Implementing RFID Information Security System

Chandu Asok
Student,Mtech CSE
Younus College of Engineering and Technology,
Vadakkevila, Kollam-691010

Abisha A
Asst.Professor ,CSE
Younus College of Engineering and Technology,
Vadakkevila, Kollam-691010

***Abstract:-* RFID(radio frequency identification) plays an important role in the exchange of data's or information. The inventors of RFID were not able to implement the RFID security but they just focussed on the general working of RFID. As we all know where there is an information flow we have to maintain the different aspects of security, thus protecting the valid information's that is present on the RFID tag. Thus we are enabling a concept called RFID INFOSEC by introducing a new layer called security layer to the already existing RFID reference model. The main objective of this security layer is to establish confidentiality, integrity, availability to the data i.e., the security aspects of data. The threats in the RFID system is being analysed using a threat modelling process called STRIDE and a risk analysis model named DREAD to determine and to mitigate security risks. The threats can be removed by the introduction of a security layer in the reference model. RFID (Radio Frequency Identification) is a technology whose employment will certainly grow in the following years. It is therefore necessary to consider the security issues that come out from the implementation of that type of systems. In this paper we present an approach to solve the security problems in RFID systems by designing a naive security layer based on authentication and encryption algorithms. The authentication mechanism is the mutual authentication based on a three-way handshaking model, which authenticates both the reader and the tag in the communication protocol.**

I. INTRODUCTION

RFID (Radio Frequency Identification) is a technology whose employment will certainly grow in the following years. Radio-frequency identification (RFID) is an automatic identification and data capturing technology, which can be used in different fields in order to identify and track goods and people. The history of RFID returns to around 70 years back in Second World War which RFID was used to identify enemy aircraft.

II. RFID FUNDAMENTALS

1. RFID TECHNOLOGY

In this section, we present an overview of the RFID technology. The first idea on RFID came out in 1948with Harry Stockman who assured that the communication by reflected power could be viable. An RFID system is always made up of three components the tag is a transponder located on an object and holds the data that identifies it; the reader is a data capture device; and an application that processes all the information gathered by the reader. RFID technology is based on the idea that an electronic circuit in a tag can be powered from a distance by a reader device which broadcasts energy to it using electromagnetic fields. When the tag is powered, it can exchange information with the reader through a physical principle known as backscatter modulation

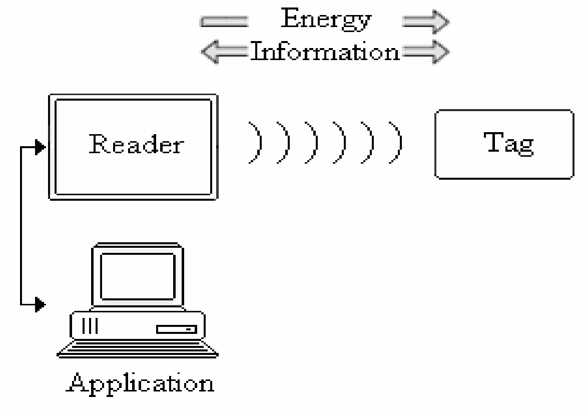


Figure 1: Simple rfid implementation

Data transfer from tags to readers must be done in a reliable way. A reliable communication depends on the coding technique and the modulation scheme of the transmissions. The coding technique in RFID systems must be selected in order to maintain the tags powered, as long as possible, not to consume too much bandwidth, and to detect collisions. Data coding determines the representation of each bit in a frame, meanwhile modulation determines how tags and readers communicate. Since RFID systems generate and broadcast electromagnetic waves, they are classified as radio systems.

2. SYSTEM COMPONENTS

2.1RFID TAG

Active tags contain their own battery that is used for both powering the chip and boosting the return signal. The battery gives the tags the ability to continuously monitor high-value goods or a container's seal status. Compared to passive tags, active tags have wider read ranges (tens of meters and even hundreds of meters), larger memory capacities, and faster processing times. However, battery life limits the life of the tag.

Therefore, it is more accurate to use the term “battery-assisted tag”. Battery-assisted tags have a power source that can keep the chip on the tag constantly powered. However, they can be programmed top reserve battery power by only signaling if an alert condition is detected, or only at predetermined time intervals. In addition, battery-assisted tags may incorporate one or more sensors, enabling them to monitor environmental conditions, such as temperature, humidity, shock, or vibration. These tags are often implemented on reusable containers or other assets in logistic applications. When the contents of the container are changed, new information can be updated on the tag. In this, we will use RFID as a generic term to describe any automated tagging and reading technology, including active, passive, and battery-assisted RFID technologies, and various formats and applications.

