International Journal of Engineering & Technology, 7 (3.34) (2018) 935-939

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Estimation of Reasonable Attacks against RFID Tags for Trusted Entities in Cyber Space

[1]Parvathy Arulmozhi1, [2]JBB Rayappan, [3]Pethuru Raj

[1, 2]Department of Electronics & Communication Engineering, SEEE,SASTRA University, India
[3]Chief Architect, Reliance Jio Cloud Services (JCS), Bangalore, India
**Corresponding Author E-mail: [1]parvathy@ece.sastra.edu*

Abstract

Authentication can be done in many ways. The significance of selecting andsetting appropriateauthentication route is maybe the most essential decision for scheming the safe systems. Authentication protocols are also able to connecting the authenticating party as well as authenticating itself to the connecting party. The password authentication schemeis the common usedmethod working with small cost, however it is very easy to recognize and consider as weak system in term of security,due to attacks in software. Password software attack is implanted and triggered byvisiting a forged site that look like the normal business-related site. Somefalse website has residential keyboard logging software to duplicate the user ID and password. This study shows that the password verification system is highly protected if the password is related to some soft tokens which is generated by the RFID systems.The authentication and security is improved by the design and manufacturing of RFID circuit,releaseextraproperty (Tag storage) in RFID that can be used for previousfunction, such as lowpower utilization anddefence of RFID tags with safety algorithms.

Keywords: *RFID System, Transponder, Encryption, Decryption, Python software.*

1. Introduction

In order to transmit data the wireless magnetic fields in radio frequency identification is used and for automatically recognizing and tracking tags attached to the objects. The tags contains information stored electronically. It has rapidly increasingly upon in the past decade years, because of its major driver for the development of tagging physical objects, things with a radio chip and computer interface. Technology in RFID is the way to "internet of Things (IoT)", and fated as persistent surveillance. As RFID is ever-present, the tags are sensibly secure. So the tags data could be secured with encryption technology. Excluding the tag IDextra memory is needed to store the securitykey valueso protection. Based on EPC global network class 1 and Generation2 (C1G2) the RFID data are encrypted with light weight memory algorithm. By using a compression techniques the data are stored either in CSV or XML format. This system does not required any central data base instead that the EPC based security key is used to encrypt and decrypt the RFID with large number of rounds. The conclusion ofthe result are discussed in Lab View software.

Radio Frequency Identification (RFID) is one of the talented automatic authentication tool in the playing fieldof cloudand pervasive computing [2]. RFID reader can sensemultiple tags at a time .The stored unique numbers (ID) and key valves are in each tags are manipulated withthe back end server.So many times it could be misread or misused.So duplicate data are generated and wrongly interpreted by the users on the internet. Therefore the RFID confidential data are exploited by the attackers. In order to avoid that, it should be safe guard withthe security algorithms. Thereforethe RFID implementation cost, making awarenessof Return on Investment (ROI) incommercial applicationsmore accomplish.

2. RFID Adoption

RFID application in industrial line can be established nowadays in management of supply chain, automated billing system, airbag management and so on. [1,2] Last few years the RFID systems are used as an communication device on Cloud and IoT platforms with and web based languages such as java, Ruby Smalltalk and python . [3]The sensitive information of RFID data is being communicated overthe internet and is stored in cloud by using a different storages.Certain authentication protocols and security algorithms make the RFID systemmore affordable and intractability. [4] RFID is a general idiom for a technology that uses a radio frequency on contact-free communication between a reader and tag.Furthermore, the encoded messages between the tag and reader that exposing the significance is more costly compared to assembled information. The encrypted version of EPC or tag ID that needs a large number of computational round to break the information. [5, 6]A traditional approach to provide the secured authentication.

2.1RFID Security Concerns and Threats

RFID is not a flawless system. Similar to other dump devices, it has a lot security and privacy risks which are addressed by IT, and any organizations. In spite of its boundless applications and acceptance, RFID posses safety risk and tasks that have to be dealt accordingly prior to formation.The encoded messagesbetween the tag and reader that exposing the significance is more costly compared to assembled information. The encrypted version of EPC or tag ID that needs a large number of computational round to break the information.

