# A Survey paper on RFID Technology, its Applications and Classification of Security/Privacy Attacks and Solutions

Ms.Neha Kamdar, Assistant Professor
Dept of Computer Science, MIST
Indore, India

Vinita Sharma, Assistant Professor
Dept of Computer Science, MIST
Indore, India

Sudhanshu Nayak, Assistant Professor
Dept of Computer Science, MIST
Indore, India

*Abstract*— **RFID (Radio Frequency Identification) system is one of the most pervasive computing technologies with technical potential and cost-effective opportunity in a different area of applications. Among their advantages is included their low price and their wide area applicability. However, they also present a number of inherent vulnerabilities. This paper describe a categorization of RFID attacks, present their significant features, and discussing feasible countermeasures. The purpose of the paper is to classify the existing weaknesses of RFID communication so that a better understanding of RFID attacks can be achieved and consequently more efficient and valuable algorithms, techniques and procedures to combat these attacks may be developed.**

***Keyword: RFID Security, RFID Attacks, Classification***

## I. INTRODUCTION

Radio-Frequency Identification (RFID) devices have a significant existence in our daily life, still when we do not observe them, and they will become ubiquitous in the next to future. The fabulous market push of RFID technology is suitable to the attention by large retailers (e.g. Wal-Mart 1), Imperative manufacturers (e.g. Gillette, Procter & Gamble, etc.) and governments. As an outcome, approximately each object is legally responsible to carry an RFID tag. RFID devices can be seen as an appropriate alternate of bar codes since they are mostly used to recognize objects. Unlike bar codes, RFID devices permit objects to be recognized with no visual contact and help in improving and automating a lot of processes e.g. supermarket checkouts, product inventories, etc.

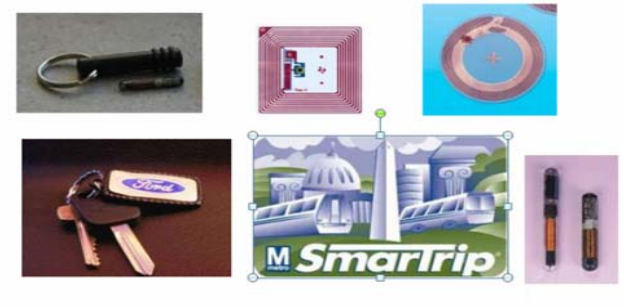


Figure 1: Types of RFID system

### *A. What is RFID?*

An RFID system is combination of tags, readers, communication protocols, computer networks, and databases. A typical RFID system is standardized by EPCglobal is shown in Figure 1. The tag is a little chip containing product information through an affixed radio antenna. The tag is attached to an item or its packaging and contains a unique serial number called an electronic product code (EPC). The EPC is use to exclusively recognize the pallet, case, or thing. For low-priced tags, a reader transmits A radio signal to the tags to invigorate them so that the tag can transmit its EPC. A reader can be both stationary in a rigid state and handheld. There are communication protocols that define the swap over of messages from the tag to reader and reader to tag. The readers are connected to a computer network so that they can be queried by a management system. Later than that the management organization can inquiry a database determined by the EPC to find out more information concerning the item to which the tag is attached.

*B. Basic operation of RFID system*

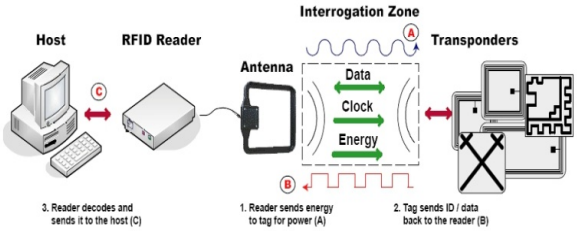


Figure 2: RFID system

An RFID system consists of three main components:–

1) *RFID tags:* They are miniature reactive devices with a mixture of possible appearances from stickers to little grains embedded in official credentials. A tag basically consists of a microchip and a metal coil, which acts as an antenna. In some cases, it can contain a battery with a few other microchips intended for raising its computational power. Tags contain information with a reader query the tag for the information. A tag is occasionally called a transponder. The word transponder comes from the words transmitter and responder. The tag responds to a reader's request by transmitting the information. The tag consists of a microchip linked to an antenna and sometimes a battery. A tag with a battery is identified as an active tag and a tag without a battery is recognized as a passive tag. Active tags produce energy from its battery and passive tags accept energy from the reader that generates a radio frequency (RF) field [1].