2.2 RFID READER

- A device that is used to interrogate an Tag.
- Basic components are a scanning Antenna
- A transceiver with a decoder to interpret data
- Helps in personalize & read data.

An RFID reader is a powered device that wirelessly communicates with the RFID tags and facilitates data transfer between the tag and the backend system. A typical reader consists of a radio frequency module, a control unit, and a coupling element to interrogate electronic tags via radio frequency (RF) communications. The basic functions of the reader include activating tags by sending querying signals, supplying power to passive tags. RFID readers differ considerably in complexity, depending on the type of tags being supported and the functions being performed, such as sophisticated signal conditioning, parity error checking, and correction. They can either be portable handheld units or fixed devices. RFID systems also rely on software. The software can be divided into three groups: front end tag reading algorithms, middleware, and backend system interface. The front-end algorithms carry out the signal processing tasks. RFID middleware connects readers to the backend server and database. It also filters the data acquired from the reader and handles various user interfaces. The real power of RFID comes in integrating RF technology with a backend system to perform functions such as matching digital information received from the reader against the backend database and routing the retrieved information to the correct application.

3. RFID REFERENCE MODEL

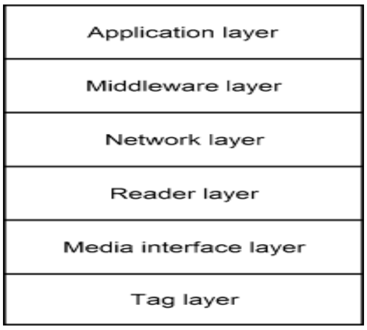


Figure 2: Reference model.

Standard six-layer grouping of different functions for an RFID system

Application layer: refers to different RFID uses (i.e. item management).

Middleware layer: refers to procedure that translates/filters data from reader to application.

Network layer: refers to the communication pathway between reader and application residing on a server.

Reader layer: refers to the architecture of a reader – a computer and receiver in one package connected to antennas.

Media interface layer: refers to the way the reader controls access to the media (generally wireless).

Tag layer: refers to the architecture of the tag including power harvesting circuit, modulator, demodulator, logic, and memory layout.

III. IDENTIFYING AND RANKING THE THREATS

1. IDENTIFYING THREATS USING STRIDE MODEL

In this section, the threats to RFID will be categorized using a well-known model for designing software systems. Threats are potential events that cause a system to respond in an unexpected or damaging way. The first step in building a secure system is to understand the threats. It is useful to categorize threats to determine strategies for mitigating them. One way to categorize threats is called STRIDE. STRIDE is an acronym for six threat categories that are listed below.

SPOOFING IDENTITY: Spoofing occurs when an attacker successfully poses as an authorized user of a system.

TAMPERING WITH DATA: Data tampering occurs when an attacker modifies, adds, deletes, or reorders data.

REPUDIATION: Repudiation occurs when a user denies an action and no proof exists to prove that the action was performed.

INFORMATION DISCLOSURE: Information disclosure occurs when information is exposed to an unauthorized user.

DENIAL OF SERVICE: Denial-of-service denies service to valid users. Denial-of-service attacks are easy to accomplish and difficult to guard against.

ELEVATION OF PRIVILEGE: Elevation of privilege occurs when an unprivileged user or attacker gains higher privileges in the system than what they are authorized.
Spoofing occurs when an attacker successfully puts on as an authorized user of a system and so, for example can perform an inventory of a store without any authorization through the scanning the EPC tags. When the attacker modifies, adds, deletes, or reorders the data, tempering attack occurs. For example modification of the tag on the passport while, modifies EPC number on tags in the shopping mall, kills or erases a tag in supply chain. Repudiation occurs when a user denies an action and no proof exist to prove that the action was performed, for example a retailer denies receiving a certain pallet, case or item or in other example the owner of the EPC number denies having information about the item to which the tag is attacked. Information exposure happens when the information is manifested to an unauthorized user i.e., a smart bomb placed at a street corner detonates in the time that a specific person with an RFID-enable passport discovered. Denial of service occurs when the system denies service to a valid user and for performing this attack, a tag can be killed, blocked to shoplifter can take the stolen item out of the shop or removed and maybe physically destroyed. Looming of privilege occurs when an unprivileged user or attacker gains higher privilege in the system than what they are empowered for example attacker can write or add malicious data in to the system as an administrator.