3. Technical Overview

3.1 RFID Tags

Microchip and a transponder are the two important component in RFID. The data and unique identifier code is written at manufacturer point and it can also be programmed by OEM or end user .Tags may be passive tags or active tags... Passive tags are smaller look like a ricegrain, and getting smaller.

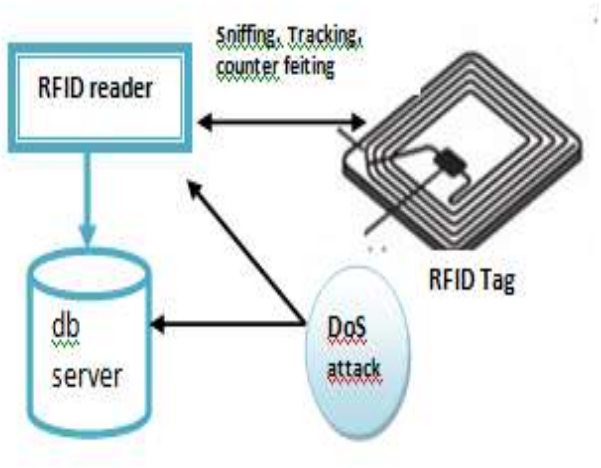

Fig. 1: Reader to Unprotected tags Security attacks

The reader's antenna sends power to the transponder which will activate the data stream when the tag reaches or enters the radio frequency range. Passive tags have smaller memory and the active tags are cheaper.

3.2 An Insecure Tags Vulnerable to the Following Issues

The needs for new tags should comprise and support the new safety applications on the internet. Nowadays the enhance RFID tags such as mifare .two problems can be solved. Authenticity difficulty problem will be dealt first. This is suitable ifany industry wants to defend designated products from embezzlement or if RFID tags are worked in car keys to control the immobilizedplan on and off. The next problem is, to stop the track of clients via the RFID tags they bring. This defence of privacy is generally a big confront in the face of the appearanceof new wireless technology.

The following table shows the attacks of RFID system on the internet.

Table 1: RFID attacks and causes.

S.No	Name RFID Security attack	Cause of issues
1	**Sniffing**	A request sent by a fake RFID reader
2	**Traffic analysis**	To predict the tag responses with respect to time.
3	**Denial of service attacks**	An attacker can employ the " pulse signal in RFID tags for security
4	**Spoofing**	The software which allow the attackers to restore RFID tag data with spoof data.
5	**RFID duplication**	Based on theRFID tags computing power
6	**Insertion attack**	Inserting commands of a system to the RFID system by in intruders
7	**Physical attack**	Interference based on electromagnetic counter script intelligence between the RFID tags and the tag reader.
8	**Virus attack**	RFID is also decumbent to attack based on virus

To attain admittance or validate authenticity of the product, intruders will mark data to basic tag or it can be changed in the tag. Three things intruders can do with the black tag are

- Changing the already available information in the tags which is very basic and can modify invalid tags into a valid tag and vice-versa.
- By embedding in another object the intruders can modify the tag of an object to that of another tag
- Creation of new tag from another one using attached personal information

Confirm that your tag is using important kindof security algorithms such as tiny encryption Algorithm, Blowfish or Extended tiny encryption algorithm. Any device that prearranging with conscious objects. Passports or any documentsfor identification make sure that has a proper security or not. For real time application or health care monitoring system, the confidential data of RFID system could not be revealed. In order to protect the RFIDtag's data and avoid any anomalies in that RFIDsystem it is necessary to go for the encryption.

3.3Move towards for Tackling Security and Privacy Issues for RFID System

RFID tags are well thought-out "dumb" devices, in that they can pay attention and react. These will increase the risks of unauthorised access and tag data alteration. A lot of clarification for undertaking thesafety and confidentiality problem in RFID.

