International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Design and Development of a RFID Attack Simulator Device

Kouame Yann Olivier Akansie, Dr. Venkateshppa

[1]Pursuing Masters Degree Program in Digital Communication and Networking, REVA University, India

[2]Associate Professor, School of Electronics and Communication, REVA University, India

Abstract: ***RFID stands for Radio Frequency Identification. It's the acronym used to define a technology that make use of readers, tags, and backend servers to elaborate a system that has a variety of applications. Before implementing any system of such kind, security issues must be considered carefully since not taking care of security issues could lead to severe consequences; as some applications of this technology offers security services such as electronic passports and RFID-embedded credit cards. Safety is one of the most important issues of any communication systems, especially for wireless communication systems which use sometimes insecure wireless channel to communicate. In RFID systems, transmission of data between tags and readers or even data transmission involving readers and back-end database uses the wireless channel which is insecure. There are some risks inherent in RFID systems, such as counterfeit RFID tag attacks, reply attacks, eavesdropping attacks, etc. Therefore, ensuring the security of RFID systems is particularly important. Our paper will deal with the inherent in RFID systems and the design of a device able to simulate the attacks in order to further propose a system able to counter the simulated attacks.***

Keywords: RFID system, RFID security, RFID Security Issues, Privacy, Authentication, Protocols, Smart Label, Tags

1. Introduction

Recently, as a new automatic identification technology, due to its inherent advantages, Radio Frequency Identification (RFID) has become a research hotspot [1]. When Compared to other automatic identification technologies, RFID technology has lots of advantages such as: the fact that it does not require a direct contact and line-of sight, it can work efficiently under bad conditions, tags can be used many times and big size data can be stored in them, they can also be reprogrammed easily (the tags), and be recognized by the reader at the same time, etc. On one side, just because of its advantages, RFID is used in many fields like industry, aviation, military, intelligent transportation systems, and supply chain, etc [2].

On the other side, with the extensive application of RFID, the issues related to it are increasing, which make people feel very uncomfortable. Among these issues, security problem is a serious one. Some of the security issues are related to forward security, backward security, replay attack, DoS (denial of service) attack, eavesdropping attack, and so on. If security problems are not dealt with proper care, further development and application of RFID are bound to be influenced greatly [3].

Our aim is to understand first the technology, then have a look on security issues and security threats. The next steps would be to simulate the identified attacks by designing a specific device able to do so.

2. Literature Review

The intention behind this literature survey is to review some of the security issues faced by RFID technology and the solutions proposed to overcome the highlighted issues. Our aim is to prove that some issues are not yet addressed despite the fact that solutions are provided and incorporated. Hence, our objective will be to simulate some attacks toward any RFID system and see which attacks can be successfully executed. This will depict the security level and point out where the tested system is failing.

Due to the low cost offered by RFID, the applications of this technology are growing every day. When something gets too much attention, especially in technology, the threats are also increasing. Hence, before using any technology, the security issues will be checked and depending on the application, it can be decided whether the technology is suitable to be used or not. The paper [1] is about many methods available to deal with security issues of RFID technology. The solutions or method available are analyzed and a new method is proposed by the author. The proposed method has been proven to be effective, with a low computational consumption. Some assumptions have been made to for simulation, since only a side of the system is of concern.

The papers [2-3] deal with the application of RFID in Internet of things. Since nowadays, internet of things has been evolving; the implementation of available systems into it is of great interest. Apart from the disadvantages brought by RFID due to its security issues, it is important to highlight the benefits that can be brought by RFID into internet of things. It is to be noticed that both technologies are evolving and RFID issues are being taken care by some researchers. What can be said is that, both technologies can progress in parallel till they reach a mature stage where security issues are no more a problem. In the paper [4], three protocols have been reviewed. The protocols take their roots in cryptography, precisely cryptography based on symmetric key and elliptic curve for encryption and decryption. All protocols in the paper are having limitations which are overcome with the proposed solutions. The first protocol proposed by Li has some limitations, but can be still used in certain applications. The remaining protocols proposed by Susilo and Guo are overcoming the first protocol limitations, but have also some limitations which are overcome by the author. An authentication failure was observed in the elliptic curve protocols. A

