Security analysis of RFID based devices in educative environments

Ahmed Saeed Alzahrani

Department of Computer Science, Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah 21589, Saudi Arabia.
asalzahrani@kau.edu.sa

Abstract: Educative environments such as public and private academic institutions are established with latest information communication technology (ICT) which includes RFID based devices. Innovation of academic infrastructure using latest ICT with maximum security is a future development in most of academic applications. Regarding the RFID based devices involved in educative environments; the level of security must be reconsidered in some applications. For instance different applications such as library, car park, laboratory etc. need different levels of security. However, there is a security problem, which is a practical challenge considered between the RFID reader and RFID tags. If more than one RFID card or tag is held by the user, more than one user is registered by the reader at the fixed time intervals. It means that monitoring of students' attendance is recorded wrongly and students who are physically absent may be involved in the serious criminal activities. In order to avoid this problem, security analysis of RFID based devices in educative environments is a potential challenge. In this paper, a theoretical model of RFID based device with security protocol is considered to employ in educative environments. Possible security analysis expected to use in educative environments are mentioned as research methods because RFID devices in latest ICT need reasonable security which must be low-cost and maximum efficiency. From these model, students will gain not only learning capabilities but also they will achieve physical and mental fitness. Even though security is not a direct impact, its influences in this model create the peaceful time to increase the listening attitudes. Memory capacities also increased through this model, because it is directly influenced with listening, learning and punctuations.
[Alzahrani A. **Security analysis of RFID based devices in educative environments.** *Life Sci J* 2014;11(1):133-140]. (ISSN:1097-8135). http://www.lifesciencesite.com. 20

Keywords: RFID based devices, Educative environments, RFID Security, Learning capabilities

1 Introduction

Evolving technology with RFID based devices and security is the one of the growing areas in all profit and non-profit sectors. In this paper, we are focusing on most of the security facilities used in the non-profit organizations such as schools and universities etc. Scientists invented a lot of new security algorithms integrated into new technologies, but they have not been used properly to public services. If RFID based devices are established for educative environments, at least 70% of the people will have or achieve reasonable knowledge with security and privacy [25, 26]. Cipher bullying is one of the examples for security threat being highlighted in educational environments.

The security of RFID in educative environments improves the direct academic service and control of goods in academic managements, decreases theft and faults, increases anti-forgery, eliminates wrong data entry and prevents complications between similar books or the books that have similar codes.

RFID is a latest wireless technology used for identification purposes. Any person or object identity is in a form of unique serial number transmitted using radio waves [1, 2]. Many automatic identification technologies are using RFID. Some of the technologies such as; bar codes, biometric, optical character recognition are used to reduce the manual efforts, cost and time. These technologies are referred as Auto-ID technologies.

General analysis of RFID security in educative environments needs to resolve the potential problems such as strong security in attendance monitoring, confidential data handling between the RFID devices, etc. Mitigation strategies of these problems are available to enhance the privacy and security. Encryption techniques, anti-collisions, filters and RFID tag holders are some of the mitigation strategies used between the RFID base devices and systems. As expected results, many security problems including cipher bullying will be resolved through this research and analysis.

The rest of the paper is organized as follows. Related work of RFID based devices for educative environments in Section 2. We discuss proposed RFID system in Section 3. In Section 4, recommendations are discussed. Final conclusion will be in Section 5.

2 RFID Based Devices

Auto-ID technologies also enhance the precision and accuracy of the data. But RFID offers more benefits including security than the auto-ID technological systems. RFID Tags are the labels which RFID systems utilize to identify an object. This tag is attached to an object which is to be identified. There are different types of tag; either it is battery assisted passive, active or passive tag. Active RFID tag periodically transmits the identification signals having an onboard battery. Passive tag has no battery. Passive tags are also smaller in size and cheaper. RFID tag has a receiver and a transmitter.

RFID tags restrain at least two parts: an antenna and an integrated circuit. Antenna is used for transmitting and receiving signals, while as integrated circuit is used for specialized tasks such as collection and processing the information etc.