1. Tag data protection
2. Integrity of the RFID Reader
3. Privacy

3.4 Tag Data Protection Solutions

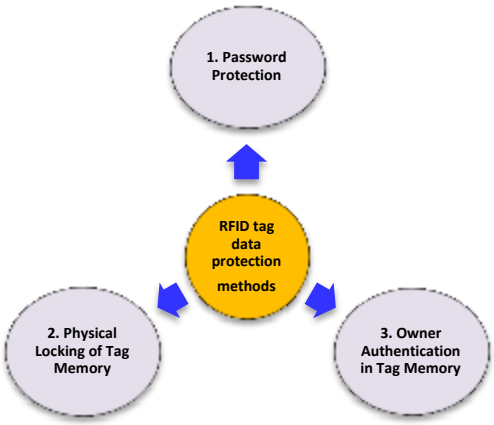

Fig 2: RFID tag protection methods

The integrity of the RFID reader and the personal privacy are related with readers .In may web applications the readers are trusted with only the RFID tag storage. Among these areas the RFID tag storage is concentrated because the tag data should not be revealed in security environment. So the encrypted data are collected by the readers and send to backend server for decryption. Here the Tiny Encryption algorithm is used and the results are verified in LAB View software .The following diagram shows the solution for RFID tag protection.

In order to protect tag data,usually the Passwords are used InIf common password is used for the tags, then the data becomes virtually public. Or else unique password, millions of passwords that want to be recorded. Any key stroke software is used by the hackers the passwords are easily hacked by the intruders. So lot of settlement is necessary for this solution.

The RFIDtag is embedded with small chip and has a unique number for identification of the object or any person. This adds identification of source. The drawback of this method is it cannot

be rewritable of data and additional memory is required for any alteration in algorithm.So advancedremembrancecharge and a larger amount memory is obtained.

4. Related Work for Designing Security Rfid Tag

4.1 Advantages of the Data on the Tag

Generally there are two different RFID systems are called close and open. In open RFID system the tags are read by every readers which is not trusted. But in closed system the tags are limited to well - known readers. So the RFID isan authentication - control system or an immobilizer system for cars. The starterlock resides a RFID reader and the tag is located in the car key.

4.1.1 Top Level Design of RFID Tag

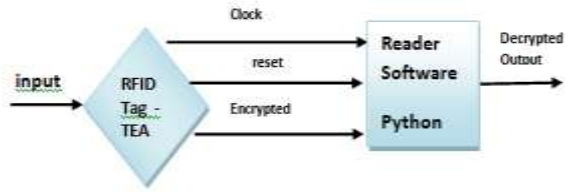

Fig 3: Information flow of RFID reader and tagfor protection

4.1.2 Background Information of RFID Tags

A simple RF based tiny encryption algorithm could be implemented forthe RFIDsystem. The size of the algorithm is very minimum and less complexity. It gives the better performance than the other cryptographic algorithms such as AES and DES. The permutation tasks are explained by f(y) = (y<<4 Å xy>> 5) + y, and sub key generatedfunctions are represented by sum + p (sum Q 3), and sum + p (sum >> 11 Q3). Some of them acts as a selector from the given subkeys p0, p1, p2, and p3 based on bits 0 and 1 of the sum or bits 11 and 12. The final output of the permutation function and generated sub key generated are XOR ed and ADD ed to V0 and V1. V2 and v3. Before going to start the value of sum is given as zero and the value of RFIDdata is fixed to 0x9E3779B9.

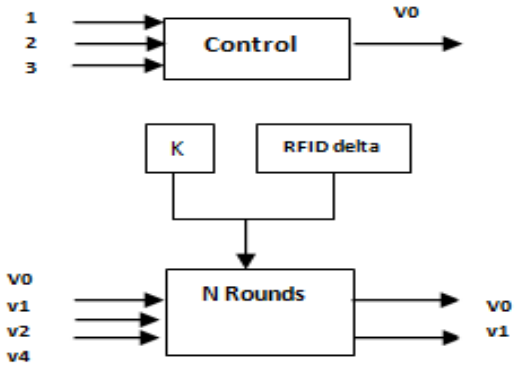

Fig 4: Software Implementation of RFID based TEA.

