Character Proximity For RFID Smart Certificate System: A Revolutionary Security Measure To Curb Forgery Menace.

Eze Chika Victor, Adeniji Oluwashola David

Abstract: Generating certificates for the graduating students is an area of administration that requires significant amounts of time and effort in a university environment, largely due to the number of students that graduate each year from both the full-time and the part-time studies. Students are expected to complete their clearance manually before receiving graduation certificates; this turns out to be very strenuous as much time and effort are wasted in accomplishing such. However, the certificate itself is the problem. It is of very low standard and quality, little or no integrity, very easy to forge, and not befitting for an institution such as the University of Ibadan. There is need to make use of vast growing radio Frequency Identification (RFID) technology to automate the graduation certificate system, which would not only standardize the format of the data collected by the university, but would also protect and secure the integrity of the university's graduation certificates, reduces administrative work, and improve graduate's creditability ratios. The objective of the research is to provide an efficient software that can protect the integrity of graduating certificate by embedding an encoded RFID tag using character proximity on each certificate before it is being issued in order to reduce, if not eradicate, the problem of forgery and fraudulent activities on certificates.

Keywords: Radio Frequency Identification, System Architecture, Character proximity, Certificates Implementation and solution statement.

1. Introduction

The 21th century has experience a lot of fraudulent activities and misconduct most especially in the practices of certificate forgery. The resultant effect of these habits in most cases normally reduces the integrity of institution concern. Certificate menace is serious activities which can be curb if not eradicated in order to safe guide the goodwill of the institutions or people concern. If you're looking for online experience degrees you should ensure that the institute has proper accreditation. Fake degrees can destroy; ruin your academic and professional career. It is important to check with the accrediting agencies or organization to know the registered institute you are about to acquire a degree because students at time end up with fake college degree. This paper is organized as follows: section 2 describes Radio Frequency Identification. Section 3: System Architecture, Section 4 Certificate implementation Section 5: Character Proximity and solution Statement.

2. Literature Review

Radio-frequency identification (RFID) is the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking. The most important criterion of different RFID systems is how the energy supplies of the transponder works which are classified into passive and active transponders.

- *Eze Chika Victor, Adeniji Oluwashola David*
- *Department of Computer Science, University of Ibadan Ibadan, Oyo State 23402, Nigeria chivitech@yahoo.com*
- *Department of Computer Science, University of Ibadan Ibadan, Oyo State 23402, Nigeria shola.adeniji@ui.edu.ng*

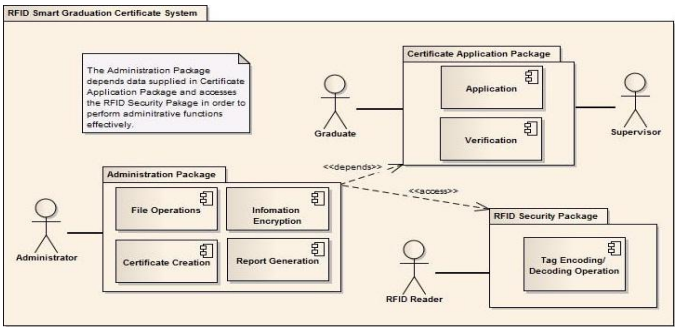
Passive transponders do not have any power supply while the Active transponders have their own energy supply, e.g. in form of a battery or a solar cell. Here the power supply is used to provide voltage to the chip. The magnetic or electromagnetic field received by the reader is therefore no longer necessary for the power supply of the chip (Kleist et al., 2004) and (Rikcha, 2004). RFID systems rely on external communication channels link in which data is registered by the reader to other data pools. Security issues regarding the back-end of the RFID system are not specific but the RFID systems rely on that external communication channels link registered by the reader to other data pools. There are different complex procedures for storing information on transponders. The cloning of transponders can be efficiently prevented by using authentication and encrypted data transmission according to (Westhues, 2005). The interception of the communication between reader and transponder is therefore one of the most prominent threats to RFID technology. The ranges given for RFID systems vary between a few centimetres (e.g. ISO/IEC 14443, 13.56 MHz) and several metres (ISO/IEC 18000-6, 868 MHz) and apply to the active communication which even requires the transponder to be supplied with power and to generate several volts at the antenna. For the identification of vehicles, the required range of the RFID system is designed such that, at the maximum vehicle speed, the length of time spent in the interrogation zone is sufficient for the transmission of the required data as reported in (Bachthaler, 1997).