2. RANK/PRIORITIZE THE VULNERABILITIES USING DREAD MODEL

DAMAGE POTENTIAL: The extent of the damage if vulnerability is exploited.

REPRODUCIBILITY: How often an attempt at exploiting a vulnerability works.

EXPLOITABILITY: How much effort is required? Is authentication required?

AFFECTED USERS: How widespread could the exploit becomes?

DISCOVERABILITY: The likelihood that the researcher or hacker will find it.

3. PROPOSED SECURITY LAYER TO RFID REFERENCE MODEL

In this section we describe the proposed security layer for solving the security problems in RFID systems.

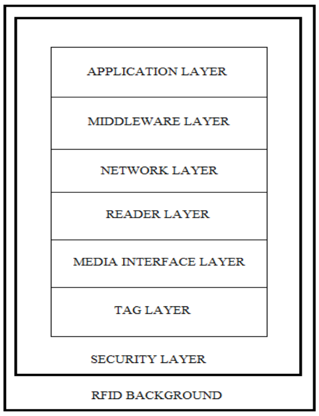


Figure 3: Proposed rfid reference model.

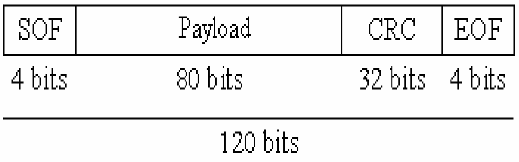
This proposal covers the air interface, the data frame, the authentication protocol and the encryption algorithm. Implementation of the security layer can be done using certain mechanisms which includes air interface, data frame, authentication mechanism, encryption mechanism and finally the hardware implementation of the security layer.

3. AIR INTERFACE

RFID systems are radio systems that work in frequencies within unlicensed bands. Unfortunately, at the present time, a general consensus on the operation of this technology does not exist since each manufacturer designs proprietary systems. The work reported in this paper proposes the operation of RFID technology in the band of 13.56MHz in order to comply with the national regulations existing in the United States and Japan. The operation mode chosen is half-duplex using FSK modulation. This mode is chosen because the active tags used in this proposal are always connected to their own power source, allowing them to have enough energy to process data.

4. DATA FRAME

Information is transferred between tags and the reader using data frames of 120 bits, of which 80 correspond to the payload of transmission and 40 to control traffic. Each frame has a 4 bits sequence to determine the header of the frame, SOF (Start Of Frame) and other to determine the trailer, EOF (End Of Frame). The SOF sequence is specified by bits “1101” whereas the EOF sequence is specified by bits “1011”. The length of these fields was determined in order to limit the control traffic and increase the transmission efficiency. There is a 32 bits field of CRC (Cyclic Redundancy Check) to provide error detection in message transmissions.



SOF	Payload	CRC	EOF
4 bits	80 bits	32 bits	4 bits

Figure 4: Data frame

5. AUTHENTICATION PROTOCOL

The authentication scheme chosen in the security layer is the mutual authentication based on a three way handshaking model which is an implementation of a Simple Authentication. In this approach, none of the communicants will receive any secret information during the authentication process. Furthermore, tag tracking is prevented since the tag would not respond at all to a query sent out by a reader that does not know the secret key.

The authentication protocol is shown in the figure. Reader A has a data base of all the private keys from each user KX. When the reader tries to establish a communication with tag B, it sends its identification number IDA and a private session key KS, both encrypted under the secret key KB, together with a random number r1 encrypted under the session key. Only entity B is able to decipher the message to obtain KS and IDA, which tells B that the source of the message is A. With the decryption of this message, the key establishment stage is completed and both A and B are in possession of the session key. Next B obtains the random number r1 by decipherment using KS. Tag B takes r1 and sends it back with another random number r2, both ciphered under KS, to establish a mutual authentication. The appearance of r1 in the message authenticates B to A. Finally, A authenticates itself by sending back the random number r2. If all the steps are successfully carried out, the mutual confidence is sufficient to enable communication, encrypted under KS. In this way, tag B identifies itself by sending IDB which is the information that the reader provides to the application.