4.1.3 Inconsistent Rounds of RFID Data for Encryption

In another scheme we have investigated to keep the value of key fixed andvary the number of rounds *(nr)* in each session.

• The tag has a pseudo-random number generator (PRNG).
• *TrO* is an *r* round encryption/decryption RF-based TEA algorithm where *r* is a random number.

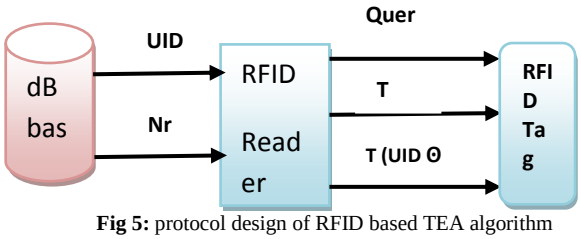

Fig 5: protocol design of RFID based TEA algorithm

The protocol operates as following:

1. At the start the reader generates a Query message for the tag.
2. The tag responds with *T (UID)* that is encrypted using n rounds (i.e. a default value is 16) and a fixed symmetric key which is known by tag and the reader
3. The reader decrypts this value to get the UID and forward it to the database. If both are matched, the tag is considered as true and it sends the PID and *nr* to the reader.
4. The reader encrypts PID using *T = (PID* $ *nr).*
5. The tag decrypts the received data to get ID $ *nr.* It uses XOR to retrieve the newvalue for number of rounds from *{(PID* $ *nr)* (f) *PID} = nr.*

5. Proposed Methodology

5.1 RFID Transponder - Formulate Location

RFID plays a very important role in redefining the process to make each person's job easier.The RFID-based equipment tracking system offers an effective solution of managing items particularly for a large-scale environment, the RFID technology combines with security devices to certify the items are always being supervised and record the important data and also enable the viewing of records via internet which is called as cloud computing.
In this methodology the RFID reader is connected local database server and the encrypted bit steam has to be stored in the tag. All the tags with additional memory and antenna that has aunique ID number (which is based EPC standard) and key value. To prevent the side channel attacks bit streams are protected by Extended Tiny Encryption algorithm with more number of rounds.

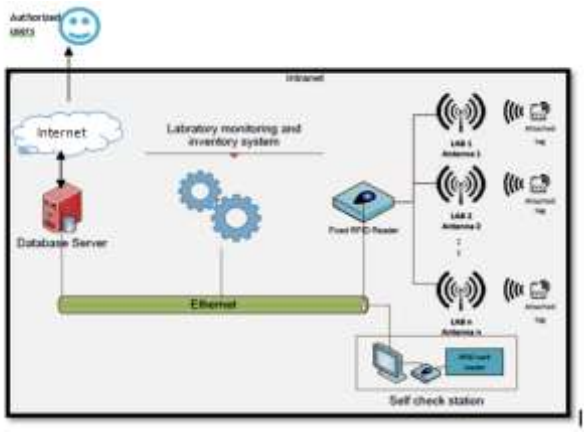

Fig 6: Application of RF based TEA algorithm for on line monitoring.

- A security key value is permanently stored in the encrypted device (Tag)

- All the encrypteddata from various tags are received by the RFID reader when the tags are come into the radio frequencies.
- The RFIDreader decryptsthe data using the security key and outputs the encrypted bit stream to the local data base server.
- Then the data are send to the Authorized person via internet. The following diagram shows the information flow of RFID data for secured authentication. To test and verify functionality of the system, it is designed with the following parameters:The random number used by the reader is a 64-bit value of Ox00000028 or 40.
- The number of rounds used for all encryption and decryption procedures at the reader and the tag are fixed to Ox00000032 or 50 rounds.

6. Algorithm Design and Results

The two protocols are implemented using the hardware/software approach similar to XTEA's implementation using Raspberry and with python software (i.e. tag in hardware and reader using software). Since this is ultimately realized on a real RFID system,using python software.
A separate technique to employ this in hardware is not developed here; rather a number is chosen at random to simulate a new key generated from a reader or dB server.
Secondly, for simplicity, it is also assumed that the reader performs functions of the back -end database.
By encrypting the inputs are two32-bit data values, and the last 32 bits are padding zero because, the RFID EPC code is 96 bits .The key is denoted as a four 32-bit hexadecimal values. A 128-bit key generator is created using a key value. The following comparison shows the throughput analysis of RFID – XTEA algorithm with security algorithms.