3. Materials and Methods

The proposed system is made up of system architecture that includes: design structure, behavior of a computer system, microprocessor, system program and the characteristics of individual components and how they interact. In order to show the design, structure, physical elements, behaviour and individual components of the proposed system, three unique unified modeling tools were used. These are Package diagram, Component diagram and Deployment diagram. The package diagram provides a way to group related elements and to scope their names; it also provides a way of visualizing dependencies between parts of the system. The

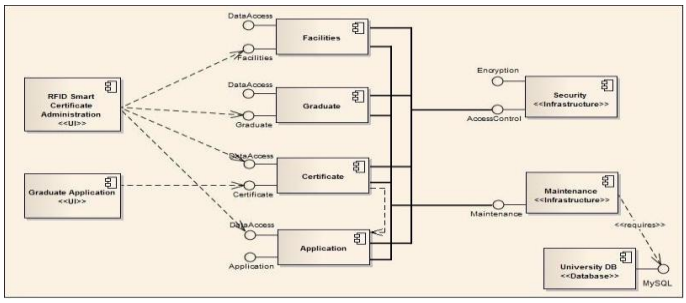
package diagram for the proposed system below in figure 1 shows a three-layered architecture, consisting of a Certificate Application package, an Administrative package, and an RFID Security package. The packages represent different generic subsystems of the proposed system. The dashed arrows represent the dependencies among the packages. The packages participate in a client-supplier relationship

Figure 1. Package Diagram



A component is an encapsulated, reusable, and replaceable part of your software; it is a physical piece of a system, such as a compiled object file, piece of source code, shared library or Enterprise Java Bean (EJB). Component diagrams model the physical software components and the relationships between them, show the structure of the code itself, model source code and relationships between files, model the structure of software releases and specify files that are compiled into an executable.

Fig 2. Component Diagram



In the component diagram for the proposed system, several software components have been identified. For example, RFID Smart Certificate Administration, Graduate Application, Facilities, Graduate, Certificate, Application. A deployment diagram shows the structure of the run-time system, capture the hardware that will be used to implement the system and the links between different items of hardware. It models the physical hardware elements and the communication paths between them. Ultimately, a deployment diagram shows the system's hardware, the software installed on that hardware, and the middleware that connects the disparate machines together.

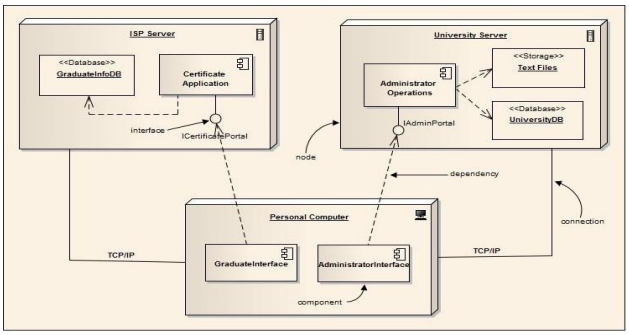
A microchip Student Graduation Certificate: The tag was use to established electromagnetic field to communicate with the Reader. The tags was programmed with the encrypted version of each graduate's certificate details before it is being appended onto the certificates to be issued. The information on this certificate is secured and protected from forgery and whenever the certificate is within the reader reading coverage area, the tag is detected and the encrypted file is read.

4. Certificate Implementation

The deployment diagram of the implementation for the proposed system shows the topology of nodes in client/server architecture, the deployment of the Certificate Application component to an Internet Service Provider (ISP) server, the deployment of the Administrator Operator component to a high-end University server and the Graphical User Interface (GUI) components to client/administrator workstations. During the implementation the following were considered and deduced.

a. The nodes in the deployment diagram below are connected using a TCP/IP Local Area Network (LAN) cable. From the GraduateInterface component, a graduate can access the Certificate Application component on his/her personal computer using the ICertificatePortal interface. The Certificate Application component requires the GraduateInfoDB database to store and retrieve data used during the certificate application process. This database is maintained in the ISP server.
b. Alternatively, from the AdministratorInterface component, an administrator can access the Administrator Operator component on his/her personal computer using the IAdminPortal interface in figure 3.

