Comprehensive Appraisal on Embedded RFID Security and Privacy Concerns in Scholastic Management System Restraining Adaption

Zainab Rasheed Fahad Mirza[1] and M Nawaz Brohi[2]

[1]*Central Registry Academic Services, Higher Colleges of Technologies, Abu Dhabi, UAE*
zfahad@hct.ac.ae
[2]Head of Campus, Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology Dubai, UAE
mnbrohi@szabist.ac.ae

Abstract: This paper explores security and privacy issues related to Radio Frequency Identification (RFID) implementation in scholastic or educative environments. Various educative environment domains: Student management, Staff/Faculty management, Visitor Management and Campus Security have increased utilization of RFID applications but has reduced or limited ubiquitous adoption due to serious and potential security and privacy concerns, which are still existing due to lack of security standards in current RFID hardware and software technology.

This research is on security and privacy problems and standards required particularly for educative smart campuses various domains. RFID limitations due to data privacy does not make it an entirely secured solution for any industry including academic industry but still the popularity of RFID has been increasing massively worldwide and various applications are been developed for various industries due to its numerous benefits. As in many industries RFID benefits, convenience and cost effective implementation weigh more than privacy risk concerns.

Still the importance of protecting user privacy in this case student and faculty privacy and data privacy cannot be overlooked and it is the most important obstacle which needs to be overcome so that the smart educative environments may take advantage or RFID technology. At the end RFID system implementation guidelines for a smart educative environment are suggested which can be followed until we get a definite solution to RFID security and privacy which is practical, scalable, and protects from all kinds of attacks. Security analysis of RFID based devices in educative environments is currently a potential challenge.

Keywords: Scholastic Environments, Embedded RFID Security, RFID Security, RFID privacy, RFID protocols, consumer merchandising, healthcare, tagging livestock, food industry, shipping, toll ways, manufacturing, retail commerce.

1 INTRODUCTION

RFID technology is a cutting edge technology which exists from decades but has been now introduced and utilized in various industries including inventory management, supply chain, antitheft monitoring on consumer merchandising, healthcare, tagging livestock, food industry, shipping, toll ways, manufacturing, retail commerce, library services as well as payment cards, personal identification cards and documents are applying RFID systems numerous benefits and cost effective solutions **[1].**

RFID has many perfect features such as completely non-contact, low cost, data reliability, high recognition rate, feasibility, high efficiency, secure access control, quality and easily be intergraded by existing management information system.

RFID system implementation in smart educative environment has been wide spread, although its application in various campus domains are still been developed. RFID implementations in smart campus system has been excelled and also been taken to clouds. Various educative environment domains suggested are authentication, student, staff and faculty location tracking, visitor management and campus security which include asset security, student valuable security, exam hall seating, exam paper security and authentic certificate security **[2].**

RFID in educative environments transfers data automatically to databases using RFID applications. As a result, RFID technology is useful in achieving better staff, Student and asset security control, as well as to improve security of campus environment. To this purpose, current RFID applications been developed to automate the student security supervision and also provide integration with current security management system for academic industry.

Corresponding Author: [2]M Nawaz Brohi, [2]Department of Computing, Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology (SZABIST) Dubai, UAE

In RFID systems, RFID tags are embedded in all moving devices and humans, including student, faculty staff as well as campus and students assets. Campuses main departments and main terminal points are equipped with RFID intelligent terminals including RFID readers to support automatic data a scanning and location tracking. Currently all U.S. passports and credit cards contain RFID's. Future applications of RFID include retail stores scan it yourself aisles with few checkout stations for disabled. Medical industry in exploring the usage of implantable RFID chips for effective patient management **[3].**

Despite of numerous benefits of RFID technology few areas of no security standards, limited data and user privacy, hinders in the substantial growth of RFID System adoption specifically in scholastic environments. Regardless of RFID systems growing attractiveness, its applications for all industries carry with them substantial privacy and security risks for individuals. Few identified and researched on privacy and security problems are targeting or tracking of individuals, or the potential disclosure of personal practices or preferences to unauthorized third parties, and how it could be attacked at any part of the RFID system (between RFID tag and reader attacks, middleware attacks and Backend station attacks) **[2].** These problems need to be addressed and requires real and practical solutions which are been researched by RFID industry.