Table2: Inspection of RFID parameters in various aspects with security algorithm.

RFID data inputs	16 Rounds		32 Rounds		64 Rounds	
	Encrypt time (s)	Decrypt Time (s)	Encrypt time (s)	Decrypt Time (s)	Encrypt time (s)	Decrypt Time (s)
64	9.10	6.89	0.00010	8.9	0.00015	0.00014
96	0.00013	0.00010	0.00018	0.00016	0.00083	0.00025
128	0.00018	0.00017	0.00023	0.00021	0.00036	0.00035

The fixed latency of XTEA circuit is 128 for a single block of 64 bit data while performing encryption and decryption. Whereas the placement and routing process gives clock period of 7ns. As mentioned in [5], irrespective of RSA, AES and DES algorithms, the present work show lesser time for encryption and decryption process with 64 bits of RFID data input. The variation time is depends on the buffer size not the file size. So in this methodology the following table3 shows 2 the encryption time and decryption time of various RFID data input like 64, 96 and 128 bits with different value of Delta.

Table3: Execution time for RF –XTEA Encryption and decryption time

S.N O	Factors Analyzed	DES	3-DES	AES	TEA	Blowfish	RF - XTEA	RSA
1	Developed year	1977	1977	1978	1988	1993	1997	2000
2	Key size (bits)	64	112,168	64	128	32-448	128	>1024
3	Type of algorithm	symmetric	symmetric	symmetric	symmetric	symmetric	symmetric	Asymmetric
4	Simulation speed	Low	Low	>DES speed	Very fast (small data)	fast (small data)	Very fast (small data)	Fast
5	Scalability	yes	yes	no	yes	yes	yes	No
6	Suitable input data	Text, Image	Text, Image	Text, Image	Text	Text	Text	Image
7	Input block size	64	128	128	64	64	64	64
8.	Encryption ratio	Low	Low	High	>DES<RSA	>DES<RSA	>DES<RSA	High
9.	Power consumption	Low	Low	Low	< DES	< DES	< DES and RSA	High
10	Encrypt & Decrypt time	Increased	Increased	Increased	Decreased	Increased	Decreased	Decreased

Fig7: Encryption and decryption time of RF based TEA algorithm using python software.

The study in [6] proves that AES is faster andmore efficient than others. Hirani showed in hisexperiment that the power saving could be done by reducing number of rounds but reducing the number of roundsleads to security attacks. That kind of algorithm prone to cryptanalysis. So increasing rounds like 256, 512 and 1024 makes time consuming for AES. Even 10 and 16 rounds can beconsidered fairly andsecure the RFID data with less power.

7. Graph and Results

In general, the XTEA circuit exhibited a fixed latency of 128 clock cycles when performing encryption or decryption operated on single block of 64-bit data. In addition, the placement and routing processes provided an achievable clock period of 7 ns. But in proposed algorithm, the python software execute the various RFID data input with 32 rounds with minimum encryption and decryption time like 0.0004 and 0.00512 respectively as shown below.