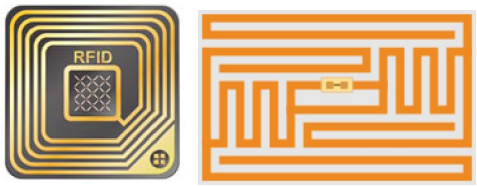

Figure 1: RFID chip

2.1 Technical characteristics of RFID

In most of educative environments, some technical characteristics of RFID are directly influenced with security [3]. Following technical characteristics will help us to develop correct security algorithms for which RFID devices is used in educative environments.

Data read and write

Huge memory capacity of data

Distance between the reader and tags

Active and passive power levels

Security analysis of RFID based devices can be used for which many smart applications are integrated with educative environments. One or more of following smart approaches may be integrated with educative environments.

- Smart Cities
- Smart Parking
- Smart Environment
- Smart Water
- Smart Metering
- Smart Agriculture
- Smart Animal Farming
- Smart Health

Education sector is one of the most important sectors that needs for the implementation of latest technologies. RFID can be used for multiple purposes in the educational sector. Some of the uses of RFID are as follows;

2.2 Tracking system for student's safety

The student's safety and security is a challenging task for the school management as well as parents or guardians' responsibility. Regarding the students' behaviour and safety, the school management and teachers are facing significant challenges to introduce the security within the educative environments. Children and school bus location can be easily traced. Also the bus speed can be controlled while continuously monitoring the activities inside the school bus. So far the satisfaction of the parents, teachers and school staff, tracking and identification can be achieved through the latest communication technology such as RFID systems [26].

2.3 Campus Management

The security in campus management is one of the problems in educative environments. Handling large data is still in complicated problem because security is not efficient. When the data managed manually or using conventional methods, there are many flaws in the existing campus management systems. So by introducing RFID devices integrated with security in campus management system, all these flaws can be solved perfectly. Here, the level of the security should be considered according to the applications.

2.4 Library Management

Now a days, library system use on-line approach for most of the daily activities which include collection and storage of e-books, and administrations. Within the library environment, short range of RFID devices can be used with reasonable security. Library uses internet facilities for quick information with existing network technology. Internet security is employed to protect the library management system from unwanted data. To enhance the security in educative environment, latest RFID network management for next generation network is being developed with flexible security. For instance, RFID EAS (Electronic Article Surveillance) anti-theft gate can be used for library management system which is easy to integrate with next generation network.

2.5 Employee's access and management

The education environment should provide all employees secure solution to access and manage their personal information confidentially. Following two problems may be concerned to maintain the employees' access and management system with security.

- Managing passwords in a security-rich fashion
- Integrating with an enterprise identity management system

In above cases, single sign-on approach is used to enhance the security [27]. To improve the security in

educative environments through the RFID devices, available security algorithms can be applied to increase the efficiency [24].

Authentication factors, Access Agent, Identity Wallet etc are some of the security solutions may be analyzed to enhance the employees' access and management. There are plenty of other options, which may be analysed through the RFID devices or systems used in the educative environments [17].

Password self-service and Strong authentication using RFID are also examples to enhance the security in selected fields of educative environment. In the employees' access system, efficient security should be implemented according to the field. In order to handle these problems, RFID based security system can be introduced as a new device which is going to solve a number of potential problems in educative environments [13, 14].

The e-reader integrated with most of the wireless devices is available for those who are interested to read academic books and relevant books for academic supports. Wireless devices and RFID devices are merged with wireless networks. There is a number of security algorithm employed in wireless networks. The e-reader can be interacted using RFID devices, which will provide instance performance of students' reading capacity. The security of wireless networks provide a number of advantages to those who use RFID devices in the educative environment [15].

There are plenty of RFID based devices used around or in the educative environments where security is one of the potential challenges. In this paper, specific RFID based devices which need some form of security with low and high complexity will be considered as a basic understanding and illustrations of the potential problems. This device will detect what students have done for last 12 hours because physical and mental conditions should be relaxed to comprehend the lessons. This device will help not only to students' learning and listing attitude but also it provides maximum improvement of suitable security for academic curriculum used in educative environment [16].

3 RFID based systems with security

Regarding the security enhancement, educative environments use a number of RFID based systems given below.