2) RFID readers: RFID readers are active devices use to study the information stored within the tags. In a nutshell, readers emit a radio wave so that every tag in their range replies by broadcasting their embedded information (i.e. a set of bits). This information, generally identified as Electronic Product Code (EPC), is generally the identifier of the object into which the tags are stuck. RFID Readers is a device designed to recognize the tag connected to database containing information concerning tag and tagged item.

3) Data processing device: The information is aggregated by these devices from numerous tags and processes data. These devices provide a database of information regarding items recognized by tags and is positioned among readers and enterprise applications. It can give a variety of computational functions on behalf of applications [7].

*C. RFID applications*

1) *Asset tracking*
2) *Barcode replacement*
3) *RFID passports*
4) Mobile credit card payment systems
5) Transportation payment systems
6) Sporting events (timing / tracing)
7) Animal identification

## II. RFID TAGS

A tag includes a microchip and a transponder. The microchip stores data interrelated to the object and the transponder transmits that data to readers. Tags are primarily programmed (data is written to the tags) at the point of manufacture (factory programming), other than also be programmed by an OEM or end user (field programming). Tag data typically include an exclusive identifier code and sometimes extra information, depending on the application and the quantity of memory on a tag. Tags are activated when they enter the range of a reader's signal. The reader's antenna sends power to the transponder, activating the data stream. Tags may be printed on paper or plastic and attached to an object, or they can be embedded under the skin of animals and humans

*A. Types of RFID Tags*

Basically RFID Tags are broadly classified in two types-

1) General types of RFID tags

There are three general types of RFID tags, active, semi active and passive RFID tags.

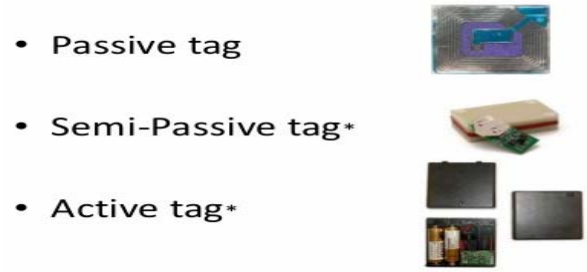


Figure 3: Possible RFID Attacks

*a) Active tags:* - This kind of RFID tag contain an interior battery which is used to allow the tag perform more complex operations, such as monitor temperature, as well as improve the communication by an RFID reader. The communication range of an active tag is capable of over 100 meters. An

active tag is the very powerful type of RFID tag, and is also the most costly

*b) Semi-active tags:*-This form of tag is also contains an internal battery, other than an active tag, the battery is just used for the tag's internal operations, and not for communication. A semi-active RFID tag relies on RFID reader to provide the essential power for communication. Note that semi-active tags are occasionally identified as semi-passive tags.