solution was suggested to deal with the failure. The proposed solution works by early detection of the flaw, which has an impact on computational and communication power required for the protocols. The paper [5] is about protocols used in RFID technology for many communication stages. The protocols used are not without limits and those protocols have been analyzed in the paper. The outcome of this paper is that security is not fully implemented in RFID based technologies. By discussing about the lack of security, it is intended to enhance research about less expensive, suitable solutions which can be implemented to the existing systems which use RFID.

The paper [6] deals with RFID applications and risks. The objective of the paper is to give an insight about the advantage that RFID offers. Not only that, but also the risks undergone while using any RFID based system. The cost of the technology is quite affordable. Compromising on the cost affects inevitably the security of the technology. A must in such communication system is the privacy, which can be compromised with a lack of security. The paper [7] is a review of research undergone in RFID technology, about security issues and attempts of solutions. The paper first explains the threats of RFID. Then it gives some countermeasures available and discussed in different articles about the same topic. At last, the open issues are brought out to incite people to investigate the topic and contribute to solve them.

3. Background of RFID

3.1 Basics of RFID

RFID is referred to a technology where digital data are encoded in RFID tags or smart label, are captured by a reader using radio waves. RFID has a similarity with barcoding in that data from a tag or label are accessed by a device that keeps the data in a database. RFID has several advantages over barcode systems. A very important thing is that RFID tag doesn't require a line-of-sight connection to work, whereas barcodes must be aligned with an optical scanner.

3.2 Working Principle of RFID

RFID belongs to a group of technologies referred to as Automatic Identification and Data Capture (AIDC). AIDC methods help in identifying objects automatically, collecting data about them, and entering them (data) directly into computer systems with easily, most of the time, without any human intervention. RFID methods make use of radio waves to accomplish this. RFID technology consists basically of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags incorporate an integrated circuit and antennas, which are used for data transmission between the tag and the RFID reader (also called an interrogator). The interrogator then converts the radio waves to a meaningful data. Data collected from the smart label is then transferred through a communications interface to a host computer system, for storage and analysis.

3.3 RFID Tags and Smart Labels

As stated above, an RFID tag contains an integrated circuit and an antenna. The tag is also composed of a protective material that keeps on all the pieces together and shields them from various environmental conditions. The protective material is selected based on the application. As an example, employee ID badges containing RFID tags are made from durable plastic, and the components are embedded in between the layers of plastic. RFID tags are available in a variety of shapes and sizes and can be either passive or active. Passive tags are the mostly used, as they are smaller and less costly. Passive tags must be "powered up" by the RFID reader before they can transmission starts. Unlike passive tags, active RFID tags incorporate power supply (e.g., a battery), which enable them to transmit data at all times. There is also a difference between smart labels and RFID tags in that smart labels incorporate both RFID and barcode technologies. They are generally made of an adhesive label built-in with an RFID tag inlay, and they also carry out a barcode and/or other printed information. Smart labels can be encoded and printed on-demand using desktop label printers, whereas programming RFID tags require more advanced and specific equipment.

3.4 RFID Applications

RFID technology is employed in many industries to perform such tasks as:

- Inventory management
- Asset tracking
- Personnel tracking
- Controlling access to restricted areas
- ID Badging
- Supply chain management
- Counterfeit prevention (e.g. in the pharmaceutical industry)

3.5 RFID Security Issues

RFID based systems are having many security issues.

a) **Jamming:** Jamming deals with a deliberate attempt to disturb the wireless channel between reader and tag and thereby attacking the integrity or the availability of the communication. This could be achieved by powerful transmitters, but also through passive means such as shielding or even a tag. As the channel is air, which is not that robust, even simple passive measures can be very effective. Jamming, which block the communication of an RFID system by generating a noise at the same frequency as that used by the system.