- Notification system
- Security system
- Experimental system
- External monitoring system;
- Open learning system

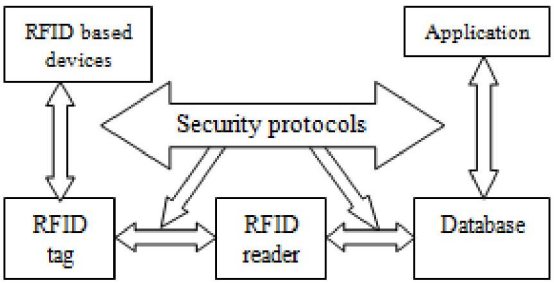

Figure 2: RFID system and security protocols

RFID based devices dominated in most of the applications need some form of the security. Figure2 shows the device interactions in RFID systems, which are already implemented in some campuses. This system can be used for students' activities whether their applications are specific or multiple purposes in the educative environments [18, 19].

RFID campus is one of the examples for the educative environments. Above mentioned systems are elaborated with potential wireless technology and security systems.

In the RFID based systems, confidentiality, integrity, availability and non-repudiation are considered as security objectives, which can be deployed in educative environments [5, 6].

3.1 Security risks of the RFID based systems

Following attacks are considered as security risks in RFID based devices allowed to use in educative environments. Counterfeit RFID tag, replay, eavesdropping electronic collisions and introduction of rogue components are some of the several attacks influenced in RFID based systems.

3.2 RFID security risks and mitigation strategies

In order to prevent the unauthorized readings from RFID tags, following mitigations strategies such as encryption, hash algorithms, Faraday cage, PIN, reader security protocols, etc. can be used in RFID based systems.

3.3 RFID tag power requirements

The tag read range is limited solely by power restrictions and obstacles placed on the system. A tag typically requires about 100µW (-10dB) of power to communicate. When a typical radio link budget is examined, the maximum theoretical read range of a passive UHF tag is around 5.8 m (19.4 ft). This distance is derived from the Friis Equation.

$$R \le \frac{\lambda}{4\pi}\sqrt{\frac{EIRP_{reader}G_{tag}}{P_{tag}}} \quad (1)$$

R is a read range of Effective Isotropic Radiated Power (EIRP) reader.

P_{tag} is the power require at RFID tag antenna

G_{tag} is the tag antenna gain

λ is the wavelength of the frequency in use

The EIRP can be related to the power transmitted from the radio (P_t), the cable losses (possibly including antenna mismatch) L, and the antenna gain (G) by:

$$EIRP = P_t - L + G$$

Low-frequency passive RFID-tags use inductive coupling which requires the RFID tag to be within the range (R) of the RFID reader.

3.3.1 RFID and e-reader

Reading habits should be monitored through the counting words per hour and some quick questions. In order to implement such a system, RFID based device can be implemented with e-reader, which is connected to a network. Here, necessary security can be implemented with e-reader to protect confidential information. Word counting is monitored daily and performance of the students' participations is recorded in the server. From these points, students' reading ability and behaviour can be monitored [20, 28].

3.3.2 RFID and e-writer

It is another way of improving students' learning capability in the educative environments. Reading and writing are comprehension of academic subjects, which should be monitored during the academic hours. RFID tag and e-reader must check correct identity of the student who participates in writing. As a security, source and destination must be checked correctly before e-writer is used in public places of educative environments because valuable and confidential information may be end up in wrong destinations. The actual design of the proposing system will be explained in the next section.

3.4 RFID in educative environments

RFID library is the one of the best example for educative environments where RFID based devices are already implemented. The question should be raised "do all students use library or any educative environments for their correct academic benefits?" Only 40% of the students understand the problems for increasing their knowledge. Rest of them is using these educative environments for just pass the exams and struggles when they face the real life. It is not acceptable in future educative environments because each student's work is monitored throughout the academic period [21, 22].

3.4.1 Activity for specific and multiple applications

Virtual laboratory for certain age groups in educative environments can be built using RFID based devices which help students to interact the laboratory exercises without wasting time, materials and testing equipments again and again. As mentioned in [7, 9, 10], RFID devices can be implemented in where same experiments are simulated repeatedly. Hence, virtual laboratory and RFID devices can be used for specific applications.

According to [11, 12, 23], activity for multiple applications can be developed and encouraged the students' learning capabilities in the educative environments [24, 28].