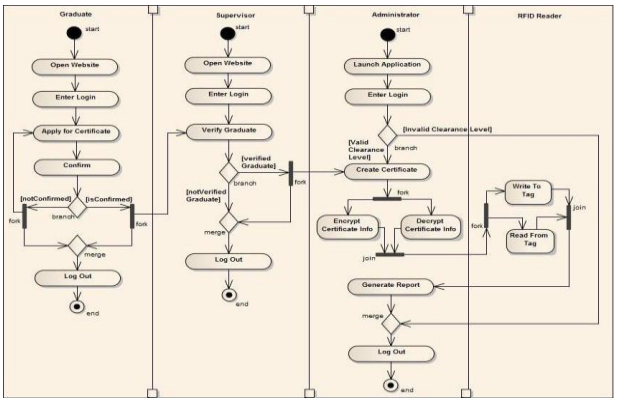
Fig 3: Deployment Diagram



The Graduate-user part is a module in the implementation which is made up of a web-based application that can be deployed on a network for easy access to graduates given the correct username and password. Forms are used to accept data from the graduates. Forms to be filled by the graduate include Bio-data Information Form and Clearance Information Form. The Supervisor-user part of the proposed system is also a web-based application that can also be deployed on a network to grant easy access to all clearance supervisors given the correct username and password. Supervisors are not expected to fill any form; they are only to indicate if a graduate has been cleared from his/her own jurisdiction. The Administrator's part of the proposed system is solely a Java GUI application which will serve as a back-end for monitoring the entire system – adding new, updating existing, deleting old, and viewing graduates' and supervisors' details – as well as creating certificates for cleared graduates, encrypting and decrypting the certificate information. The Administrator's part is a C-sharp application

for encoding and decoding encrypted data on RFID tags using the RFID reader (reason being that the RFID being used for this project supports C-sharp NOT Java). The major output of the proposed system is the RFID Smart Graduation Certificate. The proposed system also maintains a log of all operations performed and by whom. However, Reports concerning all activities which took place in generating such certificates has to be noted and presented to the University Management in form of reports to aid decision-making. Activity Diagrams of the implementation describe events needed to achieve some operation, particularly where the operation is intended to achieve a number of different things that require coordination. They also describe how the events in a single use case relate to one another; in particular, use cases where activities may overlap and require coordination, i.e. how a collection of use cases coordinate to create a workflow for an organization as shown in figure 4.

Fig 4: Activity Diagram



5. Character Proximity and Solution Statement

The design and development of character proximity scheme in the database of type B radio frequency identification tag was used to identify the originality layout in the database. During implementation, two or more separately matching term occurrences were within a specified distance, where distance is the number of intermediate words or characters. In the proposed system, every statement is executed given the right condition and test data. For example, a program statement that creates certificate would not be executed if an administrator does not attempt to create a certificate for a graduate. During statement testing, program statements under the following headings were tested and are executed every time given the right condition and test data: Add new administrator, Graduate, or Supervisor record, Update existing administrator, graduate, or supervisor record, Delete administrator, Graduate, or Supervisor record, View administrator, Graduate, or Supervisor record, Certificate Application and Graduate Verification, Certificate Creation, Encryption and Decryption, RFID tag writing and reading, Report Generation. The Taxonomy of people within the said university includes: male or female that form the gender, the type of degree which can be undergraduate or postgraduate who are student. Employer can be administrator and supervisor, the supervisor can be associate supervisor or tenured supervisor. Nationalism are mainly the citizen or foreigner. To give the important conceptual/domain modeling an indicator was introduced as shown in table 1 below.