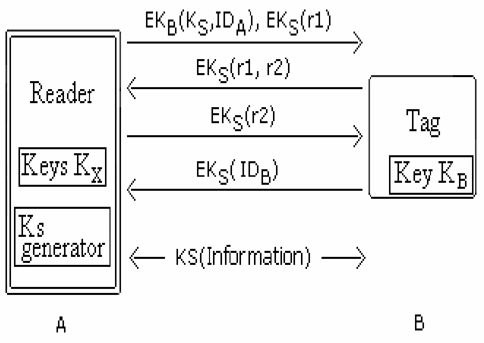
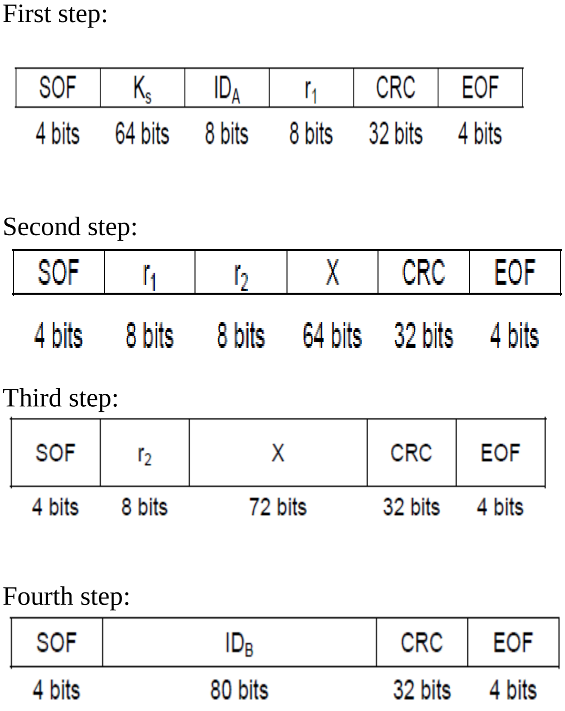


Figure 5: Authentication protocol

The information exchanged by the tag and the reader is embedded into the data frame shown in the figure. The figure provides a more detailed view of the information exchange. Note that the second and third step of the authentication process leaves unused bits (indicated by X).



First step:

SOF	K_S	ID_A	r_1	CRC	EOF
4 bits	64 bits	8 bits	8 bits	32 bits	4 bits

Second step:

SOF	r_1	r_2	X	CRC	EOF
4 bits	8 bits	8 bits	64 bits	32 bits	4 bits

Third step:

SOF	r_2	X	CRC	EOF
4 bits	8 bits	72 bits	32 bits	4 bits

Fourth step:

SOF	ID_B	CRC	EOF
4 bits	80 bits	32 bits	4 bits

Figure 6: Detailed view of the authentication protocol.

6 ENCRYPTION ALGORITHM

The architecture and limited hardware resources of RFID tags suggest the use of symmetric-key encryption methods, especially stream ciphering. The algorithm chosen to implement encryption in the system is RC4, that is, one of the most used stream ciphers. This algorithm is chosen because it is simple, fast and easy to implement. By this way, the second attack in RFID systems, eavesdropping transmissions with the purpose of successfully obtaining information, can be neutralized. Note that the implementation of RC4 requires only memory, adders and registers and, therefore, it is possible to adopt the algorithm in a low-price RFID tag.

The RC4 algorithm was designed by Ron Rivest in 1987 and was kept as a secret until 1997 when an anonymous description was published on the web. Many cryptanalysts assure that using RC4 lead to insecure cryptosystems but, in practice, it has been demonstrated that those cryptosystems have an acceptable security level. This algorithm generates a pseudorandom stream of bits called key stream. In the encryption process, it is combined with the plaintext using XOR, and in the decryption it is combined with the cipher text. The key stream is generated from a permutation of all 256 possible bytes. This permutation is initialized with a variable length key which in our proposal fits to 64 bits, using the KSA (Key-Scheduling Algorithm) algorithm. Once the permutation is done, the stream is generated using the PRGA (Pseudo-Random Generation Algorithm) algorithm. The KSA algorithm which is used to initialize the permutation in an array S, is described as follows.

```
1) Array S is initialized with the identity permutation.
for i from 0 to 255
S[i]=i
2) Array S processed 256 times.
for i from 0 to 255
j=(j+S[i]+key[I mod key_length]) mod 256
swap(S[i],S[j])
```