3.4.2 RFID security for selected applications

The RFID Security analysis that includes privacy was conducted in concert with the feasibility study. In order to analyze the security and privacy study, the following objectives employed in educative environments can be considered.

- Analysis of security and privacy issues that arise from proposed design
- Available technology to prevent above mentioned issues in educative environments
- Future recommendations to enhance the security and privacy in the proposed system

4 PROPOSED DESIGN

In this section, basic model of the RFID based device for educative environments is designed with security protocols. Reading, writing interactions and other data handling should be protected. Following figure explain the details of the design including the RFID security protocol, which can be used in the educative environment.

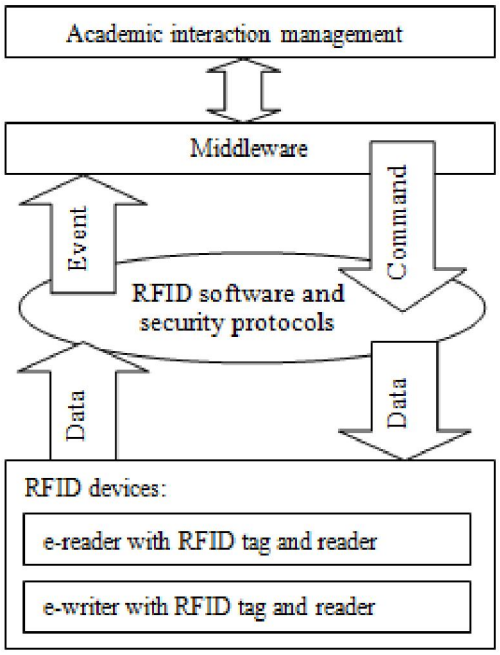

Figure 3: Security protocols of RFID system for educative environment

As shown in Figure 3, the proposed system can be designed with RFID devices. The reading part of the block diagram shows the word counting and

interaction between the students' participations during the fixed period. The RFID device will monitor the exact results dynamically. Also, statistical details of reading habits will be accumulated for overall performance of the students' behaviour.

The writing represented in Figure 3 counts words as well as security because interaction between the particular student and his/her writing should be monitored dynamically.

Security may not be enough because it can be increase according to the request which is the level of the protection for particular service used academic environments.

4.1 RFID security protocol

The protocol used in this proposed design is located to handle the communication between the middleware and RFID devices. RFID middleware used in proposed design assists with the filtering, aggregation, and routing of RFID data. It has built-in security and privacy rules that monitor the data stream of academic information and direct data to appropriate academic systems. It is used to manage data flow between the RFID networks and the IT systems within an academic organization. Figure 4 shows the details of RFID security protocol.

Transport layer: Networking with RFID devices in the educative environments
RFID security layer: Security algorithms processing, services Data framing, connection authorization
Reader layer: Information from RFID tags used in or around the educative environments

Figure 4: RFID security protocol

4.2 Benefits of proposed RFID system

It provides plagiarism detection dynamically to those who don't involve in enough reading, and writing in their academic life. Every student must be involved in reading and writing about their subject, which provides the fundamental knowledge of the concept. Students' real hard working must be monitored through this system.

4.3 Scenario of Security in RFID system

Mobile phone can be used to establish the strong security between the RFID reader and RFID tags which are active type that needs internal power. It means that active type RFID tags should be activated through the internal battery or some power source.

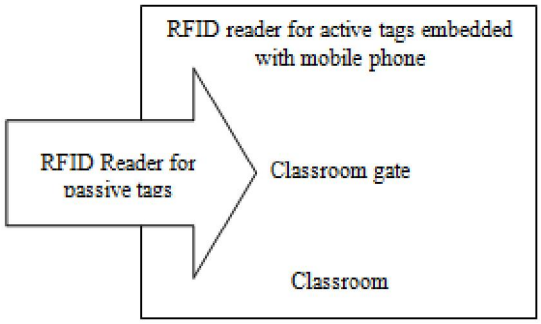

Figure 5: Student attendance with RFID security

When students are entering through the classroom gate, reader identifies the tags that are embedded with mobile phone. As a strong security, finger print is registered as a security code that provides the power to active RFID tags used in mobile phones. When active RFID tags are powered up, RFID reader located in the classroom reads the necessary personal information from the tags attached with student's mobile phones.