Table 1: Multiplicity Indicator

Indicator	Meaning
0..1	Zero or one
1	One only
0..*	Zero or more
1..*	One or more
n	Only n (where n > 1)
0..n	Zero to n (where n > 1)
1..n	One to n (where n > 1)

Indicator **0..1** which can be zero or one is the information about the graduate which may include possible messages the class is able to understand, definitions of constraints, tagged values are shown in table 1. Importantly **1..*** must be composed, accessed, secured and reviewed because the original data must be encrypted. The certificate template must be created for encryption and decryption to be secured and accessed by the RFID reader, which are reviewed and verified. However other indicator and their meaning served the purposes of modeling the software and hardware. Each process may consist of several sub-processes. Each sub-process may also be broken down into smaller units. Decomposition continues until no sub-process can logically be broken down any further. The clearance levels was intended to restrict the amount of access each administrator has on the system's data. This will help reduce the risk of external influence or forgery. The table 2 below shows the clearance levels of the developed system.

Table 2: Administrative Designation and Level

Designation	Clearance Level
Overseer	5
Security	4
Creation	3
Maintenance	2
Observer	1

- **Level 1**: Administrator can only view (cannot add, edit or delete) any graduates and supervisors record; cannot view other administrators, certificate and security information.
- **Level 2**: In addition to viewing, administrator can add, edit or delete any graduates and supervisors record. He/she can as well generate systems report on graduates and supervisors (still no access to other administrators, certificate and security information).
- **Level 3:** Coupled with the privileges of Level 2, the administrator now has access to certificate information. He/she can create new certificates, view certificate images and generate systems report on certificates. No access to administrators and security details. It will be recorded that the clearance level that support the RFID Smart Graduation Certificate System is highly secured. The interoperability among the levels is extremely important. However it will be too difficult for forgers to break the system.

- **Level 4:** Coupled with the privileges of Level 3, the administrator now has access to security information. He/she can encrypt or decrypt certificate information as well generate systems report on the RFID tags. Still no access to administrators' details.
- **Level 5:** Administrator has full access to all parts of the application. He/she enjoys the privileges of Level 4 and has complete access to other administrators' details; he can add new, update existing or delete old administrator's record. He/she can also generate systems report on administrators.

Figure 5. Administrative Designation and Level

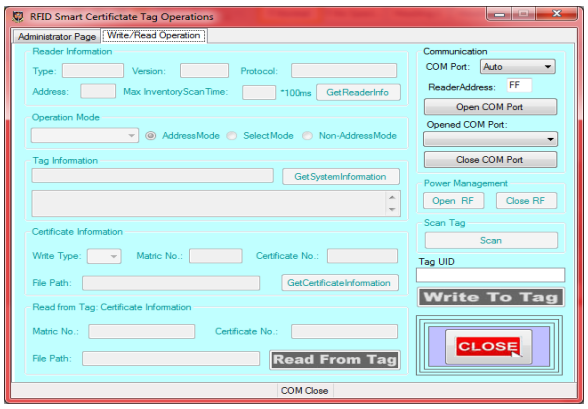


Figure 6. RFID Tag Write/Read Operations

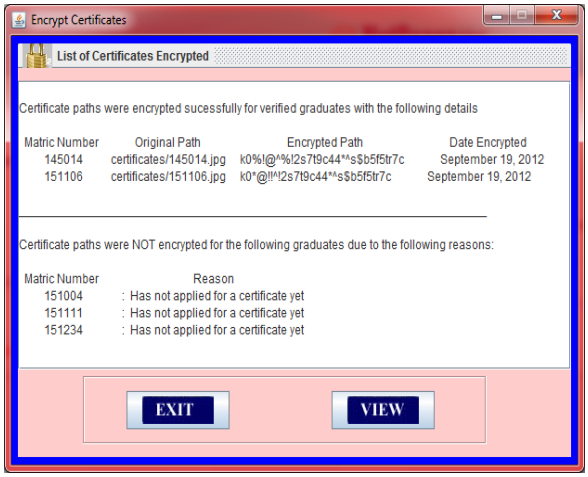


Figure 7. Preview of Certificate Info Encryption

The report menu of the administrative homepage contains report generation operations that can be performed by administrators. An administrator, depending on his clearance level, can generate systems report on administrators, graduates, supervisors, certificates and RFID tags. These reports enable the management to make decisions as regards the overall function of the system