This paper is specifically to focus on privacy and security concerns for RFID technology and Scholastic industry implementation may be limited as a result. An apparent lack of security standards within the RFID domain and specifically in scholastic environment may hinder the growth and utility of RFID within academic industry for the foreseeable future. As awareness of the potential pitfalls and RFID special requirements in the smart educative environments domain is required therefore we should have some implementation guidelines to be followed for RFID systems integration until certain security standards are developed. Basic RFID technology standards are given in ISO 18000's part 1-4, 6 and 7 standards which describe the use of RFID for item management. While EPC global Inc. which is one of the predominant industry driven standardization efforts in the RFID community, has standard "Class-1 Generation-2 (C1G2) Ultra High Frequency (UHF) RFID Protocol for Communications at 860MHz - 960MHz" similar to the ISO 18000 Part 6C standard. This paper focuses on working on passive tag security and privacy solutions as they have benefit of low cost.

The rest of the paper is structured as follows. A background on how RFID works especially in educative environments in Section 2. Section 3 is about RFID applications implemented in educative environments and there effects. RFID system security and privacy problems and their available solutions are discussed in Section 4. Section 5 describes implementation guidelines for RFID systems in educative environment. Final conclusion will be in Section 6.

2 BACKGROUND

Radio frequency identification (RFID) technology is an automatic identification system which transmits and receives information without wires and can communicate through a distance using radio waves. A tag has a unique identification number (ID) and a reader recognizes an object through consecutive communications with the tag attached to it.

An RFID technology comprises three components that is an antenna coil (coupling element), a transceiver (reader) and a transponder microchip with unique ID number. The antenna uses radio frequency waves to transmit a signal that activates the transponder. When activated, the tag transmits data back to the antenna. Using the RF the RFID tag can be read, the RFID reader can read from a distance, it can read through your wallet, clothes, purse or backpack **[4].**

In a typical RFID system any asset or human are tagged with a transponder chip generally containing a unique ID. This data stored in the tag memory is sent to the reader through RF waves. This data along with reader location both are send to the system or database through RFID application.

RFID technology when integrated in a system then we have a transponder (i.e., "tag"), a tag reader, and a database or software application. Data transmission occurs between 10 m (for passive tags—most common) and 1,000 m (for active tags) [**1].** Active tags can be read only or rewritable and typically contain 96 bits of storage. While passive RFID tags are read only **[5].**

RFID tags can be as small as rice grain therefore can be incorporated in a variety of physical form factors. RFID tag data can be read by variety of RFID reader from which are now available in various computer hardware technology (e.g. RFID fixed point reader, handheld reader, mobile computer, smart phones.

Significant privacy and security concerns pervade and arguably limit the RFID adoption due to lack of standardization. International Organization for standardization (ISO) standard 15693 is followed for conducting data transmission. This standard provides limited protection and has no universal validation, authentication or encryption protocols for securing RFID data transmission between readers and tags. **[1], [6].**

RFID system has numerous advantages including their price, size, memory capacity and their capability. The pure memory-based RFID chip without a co-processor is cheap. Some other desirable attributes of RFID technology are it does not require line of- sight for transmitting data like it required in barcode technology. In addition, data is usually read automatically through non-conducting material. Finally, multiple data points can be captured simultaneously. There are two broad categories of RFID systems – passive and active systems.

RFID has the potential to enable machines to identify objects, understand their status, and communicate and take action if necessary, to create “real time awareness”. Identification technologies like RFID allows each object to have a unique identifier that can be read at a distance allowing automatic, real time identification and tracking of individual objects. Identification technologies such as RFID, wireless sensor technologies allow objects to provide information about their environment and context, smart technologies allow everyday objects to “think and interact” nanotechnology and energy-saving technologies are packing more processing power into less space.