Mobile phone is a personal and its 99% of the information and personal data are private and confidential. So, whatever happens mobile phone is not exchangeable between the friends or close relatives.

Following ways are few technological approaches which can be applicable to increase the security in future protocols employed in RFID devices.

Encryption: Registration details including serial numbers and personal details should be encrypted. Even though it provides greater data security, it expects the significant challenges of employing technology between the RFID based devices. Encryption may not be useful for monitoring attendance directly but it increases the complexity. So, compromising strategy is very important to make a best RFID based devices with reasonable security and low-cost.

Tag password: In order to protect the data handling between the RFID tags and reader, password can be considered as a possible solution. If tag receives expected password, tag provides the authorization to continue the monitoring. However, valid password creations and managements are also some of the challenges because data size of the active and passive RFID tags are involved in the system.

Tag pseudonyms: It is another approach but password of the RFID tags is not changed. Instead of this password, serial number is changed each time dynamically. It is good for monitoring and tracking because unauthorized situations are minimized.

These are just some of the approaches that can help new security to RFID implementations.

5. Security Analysis and Discussion

One of the second generation problems in RFID devices which use for educative environments is security and privacy challenges that affect the students' behaviour that increases their listening and other activities.

Innovations given in [24], RFID can be implemented to track DNA (Deoxyribo Nucleic Acid) which provides high security to monitor the students' attendance in the next generation scheme.

The central challenge for the educational environments industry is not only in the development of the security protocols, encryption methods, reducing the physical size or in more ubiquitous devices, but in the development of standards and policies and human-computer interfaces that help to provide the appropriate visibility, use and control of information.

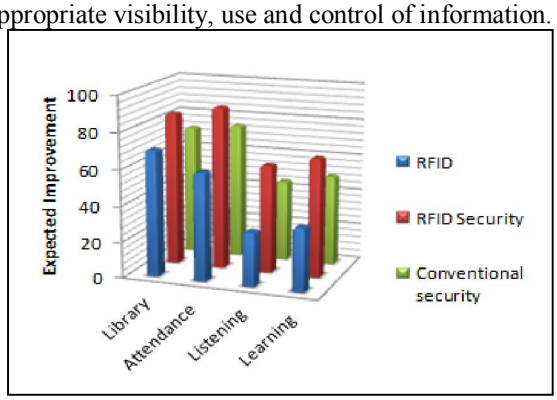

Figure 6: Security in educative environment

In the future educative environment, RFID can be used to enhance the security as well as capacity related to students' behaviour which is very important factor in the academic life. Attendance is the basic parameter which provides necessary skills to increase the listening and learning capacities that depend on the secured data and signals. As shown in figure 6, expected improvement is shown in percentage for which educative environments achieve the reasonable level through security compared with individual area.

Regarding the security analysis in RFID system, future Internet linked between the educative environments is being developed with a number of new technologies and innovations. Still, security issues are the biggest demand in all over the world because security algorithms invented and being used in many applications are hacked by some hackers. It happens every day but, none of us can control this problem. Still, this kind of problems is growing all over the world where each country is fighting to find the solutions either political or technical ways. These security problems must be solved using combined solutions, which mean political and technical solutions must be combined during the implementations. Technical experts and standardization committees must combine these two solutions, which will become a better security solution for all computer communications, as well as all other systems used in different academic communication applications. We will investigate these problems with more details, which include all current and future problems with relevant security issues.

In computer communication connected within the educative environments and Internet applications, RFID technology takes maximum roles in all aspects of the security systems. It helps everybody from basic enquiry stage to final operation or surgery stage. Currently, key challenges of security focusing with RFID technology are many, some of them are identified and some of them are unidentified.

Wireless communication including RFID technology is heavily used in medical communication [8, 9, 10]. The readers or the tags of the RFID communicate over the shared wireless channel. Hence, the collision problem occurs during the data or signal transmission. These collision problems prevent to reach the target destination or tag which reader is aiming for. Because of the prevention which creates the delay in the transmission, hackers and eavesdroppers can enter easily and spend more time to crack the code or message. The authentication is one of the security threats [11, 12] when we use RFID technology in academic applications. In order to prevent this collision problem in the RFID based system and its communication, an efficient anti-collision protocol should be developed.