The PRGA algorithm generates one byte from the key stream so it must be executed as many times as needed in order to get a stream within the desired length. The steps of the algorithm are:

```
1) Each execution increments counter i, and the new value of counter j is computed by adding the current value of j with the value of S indexed by i.
i := (i + 1) mod 256
j := (j + S[i]) mod 256
2) The values of S indexed by i and j are swapped.
swap (S[i],S[j])
3) The output generated corresponds to the value of S indexed by
(S[i]+S[j]).
output S[(S[i] + S[j]) mod 256]
```

One of the advantages of using RC4, instead of other stream ciphers, is its software implementation because it requires only byte-length manipulations. In the hardware implementation, it requires only memory modules, byte-length adders and registers. One of the vulnerabilities of the RC4 algorithm consists in the fact that the key stream generator is slightly biased in favour of certain sequences of bytes. RC4 does not take a separate nonce alongside the key. Such a nonce is a requirement for security so that encrypting the same message twice produces a different cipher text each time. A secure solution to this that works for any secure cipher is to concatenate the key and a nonce. By this way, a 64 bit length dynamic key KK is generated from an 40 bit-length static key K and a 24 bit-length initialization vector IV, as it is shown in the figure

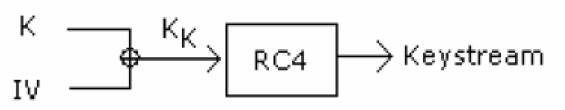


Figure 7: RC4 with dynamic key.

This cipher scheme is the one used in WLANs (Wireless Local Area Networks), also known as WEP. This encryption mechanism has a vulnerability, which consists in the transmission of the initialization vector IV in plaintext concatenated with the cipher text. As a result, in this paper we propose to modify the existing WEP protocol to make it more secure.

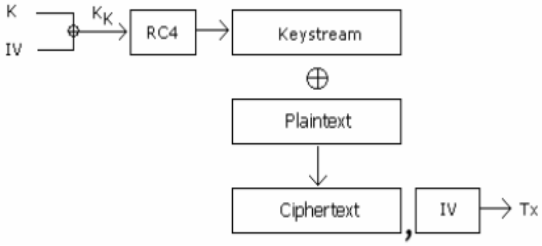


Figure 8: Wired Equivalent Privacy (WEP) protocol.

In order to neutralize the WEP security problem, we consider not transmitting the initialization vector, instead, we generate it in each entity in the communication system. That is, the generation of the IV is done by a lineal increment of its value for each data frame transmitted, and accordingly we obtain different values for the dynamic key KK. Note that a somehow similar approach has also been reported in which the idea is to update the shared secret key based on factors like network traffic and number of transmitted frames, and the results have shown that the proposed modification to the existing WEP protocol makes it more secure and robust in terms of message privacy.

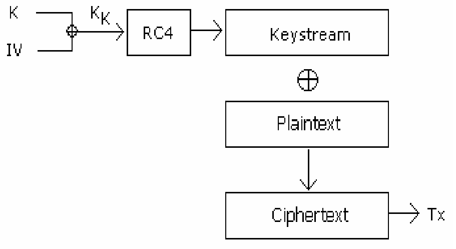


Figure 9: Modified WEP protocol.

The generation of the IV may be also randomly done, taking part of the key stream generated in the last encryption. However, this approach is not as secure as the aforementioned, because the probability of generating the same dynamic key KK for two different messages is high, thus the first perfect secrecy condition defined by Shannon would be broken.

IV. HARDWARE IMPLEMENTATION OF SECURITY LAYER

In this section we present the hardware implementation of the proposed security layer for RFID systems. Implementing the security layer with the extensions for encryption and authentication requires some considerations concerning the architecture of an RFID tag. RFID seems to be the future of next generation networks, but this will be only possible if the cost of implementation declines. Hence the architecture of tags must be simple enough to reduce manufacturing costs. In order to see the robustness and effectiveness of the security layer in a real system, we implemented it using VHDL in FPGAs communicated through RF transceivers.

One of the great advantages that VHDL has is the fact that the design of the systems can be made in a modular way. The modular design consists in dividing the main system in components in order to create subsystems specialized in certain tasks. The block diagram in Fig. 9 shows the main components of the designed system. The control unit is responsible for commanding the operation of the other modules. The communication unit is responsible for carrying out the communication protocol, which involves user authentication and data coding. The cryptographic unit is responsible for executing the ciphering algorithms, providing the communication unit with the messages encrypted. The configuration unit is responsible for configuring the transceivers used to implement the air interface. The port unit is responsible for linking the FPGA with the transceiver.