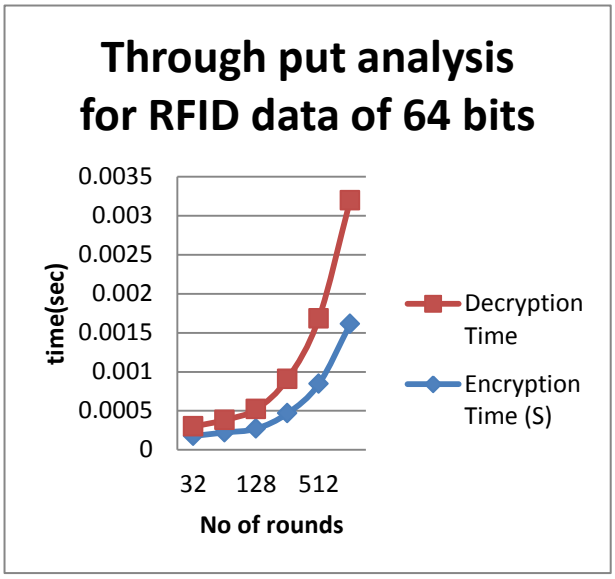

Fig 8: Encryption and decryption time of RF data for 64 input

The input of RFID data is 64, 96 and 128bits. The 128 bits are used for UHF frequency with EPC HF class 1 generation But the 96 bits is used for low frequency and high frequency like 930 MHz and 125 kHz.

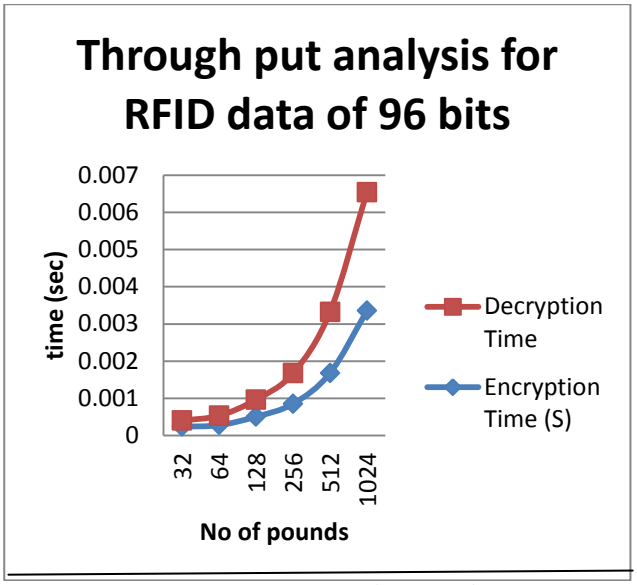

Fig9: Encryption and decryption time of RF data for 96 as an input

In AES algorithm the file size is 128,192 and 256 bit as divided into number of blocks as 32 bits. Then the input bits are shuffled by n –n number of rounds for increasing the complexity. When the input file size is 325bits then the round is 32.

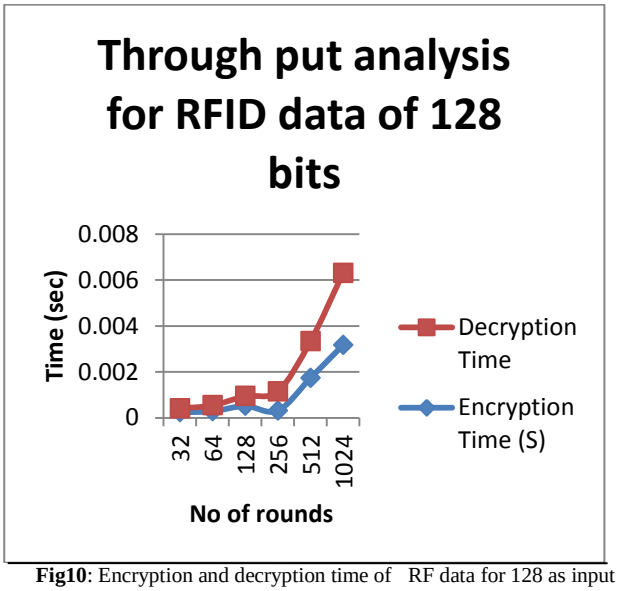

Fig10: Encryption and decryption time of RF data for 128 as input

8. Conclusion

As of today, the most popular/familiar authentication technique used over the world is the password based method which is considered/termed as a weak authentication technique. To overcome the above drawback we moved to multi factor authentication techniques i.e. using an RFID token. The feasibility of the Multi Factor Authentication depends on many factors like cost of building, maintenance of the hardware and Complexities of time. Currently the world is under the threats of cyber-attacks. Therefore a better secure and less time-complex authentication technique is required.In our Study, We proposed that the XTEA algorithm would reduce the time complexity when compared with protocols like AES, RSA and DES. A new protection scheme/ application of the data-on-tag concept has been explored in our study.

