RESEARCH ARTICLE OPEN ACCESS

Study on RFID, Architecture, Service and Privacy with Limitation

Tanuja Dahariya[1], Ankit Naik[2], Menaka Chandra[3]
Research Scholar[1&3], Lecturer[2]
Department of Computer Science and Engineering
Kirodimal Institute of Technology
Raigarh
Chhattisgarh – India

ABSTRACT
This paper gives an overview of the radio frequency identification (RFID) technology. In this paper study of RFID technology, architecture, current security and privacy, as well as limitation or advantages are discussed here. The RFID technology is already of high commercial relevance. It breaks into new application areas, and new markets are emerging. RFID technology facilitates automatic wireless identification using electronic passive and active tags.
Keywords:- RFID, Architecture, Service

I. INTRODUCTION

The Radio Frequency Identification (RFID) is an automatic identification system. RFID uses RF to identify "tagged" items. This data is then collected and transmitted to a host system using an RF Reader. The RFID technology is already of high commercial relevance. It breaks into new application areas, and new markets are emerging. Today's RFID system architecture is carried over from the architecture used in other auto-id systems, chiefly optical barcode systems. As RFID introduces new functionalities and privacy risks, this classic architecture is no longer appropriate.

RFID is a non-contact automatic Identification technology, it through Rf signal automatic target recognition to access relevant data. Identifying work without human intervention, and it can work in all kinds of bad environmental conditions. RFID technology can identify the moving objects and identify multiple tags, the operation is fast and convenient. RFID technology basic working principle is the label into the magnetic field, and then receiving a RF signal from reader, with inductive current energy for sending the information which is stored in charge of the product. （Passive Tag, Passive tags or passive tags), or sending a frequency tags with initiative of the signal （Active Tag, Active tags or active tags).

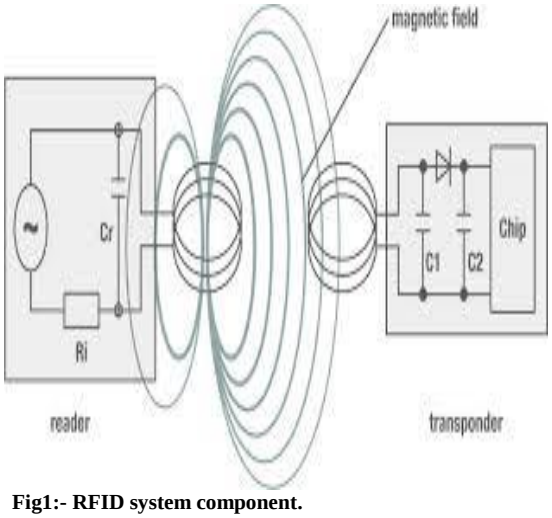

Fig1:- RFID system component.

II. RFID COMPONENTS

Modern RFID system has three major components.

- Tag –Transponder
- Reader –Transceiver
- Backend Database

Fig2:-RFID System Component

Tags

Tags are typically composed of a microchip for storage and computation, and a coupling element, such as an antenna coil for communication. Tags may also contain a contact pad. Tag memory may be read-only, write-once read-many or fully rewritable.

Broadly the tags have been classified in three categories:-

- Active Tag: An active RFID tag is equipped with a power source for the tag's circuitry and antenna. The advantages of an active RFID tag includes readability from a distances of one hundred feet or more as well as capability to have other sensors that can use electricity for power.

- Passive Tag: Passive RFID tag does not contain a power source; the power is supplied by the reader. The tag draws power from the inductive coupling with reader antenna. The major disadvantages of a passive tag are that the tag can be read only at very short distances, typically a few feet at most. However there are many advantages .The tag functions without a battery which increases the life time to more then 20 years. The tags are less expensive (10¢) and much smaller.. These tags have almost unlimited applications in consumer goods and other areas.