6. Result and Discussion

Six important tests were carried out in the course of implementation and deployment. They include Statement Testing, Branch Testing, Expression Testing, Path Testing, Black-Box Test, and White-Box Test. During Statement Test, every statement is executed given the right condition and test data. For the Branch Test a probes was inserted at various branch points in the program to ensure that every branch gets executed under the right condition such as Certificate Application, Graduate Verification and Administrative Operations. The Expression Test required that every expression assumes a variety of valued in such a way that no expression can be replaced by a simpler expression and still pass the test. In the Path Testing, data was selected to ensure that all paths of the program have been executed. It is important to draw a conclusion that about 75% path was covered during unit and integration testing. The black box test involves viewing the test object from the outside whose contents are unknown. It feeds input to the black box and notes what the output is. The test's goal is to be sure that every kind of input is submitted, and that the output observed matches the output expected. The major kind of input to be submitted to the system is the graduate's matriculation number and clearance date. The tables below show the black box test experiment on both the matriculation number and clearance date

Test case ID	Description	Test Data 1	Test Data 2	Expected Result	Actual Result
1	Less than 6 digits	15110	1511	Reject	Reject
2	Exactly 6 digits	151106	145014	Accept	Accept
3	More than 6 digits	1511065	15110655	Reject	Reject
4	Include character(s)	15110F	G15U10	Reject	Reject
5	Include negation	-151106	151106-	Reject	Reject
6	Include special xter	151/10	15&110	Reject	Reject
7	Blank character(s)			Reject	Reject

Table 3: Black box test experiment for Graduate Matriculation Number

Test case ID	Description	Test Data 1	Test Data 2	Expected Result	Actual Result
1	day/month/year	11/Nov/2012	21/Feb/2012	Accept	Accept
2	day month, year	11 Nov, 2012	21 Feb, 2012	Accept	Accept
3	day, year month	11, 2012 Nov	21, 2012 Feb	Reject	Reject
4	month day, year	Nov 11, 2012	Feb 21, 2012	Accept	Accept
5	month year, day	Nov 2012, 11	Feb 2012, 21	Reject	Reject
6	year, month day	2012, Nov 11	2012, Feb 21	Accept	Reject
7	Year, day month	2012, 11 Nov	2012, 21 Feb	Reject	Reject
8*	day greater than 31	32/11/2012	32/02/2012	Reject	Reject
9*	month greater than 12	11/13/2012	21/13/2012	Reject	Reject
10*	year less than 2012	11/11/2010	21/02/2010	Reject	Reject
11*	negative or zero day	-11/11/2012	0/02/2012	Reject	Reject
12*	negative or zero month	11/-11/2012	21/0/2012	Reject	Reject
13*	negative or zero year	11/11/-2012	21/02/0	Reject	Reject

*Date format used is day/month/year

Table 4: Black box test experiment for Graduate Matriculation Number

The white box test involves examining the code's internal logic, using a careful testing strategy. For example, we can devise test cases that execute all the statements or all the control paths with the component(s) to be sure the test object is working properly. However, it is important to note that it is impractical to completely adopt the white box test experiment. The tables below shows the white box experiment performed on the graduate certificate application and verification, as well as the administrative operations.

Test case ID	Description	Test Data 1	Test Data 2	Expected Result	Actual Result
1	Login	Not Matric No.	Not Staff ID	Invalid login details, returns to login page	Invalid login details, returns to login page
2	Login	Matric No.	Application completed	Opens graduate homepage	Opens graduate homepage
3	Login	Matric No.	Application incomplete	Opens graduate application form	Opens graduate application form
4	Login	Staff ID	-	Opens supervisor verification page	Opens supervisor verification page
5	Confirm Application	Application information	-	Confirmation error, returns control	Confirmation error, returns control
6	Confirm Application	Application information	Clearance information	Confirmation success, stores information	Confirmation success, stores information
7	Graduate Verification	Graduate Matric No.	Clearance incomplete	Verification error, returns control	Verification error, returns control
8	Graduate Verification	Graduate Matric No.	Clearance completed	Verification success, stores details	Verification success, stores details

Note: Test Data 1 and Test Data 2 must be satisfied to produce the expected result.

