INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURING RFID SYSTEM USING AES ALGORITHM

MS. PRIYA. DESHMUKH[1], MS. POOJA. DESHMUKH[2]

Student of PRMIT & R-Badnera.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract- Radio Frequency Identification (RFID) is an emerging technology which brings tremendous productivity benefits in applications. Where RFID is use for tracking and monitoring purpose. It is wireless non-contact system which uses radio frequency for tracking. As the use of RFID is growing day by day in various fields of applications. Due which the issue related to the security and privacy of RFID system has being raised. Solution to this problem is to authenticate RFID tag to the reader device using the AES as a cryptographic primitive. Which work on RFID tag with low power consumption, small size and also having low cost.

Keywords—AES, RFID.

PAPER-QR CODE

Corresponding Author: MS. PRIYA. DESHMUKH

Access Online On:

www.ijpret.com

How to Cite This Article:

Priya Deshmukh, IJPRET, 2016; Volume 4 (9): 473-477

INTRODUCTION

Radio Frequency Identifiers (RFID) is an emerging technology. It uses the radio frequency for tracking and monitoring purpose. Due to the efficiency and the flexibility of RFID make it superior technology as compare to the barcode and the QR-code technology. It does not required line of sight for reading the RFID tag. It has low cost, more durability and it can be read and write. The RFID tag is of mainly two types i.e. of active and passive tag.

Active RFID tag- Because they have their own power source, active tags transmit a stronger signal, and readers can access them from further away. The on-board power source makes them larger and more expensive, so active RFID systems typically work best on large items tracked over long distances. Low-power active tags are usually slightly larger than a deck of playing cards. Active tags can remain dormant until they come in range of a receiver or can constantly broadcast a signal. Because of their on-board power source, active tags operate at higher frequencies—commonly 455 MHz, 2.45 GHz, or 5.8 GHz—depending on the application‘s read range and memory requirements. Readers can communicate with active RFID tags across 20 to 100 meters.

Passive RFID tag-Passive tags, on the other hand, are very inexpensive; they can cost as little as 20 cents apiece, and new technologies are constantly making them cheaper to integrate into common materials and products. In addition to their low cost, passive tags can also be quite small. Current antenna technology limits the smallest useful passive tag to about the size of a quarter. The larger the tag, the larger the read range. Currently, passive RFID tags contain about 2 Kbits of memory. This is too small to hold much more complex information than identification and history information. The technology behind RFID is constantly improving, so the amount of information and capabilities of RFID tags will increase over time, allowing RFID tags to eventually contain and transmit much more information.

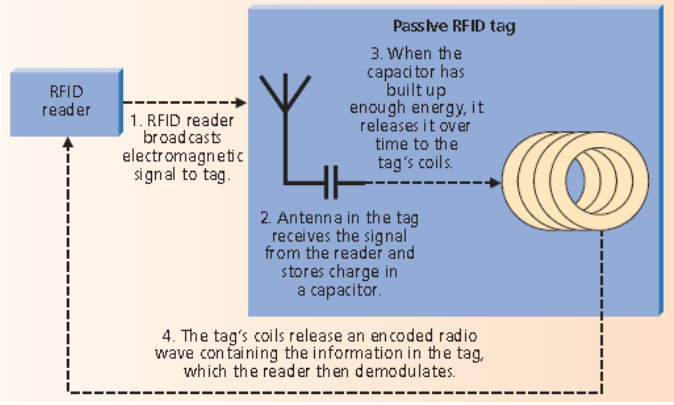

Figure1. General working of RFID tag

There are different formats of RFIDi.e, credit card size labels, token and coin, wrist band and paper tags. The advantages of RFID are:

1. Ability to read data without visual access
2. Ability to read data from moving objects
3. Ability to read data at distance, from 3cm to 100 metres
4. Ability to secure the tag dataAbility to update data in the tag (write)
5. Ability to have automated read of tags
6. .Ability to have the tag form to suit the application

The application of RFID in various field has make the impact some of the applications are
Use in library books and in book stores.
For animal tracking and monitaring.
For tacking the supply chain of the products
Tacking the documents which are confidential.
Microwave RFID are use for tracking the truck and the ships use for transportation.
RFID Tag architected

The architecture of a security-enhanced RFID tag is sketched in figure 2. It consists of four parts: analog frontend, digital controller, EEPROM, and AES module. The analog frontend is responsible for the power supply of the tag which is transmitted from the reader to the tag. Other tasks of the analog frontend are the modulation and demodulation of data and the clock recovery from the carrier frequency. The digital control unit is a finite state machine that handles communication with the reader, implements the anti-collision mechanism, andexecutes the commands in the protocol. Furthermore, it allows read and writeaccess to the EEPROM and the AES module. The EEPROM stores tag-specific data like the unique ID and the cryptographic key. These data must be retained when the power supply is lost. The security-enhanced RFID tag calculates strong cryptographic authentication with an AES module which is designed for low power requirements and low die-size restrictions.