3 RFID ADOPTION IN SMART CAMPUS

One of the vanguard of technical development is radio frequency identification technology been used for its numerous benefits and reduce manual effort, cost and time. This part discusses about how it can be useful in a scholastic environments for students, teachers, management and parents/guardians. RFID in combination with other auto ID technologies including Mobile apps and biometric can become more secure and private. RFID technology in educative environments enhances academic management boosting academic service and control of entities; reduce human mistakes and criminal activities like forgery and theft **[7].**

RFID tags when carried by each entity including every individual as well as valuable asset with in a smart campus and RFID readers been installed all over the campus areas including classrooms, laboratories, exam halls, cafeteria, library, car parking, play area, numerous benefits can be developed and applied.

3.1 RFID application in scholastic environment for student, faculty and administration

RFID technology implemented can be used for individual attendance and tracking as well as limit unwanted access to campus resources. Each entities track of e-payments at cafeteria, stationery or library borrowing, transport services, car parking, computer sign in, administration office visit can be tracked and administered according to the management requirements **[2].**

This also can benefits guardians getting instant message about their student status at campus entering, leaving, or personal check on class attendance. While teachers and management can locate students present at campus and not attending class. Portable RFID readers can be used to take exam hall attendance without disrupting the exams. Students can track their classroom, exam halls, exam hall seats, teacher’s position and many more.

Easy managing of visitor visits to campus can be obtained and also restrict them in limited areas as well as monitor their activities. No more need to key in or pass on student ID number at administration offices as RFID card swipes will initiate and load student details on screen. Management can track faculty academic performance by monitoring class timings, number of lectures per subject, class duration or out of class assignments.

3.2 Asset Management

RFID technology is also beneficial for asset management as tracking assets moving around the campus. Individual student, staff or campus RFID tagged valuables (e.g., equipment, iPads, mobile phones, laptops even exam papers/answer sheets etc.) can be tracked and saved from unauthorized use and misplacements **[3].** Many gulf countries are now using RFID tags for authentic certificate security from forgery.

All this and many additional benefits can be taken from RFID technology implementation but these new applications carry with them substantial new privacy and security risks for individuals. Few risk or security issues associated with RFID are targeting or tracking of individuals, potential disclosure of personal practices or preferences to unauthorized third parties, attacks on various parts of RFID system. Cipher bullying is one to the RFID security threat in educational environments **[7].**

3.3 Problems of RFID

Where scholastic environments have numerous benefits in adopting RFID systems same place RFID adoption is limited due to unsecured and non-private nature of system. Former implementers of latest technology are usually academic institutions, which are still not able to take advantage of RFID system complete applications due to dangers to security and privacy RFID poses. Still RFID industry is working hard to secure technology and promise innovative and secured future of academic institutions.

Various RFID applications in academics need different level of security based on their usage however a practical challenge particularly for academic industry is multiple cards swap by a user. This leads to potential problems of vicarious and erroneous attendance record specifically of absent students. Where carefully designed RFID applications can be very use full for attendance check in congestion and controlling attendee's arrival and departure at intermissions. Student regular attendance helps them gain learning capabilities, increase listening attitudes and memory capacity **[7, 8].**

Profound scholastic environment requirement based security analysis of RFID devices is required to employ RFID system with security protocols which are cost effective and provide maximum efficiency. The authentication algorithm suggested by Ahmed Saeed Alzahrani **[7]** is RFID tags should be attached to student's personal smartphones but there is a possibility that students may carry multiple mobile phones and pass on RFID tagged mobile phone for their class attendance.

With its numerous benefits RFID system also poses several security and privacy concerns affecting is adoption for instance RFID tag can remotely interrogate information regarding tagged individual or tagged private property revealing initially revealing its location. Another issue is possibility of falsify including cloning or impersonating RFID tagged device identification **[9].** A security breach is possibility of replicating the identifier while privacy weakness is disclosure of individual information.

