Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Securing RFID from External Attacks Using Enhanced Security Mechanism

Aastha
Assistant Professor
Department of Computer Science and applications
Maharishi Dayanand University, Rohtak, India

Preeti Gulia
M. Tech
Department of Computer Science and applications
Maharishi Dayanand University, Rohtak, India

***Abstract*:** This paper consists of RFID technology which is used in many applications but this technology consists of various security issues. There are various chances that it while using technology our database and various parts get hacked. So in order to boost this technology.AES technology which is generally used in security area. This is AES in modified way. Here introduction of additional security layer such as IP filter and OTP to boost the security of traditional Security mechanism so that our new system come in a more advanced way.

***Keywords*:** AES, RFID (Radio Frequency Identification), Fibre optics, Co-axial cable, Wireless Cable.

[I] INTRODUCTION

Electronical magnetic fields are used by RFID which can identify automatically and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from near RFID reader's interrogating radio waves. Active tags contain a local power source a battery and operate at hundreds of meters from the RFID reader.

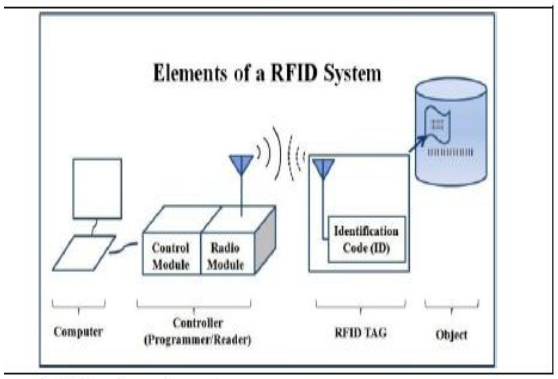

Fig 1 RFID System [6]

Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the object to be tracked. RFID is a method for AUTOMATIC Identification and Data Capture (AIDC).RFID tags can be passive, active or battery-assisted passive. An active tag covers on-board battery and periodically transmits its ID signal. A battery-assisted passive (BAP) has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader.[1][7]

[II] LITERATURE REVIEW

Elisabeth Ilie-Zudor[2] in his paper has presented an overview of the current state of the art in the radio frequency identification (RFID) technology. Aside from a brief introduction to the principles of the technology, a survey is given on major classes of RFID tags and readers, commonly used frequencies and identifier systems, current and envisaged fields of application, as well as advantages, concerns and limitations of use. Current and proposed uses of RFID span a wide spectrum of application areas and a fully comprehensive overview would certainly surpass the limits of this paper. It is, however, easy to see that the nature of a given use of RFID can be put in either one of three groups item instance or item class identification, location identification, data transfer from or to the RFID tag. His paper gave an overview of the current state and trends of RFID technology. Even though numerous limitations and unresolved issues still hinder the widespread application of RFID, it can be already seen that especially enterprises in complex supply chains will benefit from RFID, once the application difficulties are overcome.

Kamran Ahsan[3] has presented an Introductory and Exploratory Study on RFID Application. His research is part of a big project; the results of the investigations conducted on the three RFID components will be used to develop their research model. His research is based on use context based knowledge management to produce a model for mobile technology implementation within patients' movement processes. In order to do this they need to investigate RFID feasibility and integration with hospital information systems for improving healthcare. His paper explores the fundamentals of RFID technology. His study has identified and explained the nature of RFID technology evolution with respect to RFID applications. RFID technology will open new doors to make organisations, companies more secure, reliable, and accurate. The first part of this paper has explained and described the RFID technology and its components, and the second part has discussed the main considerations of RFID technology in terms of advantages and study model. The last part explores RFID technology applications. The paper considers RFID technology as a means to provide new capabilities and efficient methods for several applications.

Charles Mutigwe and Farhad [4] has presented Research Trends in RFID Technology which concludes adoption rate of Radio Frequency Identification (RFID) technology is increasing; mass-market adoption will not be achieved until a few major challenges are addressed. These challenges are: privacy, security and costs from the end-user's viewpoint

and limited power supply to the tag from the engineering perspective. We focus our attention on research in: RFID privacy and security, antennas, polymer electronics-based RFID devices, power management circuits and techniques, and efficient RF spectrum utilization. This paper has highlighted the technology's potentials, the on-going research to address the challenges, and the areas in need of more attention in terms of research.