Table 5: White box test for Certificate Application and Verification

Test ID	Description	Test Data 1	Test Data 2	Expected Result	Actual Result
1	Login	Not Admin ID	-	Invalid login details, returns to login page	Invalid login details, returns to login page
2	Login	Admin ID	Clearance Level 1	Opens application, grants Observer privilege	Opens application, grants Observer privilege
3	Login	Admin ID	Clearance Level 2	Opens application, grants Maintenance privilege	Opens application, grants Maintenance privilege
4	Login	Admin ID	Clearance Level 3	Opens application, grants Creation privilege	Opens application, grants Creation privilege
5	Login	Admin ID	Clearance Level 4	Opens application, grants Security privilege	Opens application, grants Security privilege
6	Login	Admin ID	Clearance Level 5	Opens application, grants Overseer privilege	Opens application, grants Overseer privilege
7	Certificate Creation	Clearance Level 3+	Verified Graduate Details	Creates certificate for verified Graduate	Creates certificate for verified Graduate
8	Information Encryption	Clearance Level 4+	Certificate Information	Encrypts certificate Information	Encrypts certificate Information
9	Write to (Read from) RFID Tag	Clearance Level 4+	Encrypted Certificate Data	Writes encrypted data to RFID tag	Writes encrypted data to RFID tag
10	Report Generation	Clearance Level 5+	Any operation	Generates report for selected operation	Generates report for selected operation

Note: Test Data 1 and Test Data 2 must be satisfied to produce the expected result.

Table 6: White box test experiment for Administrative Operations

7. Conclusions

In order to curb the problem of certificate forgery this research attempted to build a software tool that would protect the integrity of graduating certificate by embedding an encoded RFID tag to each certificate before it is being issued. This project delivers an efficient RFID based Smart Certificate for Graduating Students to reduce, if not eradicate, the problem of forgery and fraudulent activities on certificates. The smart certificates will include all vital university certificate information, encoded and stored onto an RFID label attached to the certificate. This information can then be read and instantly verified by any authorized government body / representatives. It is of immense benefits to universities as it protects and secures the integrity of their graduation certificate, reduces administrative work, and improves graduate's creditability ratios.

Acknowledgments

The authors wish to thank the Department of Computer Science, University of Ibadan for support in this research work

References

[1] Bachthaler, Reiner (1997) Auswahlkriterien für elektronische Datenspeicher, ident, 3. Cited in Klaus Finkenz (2003) 'RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification (Second Edition)". John Wiley & Sons. ISBN: 0470844027.

[2] Ivan Beker (Ed.) (2011) 'Proceedings of the XV International Scientific Conference on Industrial Systems (IS'11)'. University of Novi Sad. Serbia. ISBN-13: 978-86-7892-341-8.

[3] Klaus Finkenz (2003) 'RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification (Second Edition)". John Wiley & Sons. ISBN: 0470844027.

[4] Prachi Jain, Ankit Dasgupta (2012) "An Instauration to Radio Frequency Identification", in: Proceedings of the International Conference on Advances in Communication and Computing Technologies (ICACACT) 2012. International Journal of Computer Applications® (IJCA)

[5] Sagato Technology Co., Ltd (2010) Radio Frequency Identification Basic 2010 [Online]. Sagato Technology Co., Ltd. Retrieved from: http://www.sagato.co.th/rfid_basic.php [Accessed 12 March 2012].

[6] Wagdy Sawahel (2011) UAE: Smart system to prevent degree fraud 2011 [Online]. University World News: The Global Window on Higher Education. Retrieved from: http://www.universityworldnews.com/article.php?story=20110723170439132 [Accessed 12 March 2012].

[7] Wikipedia (2012) Radio-frequency identification 2012 [Online]. Wikipedia. Retrieved from: http://en.wikipedia.org/wiki/Radio-frequency_identification [Accessed 12 March 2012]