As a related problem, practical ARQ-Based security schemes for Wi-Fi and RFID networks are outlined [13, 14, 15]. Our proposed schemes are enhanced through the confidentiality and authenticity functions of these networks, respectively. Both security properties can be used in our applications when security threats and attacks are involved in the ICT communication network. In order to prevent the security threats and attacks between the RFID tags and readers, secret keys can be applied with proper cryptographic algorithms. Keeping continuous key update will prevent all the potential attackers and eavesdroppers who actively involved within the system which includes ICT communication and RFID networks.

6 Recommendations

Efficient security algorithms are recommended to maintain the future security in educative environments. Table1 shows expected security problems and available security algorithms used in educative environments.

Following recommendations are very fundamental issues in current educative environments.

Table 1: RFID Security Analysis

Expected security problem in RFID system	Security algorithms for educative environments
Counterfeit Attacks: Confidentiality Integrity	Encryption EPC Tag PINs Physical shielding sleeve One-Way Hash Locks Selective Blocker Tag
Eavesdropping Attacks: Confidentiality	Encryption EPC Tag PINs Physical shielding sleeve Selective Blocker Tag RSA Countermeasures
Electronic Collisions: Availability Integrity	Anti-collision Algorithms RFID Distribution and Assignment
Replay Attacks: Availability Integrity	EPC Tag PINs Physical shielding sleeve One-Way Hash Locks Selective Blocker Tag

RFID based device will change the student's attitude around the world and encourage to understand the academic values. Detecting the student ID and name of the student who plays bad games, which are not suitable for that particular age is the important feature of the device. Most of the bad games are supported by older people who don't understand the academic value. The bad and violent games are not suitable for certain ages but still they are used uncontrollably in most of the places around the world. The students' learning capability is changed after they play such bad games within the educative environments.

World is facing bad economic situations and global worming effects. Why? Children are terrified by the bad games which creates the unfit physical and mental conditions when they are studying in the educative environment. Children are the future of the world. If educative environment provides proper security in each action of academic fields, students will understand the future with 100% correct knowledge. Why cipher bullying is spread in educative environments? RFID device should be able to identify the students who are really involved in the bad games within the academic premises and provide correct warnings as punishment.

7 Conclusion

Security analysis of RFID based devices have been studied for providing the correct security and privacy, which will help to protect the student's activities in the educative environments. Most of the students' academic information is private and confidential. So they must be protected through the security mechanism which deals with RFID environments. It also increases the memory capacities because students are occupied with interactive programs when they are in the class rooms.

Listening with interactive programs using e-reader embedded with RFID tag increases the observations and real actions in the educative environments. Using e-writer, students will be able to check their plagiarism issues within the class room because it is still depending on RFID network systems.

We hope that all the children will get maximum benefit through this device that has an efficient security algorithm, and they will be encouraged to follow the academic principles for real life.

References

1. Junhuai Li, Hongying Liu, Jing Zhang (2008), Design and Implementation of an RFID-Based Exercise Information System, Intelligent Information Technology Application, IITA '08. 2nd International Symposinmm 2008.
2. Andrew J. Kornecki, Thomas B. Hilburn, Wojciech Grega, Miroslav Sveda, Jean-Marc Thiriet (2007) "ILERT - International Learning Environment for Real-Time Software-Intensive Control Systems", Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 943 – 948, 2007.
3. Xiangming Mu, Gary Marchionini, and Amy Pattee (2002), The Interactive Shared Educational Environment: User Interface, System Architecture and Field Study, School of Information and Library Science University of North Carnolina at Chapel Hill, 2002.
4. Gonzalo Espejo, Nieves Ábalos, Ramón López-Cózar, Zoraida Callejas, David Griol (2010), A System for User Location by Means of RFID Devices for a Dialogue System Designed to Interact in an Ambient Intelligence Environment, VI Jornadas en Tecnología del Habla and II Iberian SLTech Workshop.
5. Che Yahaya, Norrozila Sulaiman (2009), An Investigation on a Real Time System over WiFi in Educational Environment, Sixth IFIP International Conference on Network and Parallel Computing.
6. Carlos Perdigao and Miguel L. Pardal (2008), EPC Virtual Lab: Experiments using an RFID location simulator, Portuguese Foundation for Science and Technology.
7. Tsung-Yu Liu, Tan-Hsu Tan and Yu-Ling Chu (2009), Outdoor Natural Science Learning with an RFID-Supported Immersive Ubiquitous Learning