[III] EXISTING WORK

There are always security threats from hacker and attacker to network. These are persons who affect the normal performance of network and secrecy of essential information. The usually use brute force attack, IP spoofing, Dictionary attacks in order to access information without any authentication.

Instead of this there are various types of attack which are used in order to save our data. Security threats are issues for our database and front end.[13][14]

Data Flooding:

Not every successful reading of a tag (an observation) is useful for business purposes. A large amount of data may be generated that is not useful for managing inventory or other applications. For example, a customer moving a product from one shelf to another, or a pallet load of articles that passes several readers while being moved in a warehouse, are events that do not produce data that is meaningful to an inventory control system.[7]

The attacks can be categorized on the basis of behavior of the attack i.e. Passive or Active attack.

Passive attacks: A passive attack does not change the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic.

Active attacks: Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorised access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. Active attacks are classified into four groups:

Dropping Attacks: Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes.

Modification Attacks: These attacks modify packets and disrupt the overall communication between network nodes. Sinkhole attacks are the example of modification attacks.

Fabrication Attacks: In fabrication attack, the attacker send fake message to the neighbouring nodes without receiving any related message.

[IV] PROPOSED WORK

Various papers have shown different kinds of improvement here. Theortical description as well as diagrammatical description what proposed is different from other papers described here. Introduction of the new security layer in our security system.

1. IP filters are used to reject unauthenticated transmission of packets from server to client.

2. Next step is to enhance network security by customizing existing encryption techniques.

3. Loopholes of existing security mechanisms & enhance security of network has been eliminated here.

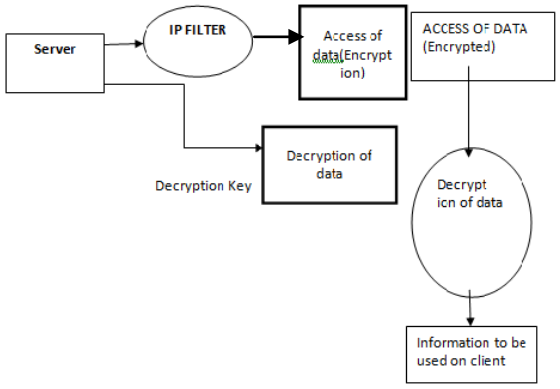

Fig 2 ***PROPOSED MODELS***

4. Socket server & corresponding client to prevent unauthentic access during data transmission has programmed

5. Use of more complex key during encryption & decryption is made.

6. A user interface to make client server communication is developed.

[V] EXPERIMENTAL FINDINGS

Here readings of packet transmission time in different cases such as fiber optic, coaxial, twisted pair cable are shown below:-

Table 1 Readings in case of Fiber optics

Sr. No	Security Level	H	L	Avg
1	Layer1(cr)	20	40	30
2	Layer2(ip)	15	30	22.5
3	Layer3(otp)	10	20	15
4	L1+L2	40	80	60
5	L1+L3	35	70	52.5
6	L2+L3	30	60	45
7	L1+L2+L3(slow_net)	55	110	82.5
8	L1+L2+L3(avg_net)	50	100	75
9	L1+L2+L3(High_net)	48	96	72
10	L1+L2(avg_net)	45	90	67.5
11	L1+L3(avg_net)	40	80	60
12	L2+L3(avg_net)	35	70	52.5

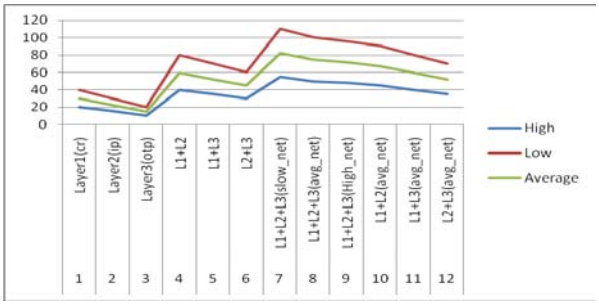

Fig 3. Graphical representation of transmission speed of packet in case of Fiber optics