*c) Passive tags:* - This category of RFID tag contains the lowest price, and obviously, are the mainly common form of RFID tags. Passive tags have no internal batteries, and rely on the RFID reader to provide the power desired to execute all tag operations and communication. [8]

*2)* RFID Tags Based off radio frequency:

*a) Low frequency tags (125-134 KHz)*

*b) High frequency tags (13.56 MHz)*

*c) UHF tags (868-956 MHz)*

*d) Microwave tags (2.45 GHz)*

## II. RFID ATTACKS

Due to moderately plain on-tag circuits and wireless communication environment, RFID system have plentiful vulnerabilities the aim of these attacks can be- Tag, reader, communication protocol, middleware, or the database. Attacks are feasible events that reason a system to respond in an unexpected or dangerous way. The major step in building a secure system is to distinguish the Attacks. There are various types of attacks occurs in RFID but we classify some them here. [9]

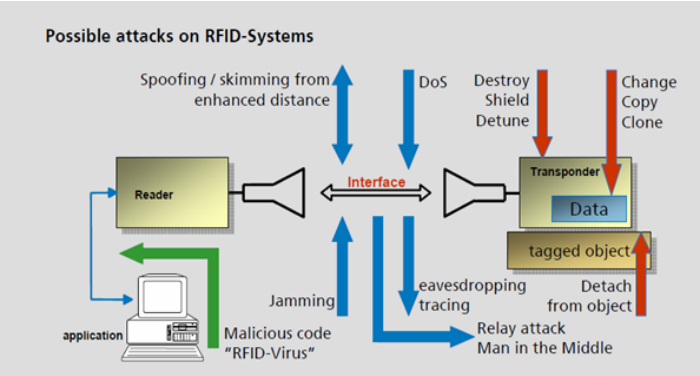


Figure 4: Possible RFID Attacks

*A. According to Network Security types of attack on RFID System*

*1) Passive attack*- within this attack an opponent deploys a sniffer tool and waits for sensitive information to be captured. This information can be used for new types of attacks. It include packet sniffer tools, traffic analysis software, filtering plain text passwords from unencrypted traffic and seeking authentication information from vulnerable communication. Formerly an enemy found any sensitive or authentication information, he will use that devoid of the knowledge of the user.

*a) Release of message contents*- A telephonic chat, an electronic mail message or a transfer file may include secret data. A passive attack probably will monitor the stuffing of these transmissions. To recognize Release of message contents, imaging that user A sends some sequence of messages to user B, one more user C is listening to the link, and therefore gets a replica of all the messages from A and B, the confidentiality of message is not maintained, such an attack is one of the passive attack. Possible solution of these attacks is encryption

*b) Traffic analysis*- here this attack the eavesdropper analyzes the traffic, determines the location, identify communicating hosts, and observes the frequency and span of message being exchanged. By the entire information they predict the nature of communication. The entire incoming and outgoing traffic of network is analyzed except not changed.

Passive attacks are extremely complex to detect because they do not occupy any modification of the data. When the messages are exchanged neither the sender nor the receiver is ***responsive*** that a third party has examine the messages. This can be prevented by encryption of data. [10]

*2) Active Attack*- In this attack an opponent doesn't wait for any sensitive or authentication info. He actively tries to separate or avoid the protected systems. It includes viruses, worms, Trojan horses, stealing login information, inserting malicious code and penetrating network backbone. Active attacks are the most unsafe in natures. Its result is in disclosing sensitive information, modification of records or complete data lost. Generally probability of Passive attacks rate is lesser then Active attacks, some of active attacks are-[11]

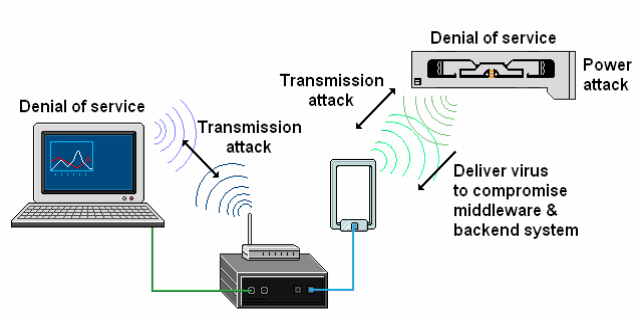


Figure 5: Attack points

*a) Insider Attack*- According to a study more than 70% attacks are insider. Insider attacks are classified in two categories; intentionally and accidentally. When an attacker intentionally harms network infrastructure or data these type of attack called an intentionally attack. Generally intentionally attacks are done by disgruntled or irritated employees for money or revenge. Damages are through by the lack of care or lack of knowledge in accidentally attack.