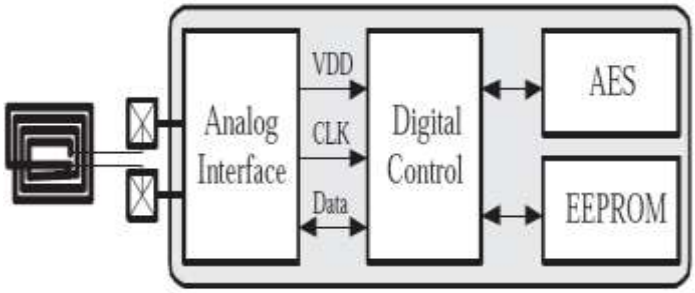

Fig.2. Architectures of RFID tag

AES architecture

RFID systems are susceptible to security attacks: as they work non-line-of-sight and contactless, an attacker can work remote and passive attacks will not be noticed. Some of the main concerns are (unwanted) consumer tracking, tag forgery and the unauthorized access to the tag's memory content. These security risks have to be dealt with in order to gain a broad user acceptance.

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm which was selected in 2001 by the National Institute of Standards and Technology (NIST) as the Federal Information Processing Standard FIPS-197 [13]. It operates on blocks of data, the so called State, that have a fixed size of 128 bits. The State is organized as a matrix of four rows and four columns of bytes. The defined key lengths are 128 bits, 192 bits, or 256 bits. As in this case AES-128 has considered for the process. Every bytes of the State matrix is affected by these transformations:

1. SubBytes-substitutes each byte of the State. This operation is non-linea..It is often implemented as a table look-up. Sometimes the SubBytes transformationis called S-Box operation.
2. ShiftRows- rotates each row of the State by an offset. The actual value of the offset equals the row index, e.g. the first row is not rotated at all; thelast row is rotated three bytes to the left.
3. MixColumns- transforms columns of the State. It is a multiplication by a constant polynomial in an extension field of GF(2^8).
4. AddRoundKey- combines the 128-bit State with a 128-bit round key by adding corresponding bits mod 2. This transformation corresponds to aXOR-operation of the State and the round key.

AES is a flexible algorithm for hardware implementations. The power requirements for RFID tags are even too restrictive. Therefore, AES algorithm is use on 8-bit data.

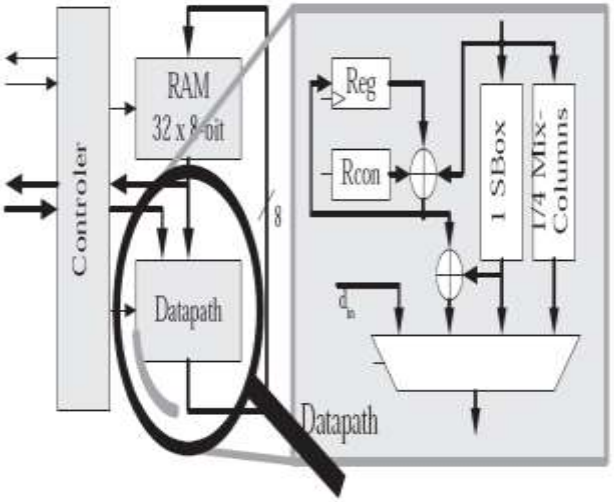

Figure3. Architecture of the AES modules

In order to work with minimum power supply.An encryption of a plaintext block works as follows. Before encryption is started the plaintext block has to be loaded into the RAM of the AES module.The communication between the reader and tag is byte-oriented which fits nicely into the 8-bit architecture of the AES module: every received byte can be stored in

the AES module.The cryptographic key is obtained in a similar way from the tag's EEPROM. Now the AES algorithm can be executed. It starts with a modification of the State by an AddRoundKey operation using the unaltered cipher key. Ten AES rounds follow by applying the transformations SubBytes, ShiftRows, MixColumns, and AddRoundKey. Only the last round lacks the MixColumns operation. Roundkeys are calculated just in time. This is usually called on-the fly key schedule. The round key is derived from its predecessor by using the S-Box, the Rcon, and the XOR functionality of the datapath.The proposed combinational S-Box by omitting the decryption circuitry to suit our encryption-only AES. One feature of this S-Box is that it can be pipelined by inserting register stages. The S-Box makes use of one pipeline stage.

CONCLUSION

In this paper, the security of the RFID system has enhanced using the AES algorithm which provides strong cryptographic authentication. This has set new milestone for new security demanding applications and for everyday usage of RFID technology.

This AES architecture which work at low power consumption. With minimum cost and low size. The data stored in the tag should be secured from unauthorized access hence AES architecture is used. As each tag has its own unique identification data, so user data privacy and location privacy are guaranteed.

REFERENCES

1. P. Chodowiec and K. Gaj. Very Compact FPGA Implementation of the AES Algorithm.In C. D. Walter, C¸ etin Kaya Ko¸c, and C. Paar, editors, Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings, volume 2779 of Lecture Notes in Computer Science, pages 319–333.
2. EPCglobal. 13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification. http://www.epcglobalinc.org/, February 2003.
3. K. Finkenzeller. RFID-Handbook. Carl HanserVerlagM¨unchen, 2nd edition, April 2003.
4. S. A. Weis. Security and Privacy in Radio-Frequency Identification Devices. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, May 2003.
5. S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Computing, 1st Annual Conference on Security in Pervasive Computing, Boppard, Germany, March 12-14, 2003, Revised Papers, volume 2802 of Lecture Notes in Computer Science, pages 201–212. Springer, 2004.
6. TruptiLotlikar, RohanKankapurkar, AnandParekar ,AkshayMohite. Comparative study of Barcode, QR-code and RFID System. In International Journal Computer Technology &Applications,Vol 4 (5),817-821.
7. BatboldToiruul, and KyungOh Lee, An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems. In International Journal of Computer Science and Network Security, VOL.6 No.9B, September 2006