- Semi-Passive Tag: Like passive tags, semi-passive tags reflect (rather than transmit) RF energy back to the tag reader to send identification information. However, these tags also contain a battery that powers their ICs. This allows for some interesting applications, such as when a sensor is included in the tag so it can transmit real-time attributes, such as temperature, humidity, and timestamp. By using the battery only to power a simple IC and sensor and not including a transmitter the semi-passive tags achieves a compromise between cost, size, and range.

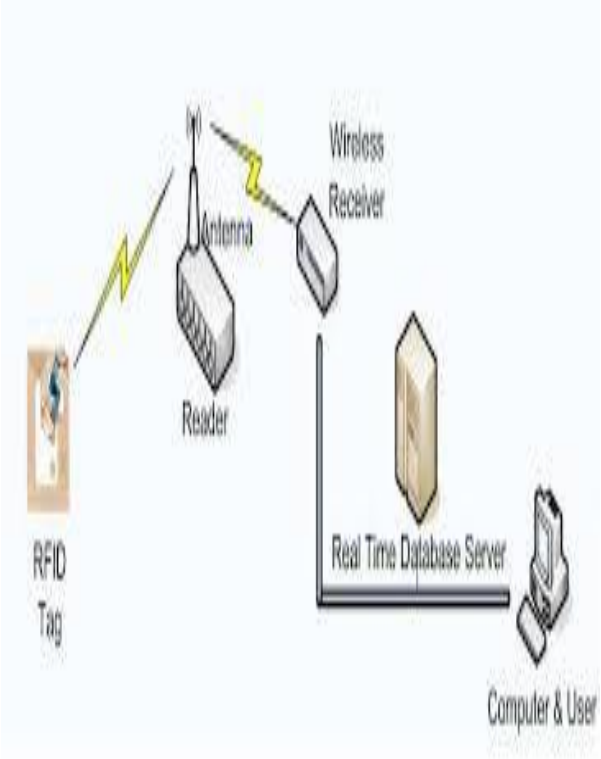

Fig3:-RFID Tags

Reader:

An RFID reader is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data. A number of factors can affect the distance at which a tag can be read (the read range). The frequency used for identification, the antenna gain, the orientation and polarization of the reader antenna and the transponder antenna, as well as the placement of the tag on the object to be identified will all have

an impact on the RFID system's read range. The RFID reader provides the connectivity between individual tags and the tracking/management system. Depending on the application and operating conditions, there may be a multiplicity of readers to fully service a specific area.

Overall, the reader provides three main functions
• Bidirectional communication with the tags.
• Initial processing of received information.
• Connection to the server that links the information into the enterprise.

Backend Database

Often, the RFID reader contains a networking element such as wired Ethernet or wireless Ethernet that connects a single RFID-read event to a central server. The central server runs a database application, with functions that include matching, tracking, and storage. In many applications, an "alert" function is also present (for example the re-order trigger, for supply chain and inventory management systems, or an alert to a guard, for security applications).

III. WORKING OF RFID

Radio-frequency identification (RFID) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by electromagnetic induction from magnetic fields produced near the reader. Some types collect energy from the interrogating radio waves and act as a passive transponder. Other types have a local power source such as a battery and may operate at hundreds of meters from the reader.

Since RFID tags can be attached to cash, clothing, possessions, or even implanted within people, the possibility of reading personally-linked information without consent has raised serious privacy concerns.