Environment, Educational Technology & Society, 12 (4), 161–175.
8. V. Drona, S. Drona, C. Rusell, M.H.N. Tabrizi (2009), RFID Based Learning Assessment System, Issue 6, Volume 8, June 2009.
9. Ahson, S. A., & Ilyas, M., (2008). RFID Handbook, Applications, Technology, Security, and Privacy, CRC Press, FL, USA, ISBN: 978-1-4200-5499 6.
10. Klaus, F., (2010). RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition, John Wiley & Sons Ltd., West Sussex, UK, ISBN:978-0-470-69506-7.
11. S.A. Weis, S. Sarma, R. Rivest, and D. Engels. (2004), Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Computing, pp: 201-212.
12. Bacheldor, B. (2009). Farmacias del Ahorro Prescribes RFID to Track Assets. Mexico: http://www.rfidjournal.com/article/view/4535
13. Bacheldor, B. (2006). Wi-Fi RFID System for Long-Term Care. RFID Journal, Inc
14. V. Thayananthan, A. Alzahrani, M.S. Qureshi.(2012). Analysis of key management and Quantum Cryptography in RFID networks. International Journal of Academic Research Part A; 4(6), 152-157.
15. V. Thayananthan, A. Alzahrani, M.S. Qureshi.(2013). Trellis Coding based on RLLPUM Codes for RFID Reader-to-Tag Channel, Australian journal of Basic & Applied Sciences, 7(4), pp. 708~717.
16. Burmester, M., & Munilla, J. (2010). A Flyweight RFID Authentication Protocol. Spanish Ministry of Science and Innovation , Vol. V, No. N, January 2010.
17. Chien, H.-Y. (2009). The Study of RFID Authentication Protocols and Security of Some Popular RFID Tags. Development and Implementation of RFID Technology, pp. 261-290, Department of Information Management, National Chi Nan University.
18. Juels, A. (28 September 2005). RFID Security and Privacy:A Research Survey. RSA Laboratories, pp. 1-19.
19. Liu, H., Bolic, M., Nayak, A., & Stojmenovi, I. (2008). Integration of RFID and Wireless Sensor Networks, Chapter 13. SITE, University of Ottawa, Ottawa, K1N 6N5, Canada, pp. 1-29.
20. Mitrokotsa, A., & Douligeris, C. (2009). Integrated RFID and Sensor Networks: Architectures and Applications. Netherland: Book chapter.
21. Nordby, K. (2010). Conceptual Designing and Technology:Short-Range RFID as Design Material. The Oslo School of Architecture and Design, Oslo, Norway: International Journal of Design Vol.4 No.1, pp. 29-44.
22. Ramli, T. S. (2006). Radio Frequency Identification (RFID), Wireless Network. Malaysian Communications and Multimedia Commission (SKMM), http://www.skmm.gov.my/link_file/what_we_do/Research/industry%20studies/RFID.pdf.
23. Roussos, G. (2008). Networked RFID System, software and services, Springer, London.
24. Song, B., & Mitchell, C. J. (2008). RFID Authentication Protocol for Low-cost Tags. WiSec'08, March 31–April 2, 2008, Alexandria, Virginia, USA.
25. Swedberg, C. (2010). Bode Technology Launches RFID System to Track DNA Evidence. RFID Journal, http://www.rfidjournal.com/article/view/7654, pp.1-5.
26. Ahmed Alzehrani, Vijey Thayananthan, and M. Shuaib Qureshi. (2012), RFID based Devices for Educative Environments, 14th International Conference on Enterprise Information Systems (ICEIS)-IDEE, Wroclaw, Poland, pp. 131~136.
27. IBM Corporation, "Enhancing Password Management by Adding Security, Flexibility, and Agility," IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A. 2012
28. V. Thayananthan, A. Alzahrani, M.S. Qureshi. (2012). RFID based Devices for Educative Environments, 14th International Conference on Enterprise Information Systems (ICEIS)-IDEE, Wroclaw, Poland, pp. 131~136, June 28-July 1, 2012.

1/6/2014