b) **Eavesdropping:** Since an RFID tag is a wireless device that emits data, usually a unique identifier, when interrogated by an RFID reader, there is a risk that the communication between tag and reader can be eavesdropped. Eavesdropping is the operation of intercepting data that has to be read. The attacker can use an adequate reader to listen to the tag. The tag memory is such that most RFID systems use clear text communication, which has the consequence of making eavesdropping even simpler. The information stolen during the attack may lead to serious implications like allowing subsequent attacks against the RFID system. Eavesdropping is one of the most particular threats to RFID systems. The eavesdropped data could be used for malicious intentions. It could also be used to simulate a replay attack.

c) **Replay attack:** When it comes to a replay attack, the attacker steals a person's identity and uses it by repeating the same authentication sequence as the one provided by an authorized person. A replay attack may lead to a clone of the legitimate transponder or by re-sending the eavesdropped data from an equipped device. In order to simulate an attack, an attacker has first to obtain some data which is sent during a normal communication. Then, the data can be further used in order to perform the attack.

d) **Deactivation:** The aim of this type of attack is to render the transponder useless through the unauthorized application or through physical destruction. Depending upon the type of deactivation performed, the reader can either no longer identify the tag, or even detect any surrounding tag.

e) **Spoofing:** Spoofing is defined as duplicating tag data and transmitting it to a reader. Data acquired, no matter the mean, is transmitted to a reader to imitate an authorized source. Let's take the example of an electronic seal; Spoofing is the action of transmitting the e-seal information to the reader from an unauthorized source that is not the original one. If the security protocol used is known, attackers can write the collected information on to a blank RFID tag. A practical case is the following: dishonest persons could replace the RFID tag on an Item by a tag corresponding to a cheaper price.

f) **Man in the middle attack**: man-in-the middle attack is a very famous attack performed on any communication system. Depending upon the configuration of the system, a man-in-the middle (MITM) attack is possible when the data is transiting from one end to another one. An attacker can block the communication path and manipulate the data back and forth between RFID components. This is known as a real time threat. The aim of this attack is to release and modify the information in transit before the receiver gets it. An RFID system is vulnerable due to a lack of sophisticated protection circuitry.

g) **Cloning:** Making a clone consists to first capture the data from a legitimate tag and then make an unauthorized copy of the collected sample on a new chip. It's important to differentiate spoofing and cloning, since they are not the same. Although both attacks copy data from a legitimate tag, spoofing emulates the transmission of tag data while cloning means implies transferring the stolen data onto a new tag in possession of the attacker. Similarly to spoofing, the communication between authorized RFID tags and readers will have to be read and stored but a tag could also be stolen and misused. The data transferred to the cloned tags can be altered to suit to the needs of the desired attack.

4. Proposed Work

4.1 Objectives

Objectives can be identified based on security issues as below:

- Study RFID technology and MIFARE tags (1KB)
- Study security issues from which RFID technology suffers
- Exploit the security issues to find out where the tested system is failing
- Design and develop a device that is able to exploit the security issues found
- Test the device in a real time situation, by simulating attacks toward a target
- Propose some solutions as future scope to solve the issues

4.2 Requirements

As requirements to fulfill our objectives:

- The device should be able to read and write from/to a card. To do so, a RFID reader module can be used.
- The RFID module should be controlled by a controller, which should be small in size.
- For the device to be connected wirelessly to a distant device such as a smartphone or a computer, Bluetooth technology or even WI-FI can be used.
- The device shouldn't depend on a mains power; therefore, batteries should be included
- Some push buttons should be included for control.
- If possible, a small OLED screen can be integrated in order to make the device user-friendly. If not, the device can still be used through a mobile application or through dedicated software, with a computer.

The working will be as follows: when the device is ON, it gets connected to the mobile phone or any nearby router. Then some commands can be sent to the device to simulate the desired attack. The buttons will be used to configure or operate the device manually.