Various potential RFID security and privacy attack methods are as follows

1) ***Eavesdropping***

Monitor tag/reader communication

2) ***Man-in-the-middle and radio relay***

Radio relay attack common risk to all contactless systems

3) ***Denial of Service***

Disabling a tag or reader

4) ***Counterfeit Tag***

Generate (valid) responses from a cloned tag

5) ***Malicious Reader***

Pretend to be a legitimate reader and communicate with legitimate tags.

6) ***Reverse Engineering***

The reader is assumed to contain a tamper resistant trusted computing module which is beyond practical attack (contains battery, sensors and wipes stored information making it useless on detecting a physical attack). It is assumed that the costs of reverse engineering a tag will be beyond the economic advantage gained from doing so.

7) ***Side Channel Analysis***

Monitor EM fluctuations from the tag or inject faults in order recover key information.

8) ***Reader Networks***

Vulnerable links between readers and databases also known as middleware.

Security and privacy issues of RFID tags effects organizations and individuals. Security applied at middle layer between reader and Database prevents unintentional disclosure of sensitive information. Unprotected tags may be vulnerable to eavesdropping, traffic analysis, spoofing or denial of service and many more. While secured tag can be tracked and effected traffic analysis attack revealing location privacy **[8].** Even latest RFID technology proposed security systems can be threatened through the denial of service attack DoS and radio relay attacks **[10, 11], [4].**

3.4 Solutions of RFID

RFID authentication protocols proposed are generally based on lightweight cryptographic operators and functions due to limited capability of tag including memory size, power and computation capacity. In last decade different authentication protocols have been proposed **[1], [12, 13]** to provide security and privacy but in-depth analysis has shown their weakness in traceability attacks. Backward traceability and forward traceability are usual attacks which allow the attacker to trace a tag, which in any case is not acceptable by RFID users to be tracked by malicious system or user. Numbers of proposed protocols are proposed for RFID systems which provide required identifier information security fit into categories.

1) ***Tag Killing & Sleeping Approach***

Kill (disable) the RFID tag at point of sale to protect consumer privacy.

2) ***Blocking or Soft Blocking***

Selective blocking by blocker tags for privacy protection then no one can scan the tag.

3) ***Relabeling Approach***

Rewrite RFID tags with a new random number on each checkout. Two ways are mask the permanent ID under private id or split permanent ID into two parts one part assigned to object and second will change.

4) ***Re-Encryption***

The basic idea in this approach is to employ re-encryption to cause cipher texts to change in appearance while original code remains same. One master key should be shared by all the tags and readers in a system.

5) ***"Minimalist" Cryptography***

In this approach the tag can not only relabel by the reader even it can relabel themselves.

6) ***The Proxy Approach***

Carry their own privacy-enforcing devices for RFID system e.g. The RFID Guardian which offers centralized RFID security and privacy.

After in depth security and privacy analysis protocols modeled should be able to be responsible for secure and private transfer of data and avoid tag anonymity, tag location privacy, reader privacy, forward secrecy, and mutual authentication, replay attack, desynchronization attacks. Majority protocols proposed for RFID systems despite their intended generality are not scalable for Internet of Things IoT or cloud applications **[6], [12], [14]** Applying these protocols on multiple readers severely complicates the job for instance an RFID card been accessed at multiple buildings, printer systems, vending machines, classrooms etc. Some security models proposed are based on unrealistic assumptions; others are impractical to apply **[15].** A real world challenge drawing significant attention for RFID community is to design authentication protocols preserving privacy for massively deployed RFID systems where main bottleneck is to search enormous amount of tag entries appearing in backend database **[14], [16].**