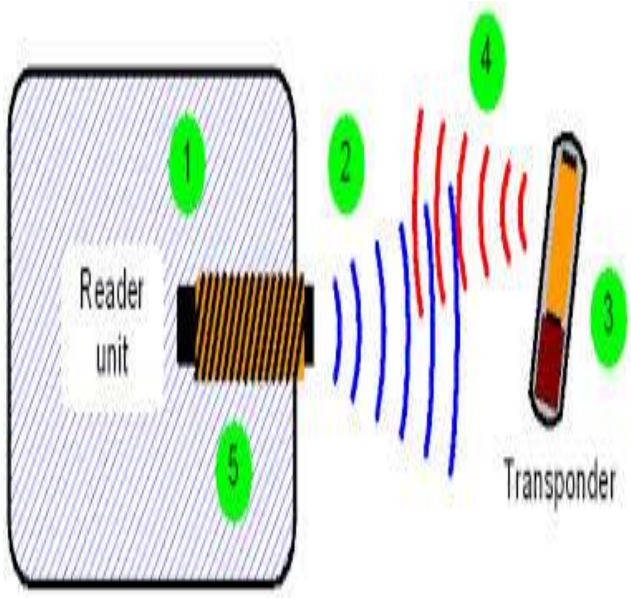

Fig 4: Working of RFID

Architecture of RFID

Before RFID can be understood completely, it is essential to understand how Radio Frequency communication occurs. By generating a specific electromagnetic wave at the source, its effect can be noticed at the receiver far from the source, which then identifies it and thus the information. An RFID tag is composed of an antenna, a wireless transducer and an encapsulating material. An RFID reader consists of an antenna, transceiver and decoder, which sends periodic signals to inquire about any tag in vicinity.

RFID systems can also be differentiated based on the frequency range it uses. The common ranges are Low-Frequency (LF: 125 - 134.2 kHz and 140 - 148.5 kHz), High-Frequency (HF: 13.56 MHz) and Ultra-High-Frequency (UHF: 868 MHz - 928 MHz).It shows that the architecture is based on the one known from other kinds of auto-id systems, like optical barcode systems. Barcodes provide product information via bars with different width and space between them. To read the information for a given product, the barcode of the product is captured using a barcode reader, sometimes also called "scanner". In the example, the reader is directly connected to the cash register.

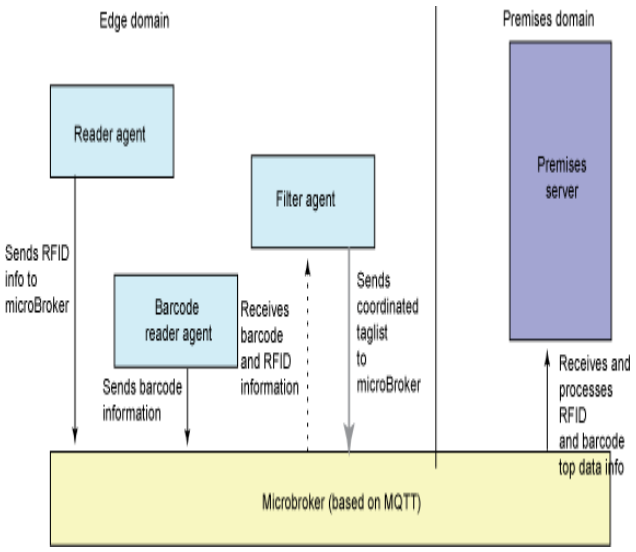

Fig 5: System barcode architecture

IV. SECURITY AND PRIVACY

Security Risk assessment:

1.) Counterfeit RFID Tag Attacks **:** RFID Tags are devices prone to several modes of physical attack, to include counterfeiting attacks which seek to duplicate legitimate tags through cloning or forgery. By virtue of its inexpensive functionality, the low cost RFID Tag contains an unencrypted identifier that can be stolen for duplication efforts. The RFID Tags in a deployment are usually manufactured in manner such that the information that provides a tag with its unique value is a predictable number amidst a series of numbers.

2). Replay Attacks: The successful creation of counterfeit tags can inflict damage to the integrity of system data. An attacker can perform replay attacks with counterfeit tags, mimicking the valid arrival and Departure of tags. Replay attacks on a grand level can ultimately lead to a Denial of Service (DoS) attack in which counterfeit tags are replayed to readers in excess form

3.) Eavesdropping Attacks:- Lightweight RFID Tags do not have the resources required to communicate with RFID Readers through encrypted channels. Electronic access to tag contents occurs via eavesdropping by attackers in possession of rogue readers.