4.3 Block Diagram

The figure below shows the block diagram of the device to be designed. It consists of five main blocks which are:

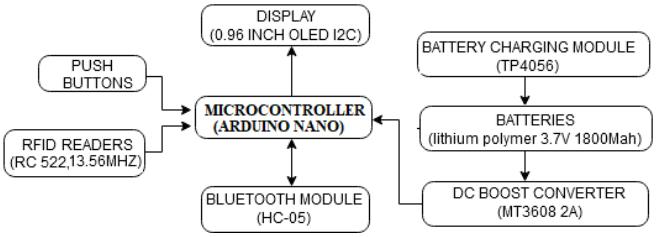

Figure 1: Block diagram

a) Controller: the controller is used to control all the operations performed in the device. Since the device consists of many parts, a link between all the parts should be established. This is done by the help of a microcontroller. As per the requirements, the controller should be small in size, the power range should be within 3 to 5v so that it can be powered up easily using a battery, the power consumption should be less, and the memory size should be adequate. The Arduino Nano microcontroller seems to be suitable as per our requirements.

b) Communication module: depending upon the attacks to be performed, it can be required to establish a link with a distant system such as a computer or a smartphone. In such cases, a communication module is required. Depending upon the communication distance and infrastructure, Bluetooth or Wi-Fi can be used for that. Compatible (with the microcontroller) modules such as the HC-05 Bluetooth module or the ESP8266 Wi-Fi module can be used.

c) Display: any display can be used for the purpose. A display is not highly required since the device can be connected to a distant device. However, for the device to be independent, a display should be incorporated inside the device so as to guide the user. Since the device is supposed to be small in size, a small size display, which can be controlled with fewer pins, is advised. Such requirements can be met by using a small OLED display, which can be controlled with the I2C bus.

d) RFID reader: how target is a MIFARE card which can be accessed with a 13.56 MHz card reader. As per our requirements, a RC 522, 13.56 MHz can be used to read tags. It can be interfaced with the controller using the SPI bus.

e) Power: it's an association of many blocks which help in storing the energy, converting it and supplying it to the controller. Batteries are used to store energy, so that the device can be used anywhere, without any fixed power supply. The batteries should be small in size, with high capacity so that they can last long. The lithium polymer batteries can be used since they are small in size and suitable for our device. The batteries are rated 3.7volts. Since the microcontroller works at a reference voltage of 5v, the voltage level should be stepped up to 5v. This can be achieved by using a DC boost converter. A small size DC boost converter which can be used is the MT3608, 2A module. It offers a high input and output range with less loss. The batteries should be charged whenever they are discharged. For a safe and controlled charging, a lithium charger module can be used. Any charger module based on TP4056 can be used. It's advised to use a TP4056 based module, with protection, in order to prevent any damage of batteries due to overcharging or short circuits.

f) Buttons: they are provided for a manual control. They help the user in operating the device.

Flowcharts

Many attacks can be performed on a RFID based system as seen earlier. The device is designed to simulate five attacks. The working of the device is resumed in the following flowcharts:

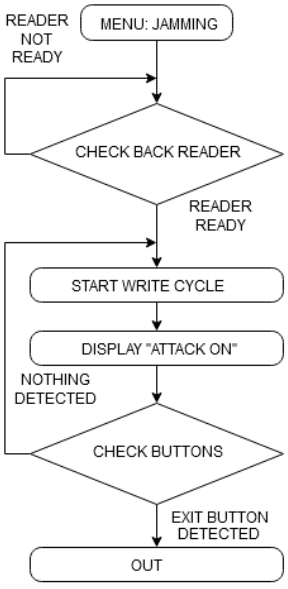

Figure 2: Jamming Attack

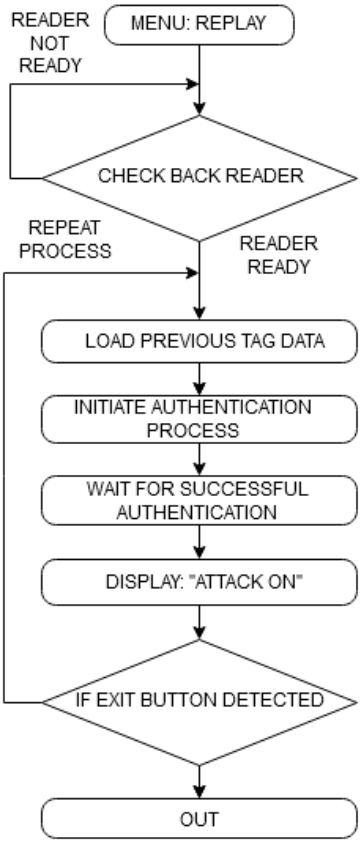

Figure 3: Replay Attack

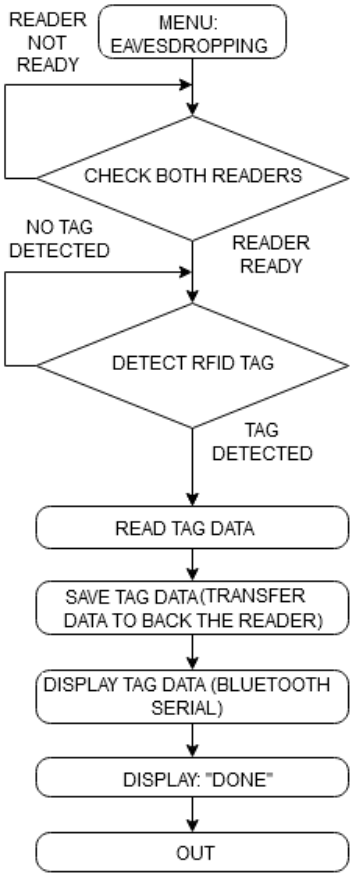

Figure 4: Eavesdropping Attack

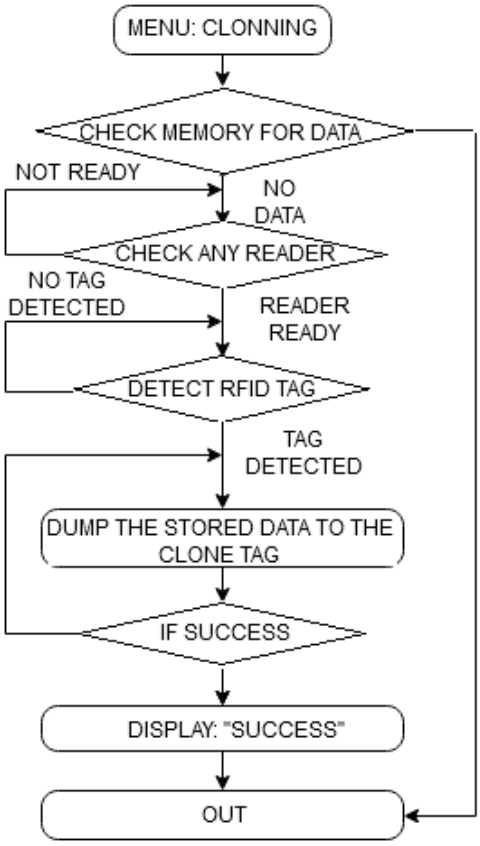

Figure 5: Cloning Attack

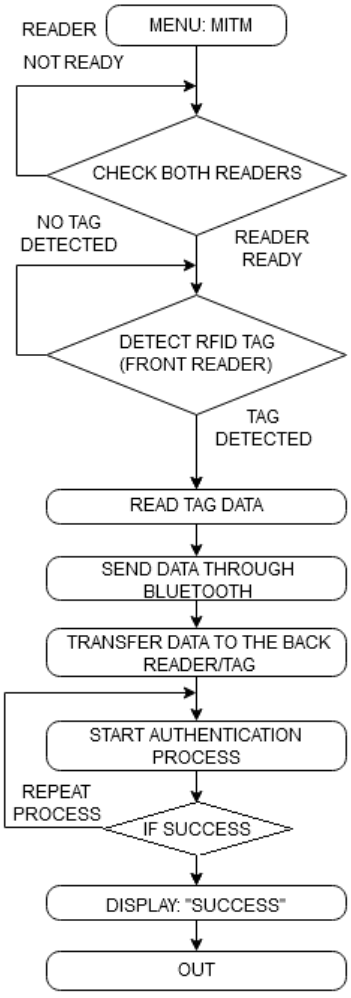

Figure 6: MITM Attack

5. Results and Discussion

The device has been designed, developed and tested successfully. Here are some photos of the hardware:

Figure 7: Device front and back view

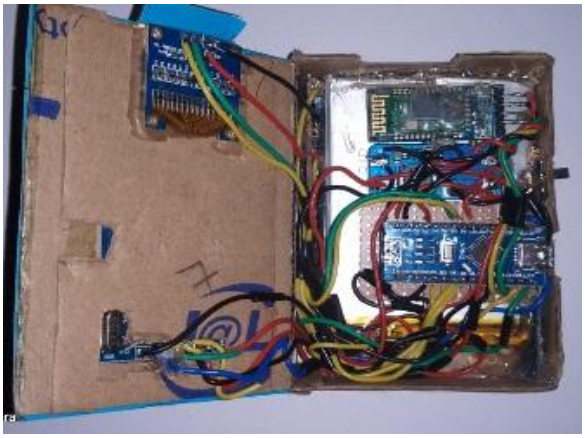

Figure 8: Device inside view

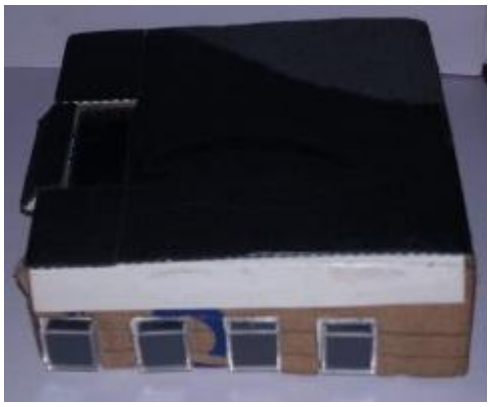

Figure 9: Device side view

The result of the simulation is shown below:
SYSTEM READY!

PREPARING THE AUTHENTICATION KEYS
FF FF FF FF FF FF

AUTHENTICATION KEYS READY!

PRESS THE FIRST BUTTON TO START

SYSTEM ARMED, FOLLOW THE STEPS

READY TO SENSE A TARGET CARD!

INSERT THE CARD AND PRESS THE FIRST BUTTON

CARD DETECTED! KEEP IT STEADY FOR READING

Card UID: F6 30 1F EF
Card SAK: 08
PICC type: MIFARE 1KB

**********SUCCESSFULLY READ!**********

READING CURRENT DATA CONTENT IN SECTOR 0
block no 0
246 48 31 239 54 8 4 0 1 228 138 91 157 52 246 29
block no 1
82 49 56 77 68 78 48 54 0 0 0 0 0 0 0 0
block no 2
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

**********OPERATION SUCCESSFULL!**********

PRINTING THE DATA BLOCK MAP (using key A)

0 3 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [0 0 1]
2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
1 52 31 38 4D 44 4E 30 36 00 00 00 00 00 00 00 00 [0 0 0]
0 F6 30 1F EF 36 08 04 00 01 E4 8A 5B 9D 34 F6 1D [0 0 0]

SUCCESSFUL OPERATION!

PRINTING ACTUAL COPIED DATA:
block 0
ʕ 0 ʕ 6

Out of the 5 attacks that can be performed, the cloning attack was simulated successfully. First, the target card, which should be cloned, is inserted in the device. Then following the instructions, the information available in the target card is read and displayed. Then the same information is copied and dumped on to another card.