b) *Masquerade Attack*-An attack that uses a forged identity, such as a network identity, to get unofficial right of entry to personal computer information through legal access identification.

c) *Reply Attack*- an attacker intercepts contact among a reader and a tag to capture a valid RFID signal. When the attacker receives a query from the reader, the recorded signal is re-played into the system. So the data appears valid, it will be accepted by the system. Countermeasures the most trendy solution is the use of a challenge and response mechanism to prevent replay attacks.

d) *Offline Password Attack*- This attack is performed from a location other than the genuine computer where the passwords reside or were used. Offline attacks require physical access to the computer which stores password file, the attacker copies the password file and after that try to crack passwords in his own system. There are no locks or anything else to stop you on an offline attack unlike an online attack, because you are doing it on your own machines. Offline attacks comprise dictionary attacks, hybrid attacks, brute force attack, pre computed hash attacks, syllable attacks, and rule based attacks and rainbow attacks.

e) *Denial of Service attack*- A series of attacks is understood as Denial of Service attack. These attacks are ready to acquire completely different forms by offensive the RFID tag, the network, or the backend. The aim isn't to steal or amendment data, however to disable the RFID system so it can't be used. a distinct variety of DoS is to destroy or hinder RFID tags by removing them from the things, laundry out their contents entirely, or covering them with metal foil.

f) *Spoofing attack*- Spoofing attacks Offer false info typically, spoofing attacks involve fake name, net Protocol (IP) address, or Media Access Code (MAC). Imitating the behavior of a genuine tag.

*B. According to Network Security types of Attack on RFID tags*

Most common types of attack on RFID tags: unauthorized disabling, unauthorized cloning, unauthorized tracking, and response replay

*a) Unauthorized disabling*-These square measure Denial-of-Service (DoS) attacks in which an attacker causes RFID tags to assume a state from which they they will now not operate properly. This results in the tags becoming either temporarily or permanently incapacitated. Such attacks usually exacerbated by the mobile nature of the tags, permitting them to be manipulated at a distance by covert readers.

*b )Unauthorized tag cloning*- These are integrity attacks in which an attacker succeeds in capturing a tag's identifying information. These attacks are exacerbated by the fact that the tags can be manipulated by rogue readers. The ability to create duplicates of tags can be used as a means to overcome fake protection (e.g., in passports and drug labels) and as a foundation step in a (large-scale) theft scheme. It exposes corporations to new vulnerabilities if RFIDs are used to computerize verification steps to streamline security procedures.

*c) Unauthorized tag tracking*- These are privacy attacks within the attacker know how to trace tags throughout rogue readers. We categorize these attacks from "Big Brother" concern that cooperate entities managing the back-end server might control RFID capabilities to infringe on the privacy of consumers. A detailed analysis of consumer privacy issues is given in, addressing policies, standards, and checks to protect consumer interests. In this paper we concentrate in its place on the prospect of rogue readers, controlled by hackers or adversarial organizations, being used to monitor tags. This issue is difficult to address, since hackers cannot be presumed to adhere to policies or standards, or to follow specified protocols.

## IV. SOME PROPOSED SECURITY SOLUTION

There are various types of attacks occurred in RFID systems. Here we described some of proposed algorithms and methods of detection and prevention of RFID attacks. As we discussed about passive and active attacks which above mentioned, the passive attack can be eliminated by implementing good network encryption technologies. And Active attacks can be prevented by using Firewalls techniques and IPS (Intrusion Prevention Systems).