Table 2 Readings in case of Coaxial Cable

Sr. No.	Security_Level	H	L	Avg
1	Layer1(cr)	25	50	37.5
2	Layer2(ip)	20	40	30
3	Layer3(otp)	15	30	22.5
4	L1+L2	45	90	67.5
5	L1+L3	40	80	60
6	L2+L3	35	70	52.5
7	L1+L2+L3(slow_ net)	60	120	90
8	L1+L2+L3(avg_n et)	55	110	82.5
9	L1+L2+L3(High_ net)	53	106	79.5
10	L1+L2(avg_net)	50	100	75
11	L1+L3(avg_net)	45	90	67.5
12	L2+L3(avg_net)	40	80	60

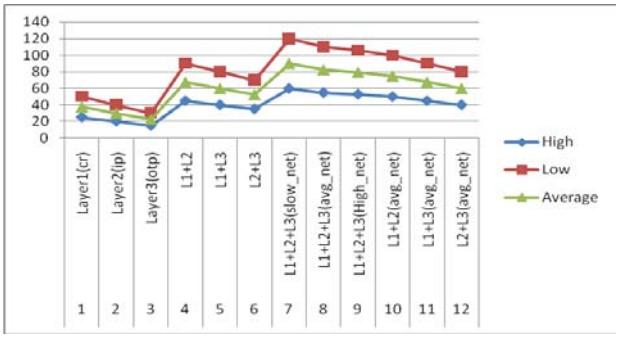

Fig 4 Graphical representation of transmission speed of packet in case of Coaxial Cable

Table 3 Readings in case of Twisted Cable

Sr. No.	Security_Level	H	L	Avg
1	Layer1(cr)	30	60	45
2	Layer2(ip)	25	50	37.5
3	Layer3(otp)	20	40	30
4	L1+L2	50	100	75
5	L1+L3	45	90	67.5
6	L2+L3	40	80	60
7	L1+L2+L3(slow_net)	65	130	97.5
8	L1+L2+L3(avg_net)	60	120	90
9	L1+L2+L3(High_net)	58	116	87
10	L1+L2(avg_net)	55	110	82.5
11	L1+L3(avg_net)	50	100	75
12	L2+L3(avg_net)	45	90	67.5

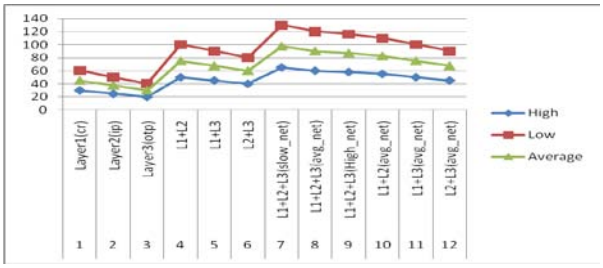

Fig 5 Graphical representation of transmission speed of packet in case of Twisted Cable

Table 4 Readings in case of Wireless Network

Sr. No.	Security_Level	H	L	Avg
1	Layer1(cr)	35	70	52.5
2	Layer2(ip)	30	60	45
3	Layer3(otp)	25	50	37.5
4	L1+L2	55	110	82.5
5	L1+L3	50	100	75
6	L2+L3	45	90	67.5
7	L1+L2+L3(slow_net)	70	140	105
8	L1+L2+L3(avg_net)	65	130	97.5
9	L1+L2+L3(High_net)	63	126	94.5
10	L1+L2(avg_net)	60	120	90
11	L1+L3(avg_net)	60	120	90
12	L2+L3(avg_net)	50	100	75

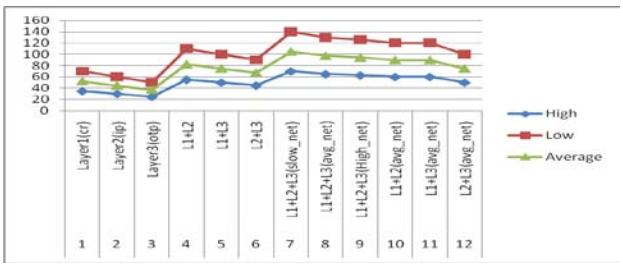

Fig 6 Graphical Representation of transmission speed of packet in case of Wireless network

[VI] CONCLUSION

Here, confab of various readings in various kinds of conditions. Tables have shown readings in three types of cases. On the basis of this analysis conclusion is speed of transmission of speed in case of wireless network, Fibre optics, and Coaxial cable.