The result of the simulation can be summarized as follows:

- No security against eavesdropping
- No solution to detect clone card
- Easy access to card data
- No prevention against card rewriting

By simulating this attack, we proved the ability of the device to simulate some attacks, following the flowcharts. As a result, we can see that first of all, the data available can be read easily by our device. The second remark is that the data is not encrypted, hence, on performing eavesdropping, since there is no mean of preventing attackers to access the data, the data can be accessed. From the moment data can be accessed, read, and rewritten, the security of the system is threatened. Therefore, some solutions should be proposed, so that the issues are overcome.

6. Conclusion and Future Scope

RFID is an emerging technology which can be used for many applications related to identification. It's a communication system which involves transmission of data from a source to a destination through a medium. As soon as data transmission is involved, data integrity as well as security comes into picture. Likewise in all communication systems, providing security is a must for data integrity and reliability of any system. Unfortunately, there are many threats which threaten RFID communication systems.

In order to propose a solution, our approach was consisting of finding and proving that the regular methods proposed to solve RFID issues was intended to solve specific issues, while many others were not addressed. In order to do so, a device has been designed and developed, to be used as a tool for performing attacks to any RFID system, thereby testing where the tested system fails.

Five major attacks were proposed to be a part of the testing scheme and out of them, one was simulated. After performing the simulation, the result was as expected, since the device was able to read data from the target card, and copy the eavesdropped data to another card. A simple way to counter eavesdropping is the use of encryption, which wasn't implemented and gave us access to the data stored in the card.

Likewise, the remaining attacks can be simulated to detect any leakage in the system and also to test any proposed solution. The design and development of the device was intended to expose the system vulnerabilities in order to propose suitable countermeasures. As a future work, the targeted issues will be addressed by proposing a solution based on block chain technology. Then the proposed scheme will be compared with the available proposed solutions and the developed device will be used to check whether the security level has been increased or not.

As a future work, a solution based on block chain technology will be introduced. The solution goal is to enhance the security of RFID based system and protect the system against some specific threats such as cloning, eavesdropping etc.

References

[1] Leian Liu, Zhiqiang Chen, Ling Yang, Yi Lu, Hongjiang Wang, "Research on the Security Issues of RFID-based Supply Chain", International Conference on E-Business and E-Government, 2010
[2] ShaoXiwen, "Study on Security Issue of Internet of Things based on RFID", Fourth International Conference on Computational and Information Sciences, 2012
[3] Karamdeep Singh, Gurmeet Kaur, "Radio Frequency Identification: Applications and Security Issues", Second International Conference on Advanced Computing & Communication Technologies, 2012
[4] Nidhi Desai, Manik Lal Das, " On the Security of RFID Authentication Protocols", International Conference on Electronics, Computing and Communication Technolo-

gies (CONECT), 2015
[5] Lijun Gao ,Zhang Lu, "Low-Cost RFID Security Protocols Survey", Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, 2011
[6] Gurudatt Kulkarni, Ramesh Sutar, Sangita Mohite, "RFID Security Issues & Challenges", International Conference on Electronics and Communication System (lCECS), 2014
[7] Dang Nguyen Duc, Hyunrok Lee, Divyan M. Konidala, Kwangjo Kim KAIST, Daejeon, "Open Issues in RFID Security", International conference for internet Technology and secured Transactions, (ICITST), 2009
[8] Namje Park, Howon Kim, Kyoil Chung, and Sungwon Sohn, "Design of an Extended Architecture for Secure Low- Cost 900MHz UHF Mobile RFID Systems", IEEE International Symposium on Consumer Electronics, 2006
[9] "Passive UHF RFID Transponders for switching and controlling", 2013 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)
[10] Jian Shen, Dongmin Choi, Sangman Moh, Ilyong Chung, "A Novel Anonymous RFID Authentication Protocol Providing Strong Privacy and Security", International Conference on Multimedia Information Networking and Security, 2010

Author Profile

Kouame Yann Olivier A. is currently pursuing masters degree program in Digital Communication and Networking, in REVA University, India,

Dr. Venkateshappa, Associate professor, School of Electronics and communication, REVA University, India