*A.* Some researcher proposed algorithms and methods for RFID securities using Hash algorithm .Hash algorithm is the most secure authentication algorithm in network security. In RFID, Hash algorithm provide authentication between Tag and Reader. [2]

*B.* There is another authentication techniques has been implemented in RFID which is a new algorithm based on smart cards. The idea behind this algorithm in which data send through the tags can be made secure using the Et Al's algorithm so that the un-authorized users can not access the data without any unique identification numbers. [3]

*C.* Martin Feldhofer et.al has been worked on security issues of RFID systems. They are implemented a authentication protocol which act as a proof of concept for authenticating an RFID tag to a reader using the Advanced Encryption Standard (AES) as cryptographic primitive. The major work is a novel approach of an AES hardware implementation which encrypts a 128-bit block of data. [4]

*D.* Axel Poschmann et.al has been worked on prevention of linear and differential cryptanalysis, and the Davies-Murphy-attack. A latest block cipher, DESL (DES Lightweight extension), which is strong, compact and capable. Due to its low area constraints DESL is mostly appropriate for RFID (Radio Frequency Identification) devices. DESL is based on the Data Encryption Standard cryptography technique, however, unlike DES it uses a single S-box repeated eight times. This approach makes it possible to significantly decrease chip size requirements. The S-box has been highly optimized in such a way that DESL resist general attacks, i.e., linear and differential cryptanalysis, and the Davies-Murphy-attack. [5]

*E.* In this research paper, we have discussed a "hybrid approach" that merges two separate broader areas unethical hacking and network security. It also tell how black hat hacker applies unethical hacking to steal information in online and offline mode and also provide prevention during online mode by using the concept of NAC. [6]

## V. CONCLUSION

In this paper we've got delineate the summary of RFID technology, their applications and a few potential attacks that is feasible in RFID. For preventing these attacks here during this paper we've got delineate a number of Security solutions relating to these attacks. But there square measures several potential attacks except we've got delineate, square measure potential in RFID systems. In future, for bar of those attacks totally different Security solutions and new technologies are going to be planned.

## REFERENCES

[1] J.Aragones-Vilella et.al"A Brief Survey on RFID Privacy and Security", Proceedings of the World Congress on Engineering 2007 Vol II, WCE 2007, July 2 - 4, 2007, London, U.K

[2] Xiao Nie, Xiong Zhong"Security in the Internet of Things Based on RFID: Issues and Current Countermeasures" in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)

[3] Jitendra Kumar Gupta & K. K. Mishra"Efficient Authentication in RFID Devices Using Et Al's Algorithm" on Global Journal of Computer Science and Technology Network, Web & Security, Volume 12, Issue 16, Version 1.0 ,Year 2012

[4] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer" D.VAM.11 Suggested Algorithms for Light-Weight Cryptography n supported by the Commission of the European Communities through the IST program under contract IST-2002-507932.

[5] Axel Poschmann, Gregor Leander, and Kai Schra "New Light-Weight Crypto Algorithms for RFID" Conference: Circuits and Systems, 2007. ISCAS 2007. IEEE International Symposium.

[6] Jatinder Teji, Rimmy Chuchra, Sonam mahajan, Manpreet Kaur Gill, Manju Dandi "Detection and Prevention of Passive Attacks in Network Security" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013.

[7] Agusti Solanas and Jesus Manj "RFID Readers Deployment for Scalable Identification of Private Tags" P. Kitsos, Y. Zhang (eds.) RFID Security: Techniques, Protocols 289 and System-on-Chip Design, Springer Science Business Media, LLC 2008.

[8] Kapil Singh "Security in RFID Networks and Protocols", International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 5 (2013), pp. 425-432, International Research Publications House.

[9] Dale R. Thompson, Jia Di, Harshitha Sunkara, and Craig Thompson "Categorizing RFID Privacy Threats with STRIDE".

[10] http://www.idconline.com/technical_references/pdfs/data_communications/Security_attacks.pdf

[11] http://computernetworkingnotes.com/ccna-study-guide/network-security-threat-and-solutions.html