A substantial benefit of RFID devices over the stated is that the RFID device does not demand to be found exactly relative to the scanner. We're all require with the difficulty that store checkout clerks sometimes have in making sure that a barcode can be read. And obviously, credit cards and ATM cards must be swiped through a special reader.

In contrast, RFID devices will work within a few feet (up to 20 feet for high-frequency devices) of the scanner. For example, you could just put all of your foodstuffs or purchases in a basket, and set the bag on the scanner. It would be able to query all of the RFID devices and total your purchase immediately.[10][11][12]

RFID technology has been obtainable for more than fifty years. It has only been recently that the ability to manufacture the RFID devices has fallen to the point where they can be used as a "throwaway" inventory or control device. Alien Technologies recently sold 500 million RFID tags to Gillette at a cost of about ten cents per tag.

One reason that it has taken so long for RFID to come into common use is the lack of standards in the industry. Most companies invested in RFID technology only use the tags to track items within their control; many of the benefits of RFID come when items are tracked from company to company or from country to country.

[VII] REFERENCES

1. "RFID Technical Basics." Available from <http://www.aimuk.org/pdfs/Comp04-4.pdf > [10 August 2007] "Silicon on Sapphire CMOS for Optoelectronic Microsystems." By Andreou, A.G., Kalayjian, Z.K., Apsel, A., Pouliquen, P.O., Athale, R.A., Simonis, G., and Reedy, R.in 2001 IEEE Circuits and Systems Magazine 1, (3)

2. "THE RFID TECHNOLOGY AND ITS CURRENT APPLICATIONS" In proceedings of The Modern Information Technology in the Innovation Processes of the Industrial Enterprises-MITIP 2006, ISBN 963 86586 5 7, pp.29-36.

3. "RFID Applications: An Introductory and Exploratory Study" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 1, No. 3, January 2010 By Kamran Ahsan, Hanifa Shah and Paul Kingston.

4. "Research Trends in RFID Technology" by Charles Mutigwe and Farhad Aghdasi.

5. "The history of RFID", by J.Landt IEEE Potentials, Vol.24, No.4, pp. 8-11, in 2005.

6. "Inventory Management Using Passive RFID Tags: A Survey."BY Abraham, C., Ahuja, V., Ghosh, A.K., and Pakanati, P. (n.d.) from <http://www.cs.rutgers.edu/~badri/553dir/papers/MCPaperFinal-coldetect.pdf

7. "An Elliptic Curve Processor Suitable For RFID-Tags." BY. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., and Verbauwhede, I. Cryptology ePrint Archive in 2006 [online] Report 2006/227. Available from<http://eprint.iacr.org/2006/227.pdf> [10 August 2007]

8. Baude, P.F., Ender, D.A., Kelley, T.W., Haase, M.A., Muyres, D.V., and Theiss, in 2006 S.D.2003)"Organic Semiconductor RFID Transponders." IEEE International ElectronDevices Meeting Technical Digest [online] available from <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1269238> [10 August 2007]

9. "RFID-facilitate Construction materials management (RFID-CMM) - a case study of water-supply project", BY Z. Ren, C. J. Anumba, J. Tah Advanced Engineering Informatics, Vol.25, No.2, pp. 198-207, 2011.

10. "Scenarios for applying RFID technology in construction project management", BY W. Lu, G. Huang, H. Li, Automation in Construction, Vol.20, No.2, pp. 101-106, in 2011.

11. "Information lifecycle management with RFID for material control on construction sites", BY J. Lee, J. Song, K. Oh, N. Gu Advanced Engineering Informatics, sVol.27, No.1, pp. 108-119, 2013.

12 "Radio-frequency identification (RFID) applications: a brief introduction" BY K. Domdouzis, B. Kumar, C. Anumba, Advanced Engineering Informatics in 2007.

13. "Security and Privacy in large-scale RFID system: challenges and solutions" by D. henrici (PhD dissertation), University of Kaiserslautern, in 2009

14. Avoine, G. (2007) "Bibliography on Security and Privacy in RFID Systems." By Avoine, G. (2007) available from <http://lasecwww.epfl.ch/~gavoine/download/bib/bibliographyrfid. pdf> [10 August 2007]