Privacy Risk Assessment:

RFID privacy issues fall into two broad categories: data privacy and location privacy. Data privacy involves control over personal information contained on the tag and in associated database(s). Location privacy involves control over the information regarding the individual's physical location and movement. Security controls that protect data privacy may not address location privacy and vice versa. This section of the report addresses RFID-related privacy issues as they apply to US-VISIT Increment 2C. The UHF tags operating between 868 and 956 MHz can be read from distances of up to 30 feet away.

V. LIMITATION OF RFID

The RFID cannot completely replace the barcode technology due to its higher cost, the scope for accuracy, speed and the return on investment is high in RFID system. RFID technology has already been applied effectively, it has certain technological barriers that still need to be overcome to optimise its application. These lacunas are high investment, lack of security and privacy, and some related to the technology of RFID.

Cost: Although there is a great potential of RFID in the local logistics sector, the major drawback is the cost of the RFID tag, which is higher as compared to barcode system. So industrial leaders are concerned about the return on investment and net profit by investing the extra cost in the existing system. The cost depends on the volume of usage. Security and Privacy: The security and privacy of the RFID against unauthorized readers is in debate from the very beginning. There is a great challenge to the consumer privacy. The consumers using the product with RFID tags can be traced easily. The RFID tag broadcasts the ID serial number or the Electronic Product Code (EPC) to the nearby reader. There is a very high chance of privacy violations.

Technology: As the RFID is based on the concept of Radio Frequency, it can be interfered with other radio transmissions, metals, liquids, etc. The degree of interference depends upon the frequency of the tag and the usage environment.

Standardization: Though the characteristics of the application and the environment of use determine the appropriate tag, the sparsestandards still leave much freedom in the choice of communication

protocols and the format and amount of information stored in the tag. Companies transcending a closed-loop solution and wishing to share their application with others may encounter conflicts as cooperating partners need to agree in standards concerning communication protocols, signal modulation types, data transmission rates, data encoding and frames, and collision handling algorithms.

VI. CONCLUSION

This paper gave an study of Radio Frequency Identification Device (RFID) technology. The RFID technology will be an inevitable part of our everyday life in the foreseeable future. It offers various application spectrums that raise productivity, increase comfort, and open new markets and many other goods will be tagged and identified with RFID tags. Designing concepts and methods that ensure security and privacy protection for systems of global scope is one of the main research goals in the field of RFID. Moreover, a range of quality requirements like reliability, scalability, flexibility, openness, and sustainability, security and privacy etc. There are many more research challenges. Systems need to support inter-organizational business processes. Also, the integration of people carrying the RFID tags ("tag bearers") into the system is important for providing information self-determination. RFID technology basic working principle is the label into the magnetic field, and then receiving a RF signal from reader, with inductive current energy for sending the information which is stored in charge of the product.

REFRENCES

[1] RFID Introduction, Present and Future applications and Security Implications Nandita Srivastava MSEE Student George Mason University Advisor:Dr Jens-Peter Kaps

[2] en.wikipedia.org/wiki/Radio-frequency_identification. How work on RFID

[3] www.tutorialreports.com/wireless/rfid/technology.php FID Technology and Architecture.tutorial reports.com

[4] RFID System Architecture Reconsidered Dirk Henrici, Aneta Kabzeva and Paul Müller University of Kaiserslautern Germany

[5] Attachment e: rfid security and privacy white paper.https://www.dhs.gov/xlibrary/assets/foia/us-visit_rfidattache.pdf

[6] Scope & limitations of RFID. www.indiantextilejournal.com/articles/fadetails.asp?id=478

[7] RFID Technology Principles, Advantages, Limitations & Its Applications Mandeep Kaur, Manjeet Sandhu, Neeraj Mohan and Parvinder S. Sandhu International Journal of Computer and Electrical Engineering, Vol.3, No.1, February, 2011 1793-8163