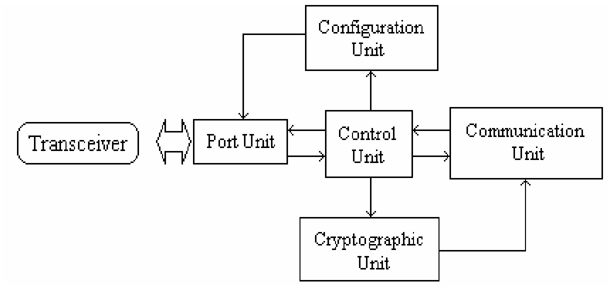


Figure 10: System block diagram.

The FPGA used for the implementation is the Xilinx xc3s200 model, from the Spartan3 family. The transceiver used for the air interface is the Atmel AT86RF211DB model. The system is implemented using two FPGAs, communicated through RF transceivers, which simulates the behaviour of an RFID network composed by a reader and a tag.

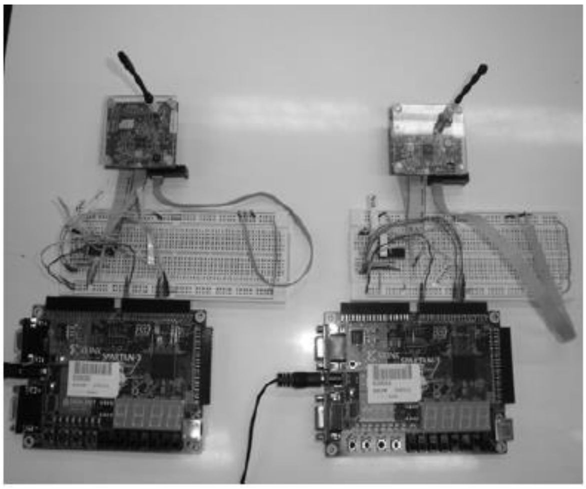


Figure 11: Hardware implementation of the proposed security layer for RFID systems.

The implementation of this modified WEP protocol can be realized very economically on FPGAs using a number of 192 gates like shown in similar approaches. It is important to note that the low cost demanded for RFID tags causes them to be very resource limited. In general, they can only have between 5000 and 10000 logic gates. Within this gate counting, only between 250 and 3000 gates can be committed to security functions. Note that encryption algorithms like Data Encryption Standard(DES) or Advanced Encryption Standard (AES) require more than 20000 gates to be implemented. Furthermore, power restrictions should be taken into account, since most RFID tags in use are passive.

V. CONCLUSION

In the work presented here, we were able to develop educational materials for teaching RFID INFOSEC and developed a new RFID reference model for organizing and teaching the material. The main contribution of this work is the threat modelling process used to categorize threats, quantify risks and to identify mitigation techniques that can be applied to any information system. Thus helped to develop a new layer called security layer to the already existing rfid reference model. The various mechanisms used to implement the security includes both the hardware concept as well as the software concepts. The hardware concepts include the use of the air frame, data frame, authentication mechanisms and encryption algorithm while the hardware concepts include the use of VHDL with FPGA transceivers. Thus help to maintain a security concepts to the security layer of the reference model in an rfid system.

VI. FUTURE ENHANCEMENT

The various enhancement that can be used in an RFID system includes the implementation of a new methods of identifying the threats. The threat identification and ranking mechanism used in this approach lacks the concept of efficiency. The procedure of ranking the threats is not the ideal method of classifying the threats. The STRIDE as well as the DREAD MODEL is not the ideal method of classifying as well as recognizing the threat. So a further improved mechanism should be implemented.

VII. REFERENCES

[1]Weis, A. S., Security and Privacy in Radio- Frequency Identification Devices, Master Thesis. MIT,2003.

[2]Garfinkel, S., A. Juels and R. Pappu., RFID Privacy: An Overview of Problems and Proposed Solutions, IEEE Security & Privacy. May/June 2005, pp. 34-43.

[3]A. Juels, “RFID security and privacy: A research survey,” IEEE J. Sel.Areas Commun., vol. 24, no. 2, pp. 381–394, Feb. 2006.

[4]D. R. Thompson, “Teaching RFID information systems security to non-RF students,” in *Proc. IEEE Wireless Microw. Technol. Conf.*, Clearwater, FL, USA, Apr. 20–21, 2009.