Yet this approach always depends on the RFID technology which is being used. In the proposed technology, EPC number of each RFID token is unique and it is considered for the authentication purpose. All the software is built on the python platform for execution and the results are drawn. The Throughput analysis results are obtained for the encryption and decryption times with respect to No of rounds used in the technique. Therefore, with the proposed algorithm, the minimal encryption and decryption times are achieved for small sets of RFID data.

References

[1] M. Kassim, H. Mazlan, N. Zaini, and M.K. Salleh, "Web-based student attendance system using RFID technology,"Control and System Graduate Research Colloquium (ICSGRC), 2012 IEEE , PP.213-218, 16-17 July 2012.

[2] N.M. Noman, S.M.M. Rahman, and C. Adams, "Improving security and usability of low-cost RFID tags, "Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on , PP.134-141, 19-21 July 2011

[3] A.Parvathy[#1], B. Rajasekhar[#2], C.Nithya[#3], K.Thenmozhi[#4], J.B.B. Rayappan[#5], Rengarajan Amirtharajan[#6] and Pethuru Raj RFID in the cloud environment for Attendance monitoring System.

[4] Jaeik Cho,, Setiawan Soekamtoputra, Ken Choib, Jongsub Moon ," Power dissipation and area comparison of 512-bit and 1024-bit key AES " 0898-1221, © 2012 Elsevier Ltd

[5] B. Padmavathi, S. Ranjitha Kumar **"**A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique", IJSR, India Online ISSN: 2319-7064.Volume 2 Issue 4, April 2013

[6] S.Hirani, "Energy consumption of Encryption Schemes in Wireless Devices Theses," university of Pittsburg, April 9, 2003. Retrieved October 1, 2008.

[7] Ravi Prakash, Prachi Agarwal "The New Era of Transmission and Communication Technology : Li-Fi (LightFidelity) LED & TED Based Approach", International Journal of Advanced Research in Computer Engineering Technology (IJARCET) Volume 3, Issue 2, February 2014

[8] P. Israsena, "Securing Ubiquitous and Low-Cost RFID Using Tiny Encryption Algorithm", Wireless Pervasive Computing, 2006 1st International Symposium, pp. 1-4, 2006.

[9] Juels A. RFID security and privacy: A research survey, IEEE Journal on Selected Areas in Communications, 2006, 24(2):381-394.

[10] Dimitriou T. A lightweight RFID protocol to protect against traceability and cloning attacks. The 1th International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005:59-66.

[11] XieLei, YinYaFeng, ChenXi and others. RFID data manage: algorithm, protocol and performance evaluation. Journal of computer, 2013, 36(3):457-470.

[12] Dirk Henrici and Paul M ller. Hash-based enhancement of location privacy for radio frequency identification devices using varying identifiers. IEEE international Workshop on Pervasive Computing and Communication Security, 2004:149-153.

[13] Sangshin Lee, Tomoyuki Asano and Kwangjo Kim. RFID bi direction authentication scheme based on synchronized secret. The 2006 Symposium on Cryptography and Information Security,2006:17-20.

[14] Chiu C. Tan, Bo Sheng, and Qun Li. Secure and serverless RFID authentication and search protocols. IEEE Transactions on Wireless Communications, 2008, 7(4):1400-1407.

[15] Song Han, Tharam S. Dillon, Elizabeth Chang. Anonymous bidirectional authentication protocol for RFID tag without back-end database. Mobile Sensor Networks 2007, Lecture Notes in Computer Science, 2007:623-632.

[16] K. Vijayakumar and C. Arun, "A Survey on Assessment of Risks in Cloud Migration", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.66 May 2015.

[17] K. Vijayakumar and C. Arun, "Continuous Security Assessment of Applications in Cloud Environment", International Journal of Control Theory and Applications, ISSN: 0974-5645 volume No. 9(36), Sep 2016, Page No. 533-541.