RFID middleware which is between RFID reader and database application collects, filters, aggregates, grouping and formatting RFID data should be secured from eavesdropping or parameter manipulation attacks of malicious users thus raising privacy concerns **[1].** Ouafi and Phan have proposed a RFID privacy model. Various proposed protocols analyzed and compared based on this model show security and privacy breaches as they cannot are not protected from various traceability attacks such as traceability, backward traceability and forward traceability attacks. Improved version of Cho et al.'s protocol proposed by Dehkordi and Farzaneh as well as Khedr's proposed novel hash-based RFID mutual authentication protocol and Habibi et al improved version of security protocol all are proved to be none resistance against backward traceability and forward traceability attacks. Improved versions of their protocol are modeled in this paper **[13].**
Another comparison performed on Yoon and Jung et al protocols show security weakness from traceability attacks and DoS attacks respectively and advance version of protocols is proposed claiming to remove all privacy weakness and have secured RFID communications **[15].**

4 IMPLEMENTATION GUIDELINES FOR RFID

Privacy, reliability, obtainability and accessibility are main security goals for an RFID system deployment in scholastic environments. While various malicious attacks including counterfeit RFID tag, replay, eavesdropping electronic collisions are a threat to RFID system particularly in educative environments. More over a feature of RFID where multiple cards can be detected and registered with system in few seconds has become a problem in adoption of system particularly for class rooms where mischievous students can take advantage **[13], [15, 16].**

Until some set standards of Security protocols of RFID are presented and adopted some RFID system application design and implementation guidelines can be followed to avoid RFID problems occurring especially in case of Campus RFID system. Some technological strategies can be implemented to avoid RFID related privacy and security problems.

4.1 Combining RFID with Biometric

Biometric implementation at main entry exit points along with RFID tag detection will confirm student attendance at the campus. This increases the probability of student's class attendance. Secondly no RFID tag will be active in classrooms if students biometric are not verified on the gate **[2].**

4.2 Tagging Mobile Phones

Tagging student smart phones which is the personal device and holds up individual's personal data and contacts will reduce the chance of personal mobile exchange within students for class attendance **[7].**

4.3 Using RFID Passive Tags

Using low-frequency passive RFID-tags reduces the chances of unauthorized reading of tags from long distance readers as they use inductive coupling which requires the RFID tag to be within a certain range of the RFID reader. Furthermore as passive tags have limited memory therefore will contain only serial number and no individual personal details. While in secured system database each tag serial number will be associated to student identification and other student details. This increases student's privacy from unauthorized readers **[17].**

4.4 Monitoring and Controlling Reading

RFID reader's reading of tags can be monitored internally by system by counting detected tags per minute and controlled by pausing the reading if more than one card is detected by the reader within a second and informing the authorities **[9].**

4.5 RFID Reader and Writer

Also known as Tag pseudonyms. In this process each student tag serial number can be rewritten with certain encryptions dynamically on daily basis to reduce the risk of individual location tracking and preserve confidentiality or valuable information by unauthorized readers. This technology works with reader when a tag is detected same time the writer changes the tag number fully or partially and updated the records of the students in the database **[5, 6].**

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. Applying simple technological approaches to increase security includes the process to encrypt tag serial number when passing the data from the reader to the middleware, when encrypted tag serial number will reach the database application it will be decrypted in to original serial number and associated to the person identification.

5 CONCLUSIONS

The paper explains the benefits of RFID system particularly for scholastic environments. After sharing RFID technology in scholastic environments background details and technical approach to various problems, RFID applications and implementation for smart campuses are discussed. As RFID technology is used for increasing security in various systems but by nature it is not a much secured technology and has many security and privacy problems which are discussed and various recently proposed RFID privacy and security protocols and solutions is conversed in detail as well as their drawbacks is also discussed. At the end various simple application development technological strategies are given which can help in reducing security and privacy attacks until a uniform standard protocol is developed and proposed without shortcomings of scalability and complexity. Given strategies may increases the complexity but will help securing the system and thus helps is RFID adoption for scholastic environments in current era.

REFERENCES

[1]. Benjamin P. Rosenbaum, "Radio Frequency Identification (RFID) in Health Care: Privacy and Security Concerns Limiting Adoption," Journal of Medical Systems, vol. 38, issue 3, pp.19. 2014.

