (Ed.). 2nd Edn., IGI Global, New York, pp: 3377-3382.

Modrák, V. and V. Moskviè, 2006. Elimination of time dependence of information validity by application of RFID technology. Proceedings of the 8th International Conference of Enterprise Information Systems (ICEIS 2006), May 23-27, Pathos, Cyprus, pp: 130-135.

Moskviè, V. and V. Modrák, 2007. RFID In Automotive Supply Chain Processes-There is a Case. In: Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, Sobh, T., K. Elleithy, A. Mahmood and M. Karim, (Eds.). Springer, New York, USA., pp: 475-480.

Myerson, J.M., 2007. RFID in Supply Chain-A Guide to Selection and Implementation. 1st Edn., Taylor and Francis Group, USA.

Rieback, M.R., B. Crispo and A.S. Tanenbaum, 2006. The evolution of RFID security. IEEE Pervasive Comput., 5: 62-69.

Shepard, S., 2005. RFID: Radio Frequency Identification. 1st Edn., McGraw-Hill, New York, pp: 256.

Shutzberg, L., 2004. Analyzing RFIDs reliability and stability limitations. Part Four, Informationweek, Online Article, November 16. http://www. informationweek.com/news/mobility/RFID/showAr ticle.jhtml?articleID=53200075.

Soleymani, H.R. and S.D. Zahedani, 2006. RFID privacy and security for ID cards and E-passports. RFID Seminar WS 05/06 Final Technical Report, TU Darmstadt, Germany. March 2006. http://www.dvs.tu-darmstadt.de/publications/pdf/rfidsem_techreport. pdf.

Spiekermann, S. and O. Berthold, 2005. Maintaining Privacy in RFID Enabled Environments-Proposal for a Disable-Model. In: Privacy, Security and Trust within the Context of Pervasive Computing, Robinson, P., H. Vogt and W. Wagealla (Eds.). Springer Science and Business Meida Inc., New York, pp: 137-146.

Teskey, M., 2006. Turning RFID data into information. Online Article. http://www.devx.com/enterprise/ Article/32251/0/page/4.

Thiesse, F., 2006. Managing risk perceptions of RFID. Auto-ID Labs White Paper, WP-BIZAPP-031.

Thornton, F., B. Haines, A. Das, H. Bhargava, A. Campbell and J. Kleinschmidt, 2006. RFID Security. 1st Edn., Syngress Publishing, Inc., Rockland, MA, USA., ISBN: 1597490474.

Vajda, I. and L. Buttyán, 2003. Lightweight authentication protocols for low-cost RFID tags. Proceedings of the 2nd Workshop on Security in Ubiquitous Computing. Seattle, Washington, USA., October 12, 2003.

Want, R., 2006. An introduction to RFID technology. Perv. Comput., 5: 25-33.

Weis, S.A., S.E. Sarma, R.L. Rivest and D.W. Engels, 2004. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Security in Pervasive Computing, Hulter, D. *et al.* (Eds.). LNCS. 2802, Springer-Verlag, Berlin, Heidelberg, ISBN: 978-3-540-20887-7, pp: 50-59.

Wyld, D.C., 2005. RFID: The right frequency for government: A research monograph from the IBM center for the business of Government. http://www.businessofgovernment.org/main/public ations/grant_reports/details/index.asp?gid=232.