[2]. Mirza, Zainab Rasheed Fahad and M.N. Brohi, "Integrating radio frequency identification technology in academic management system," J. Comput. Sci., vol. 10, issue 2, pp. 361-365, 2014.

[3]. Mirza, Zainab Rasheed Fahad and M.N. Brohi, "An in-depth analysis on integrating campus radio frequency identification system on clouds for enhancing security," J. Comput. Sci., vol. 9, issue 12, pp. 1710-1714, 2013.

[4]. R.K. Pateriya, Sangeeta Sharma, "The Evolution of RFID Security and Privacy", A Research Survey.Communication Systems and Network Technologies (CSNT) International Conference on 3-5, June 2011, p.115 – 119.

[5]. Steven Tucker, Peter Darcy, Bela Stantic, "A Comparative Study of RFID Technology Measuring Efficiency and Acceptance when Capturing Attendance", Proceedings of the Thirty-Seventh Australasian Computer Science Conference (ACSC 2014), Auckland, New Zealand.

[6]. Jens Hermans, Roel Peeters, and Bart Preneel, "Proper RFID Privacy: Model and Protocols," IEEE TRANSACTIONS ON MOBILE COMPUTING, vol.13, issue 12, pp. 2888-2902,2014.

[7]. Ahmed Saeed Alzahrani**, "**Security analysis of RFID based devices in educative environments**,"** Life Science Journal, Vol. 11, issue 1, pp.133-140, 2014.

[8]. Rand A. Mahmood, Wasim A Al-Hamdani, "Is RFID Technology Secure and Private**?,"** Proceedings of the 2011

Information Security Curriculum Development Conference, InfoSecCD 2011, Kennesaw, GA, USA, September 30 - October1, 2011, p. 42-49, 2011.

[9]. Jin Kim1 and Seung-Kook Cheong2, “Research on an Authentication Algorithm for an Electronic Attendance System in the Constructing of a Smart Campus,” International Journal of Security and Its Applications, vol. 7, issue 6, pp.199-208, 2013.

[10]. Wiem Tounsi, Fr´ed´eric Cuppens, “Access and privacy control enforcement in RFID middleware systems: Proposal and implementation on the fosstrak platform,” World Wide Web, vol. 19, issue 1, pp.: 41-68, 2015.

[11]. Tim Good · Mohammed Benaissa, “A holistic approach examining RFID design for security and privacy,” J Supercomput 64, pp. 664–684, 2013.

[12]. Mete Akgun, M. Ufuk Cagˇlayan, “Providing destructive privacy and scalability in RFID systems using PUFs,” Journal of Ad Hoc Networks, Vol. 32, pp. 32-42, 2015.

[13]. Seyed Mohammad Alavi , Karim Baghery1, Behzad Abdolmaleki, Mohammad Reza Aref, “Traceability Analysis of Recent RFID Authentication Protocols,” A Family of Transaction on Wireless Communications, vol. 14, issue 1, pp. 570-584, 2015.

[14]. Imran Erguler · Emin Anarim · Gokay Saldamli, “Unbalanced states violates RFID privacy,” Springer Science+Business Media, J Intell Manuf, pp.25:273–281, 2014.

[15]. Karim Baghery, Behzad Abdolmaleki, Bahareh Akhbari, Mohammad Reza Aref, “Privacy Analysis and Improvements of Two Recent RFID Authentication Protocols,” 11th International ISC Conference on Information Security and Cryptology. IEEE, 978-1-4799-5383-7/14, 2014.

[16]. Ben Niu · Xiaoyan Zhu · Haotian Chi · Hui Li, “Privacy and Authentication Protocol for Mobile RFID Systems,” Springer Science+Business Media New York, Wireless Personal Communications, vol. 77, issue 3, pp. 1713-1731, 2014.

[17]. Divyan M. Konidala, Daeyoung Kim, Chan Yeob Yeun and Byoungcheon Lee., “Security Framework for RFID-based Applications in Smart Home Environment,” Journal of Information Processing Systems, vol. 7, issue 1, pp. 111-120, 2011.