ISSN:0975-9646

Secure Smart Environment Using IOT based on RFID

Jebah Jaykumar[1], Abishlin Blessy[2]

[1]*Assistant Professor, BNM Institute of Technology, Bangalore,India.*
[2]*Chennai,India.*

***Abstract*— IOT(Internet of Things) relying on exchange of information through radio frequency identification(RFID), is emerging as one of important technologies that find its use in various applications ranging from healthcare, construction, hospitality to transportation sector and many more. This paper describes about IOT, concentrating its use in improving and securing future shopping. This paper shows how RFID technology makes life easier and secure and thus helpful in the future.**

Keywords- IOT,RFID, Intelligent shopping, RFID tags, RFID reader, Radio frequency

1 INTRODUCTION

The Internet of Things (IoT) is the network of physical objects accessed through the Internet, as defined by technology analysts and visionaries. These objects contain embedded technology to interact with internal states or the external environment. In other words, when objects can sense and communicate, it changes how and where decisions are made, and who makes them. The IoT is connecting new places–such as manufacturing floors, energy grids, healthcare facilities, and transportation systems–to the Internet. When an object can represent itself digitally, it can be controlled from anywhere. This connectivity means more data, gathered from more places, with more ways to increase efficiency and improve safety and security.

Internet of Things gives objects the capacity to identify itself, perceive the surrounding data, interact with servers over the internet and make queries to change their state. These objects can be personal objects such as smart phones, digital cameras or elements in our environment.

Radio-frequency identification (RFID) is seen as prerequisite for the Internet of Things. RFID is used for sensing the objects and also for transfer of information about the object onto the network wirelessly till it reaches its destination.

The basic ideology behind the working of RFID technology is explained in section II, section III briefs on how RFID is used in implementing internet of things, the use of IOT in Smart Environment and its secure use is briefed in section IV and V respectively and section VI has conclusion with the basic summary of the advantages of using this method of authentication.

II. RFID TECHNOLOGY

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. Data stored on RFID tags can be changed, updated and locked. RFID tags can be broadly classified into 3 types: active, semi-passive and passive. Active and semi-passive RFID tags use internal batteries to power their circuits. An active tag also uses its battery to broadcast radio waves to a reader. The semi-passive tag relies on the reader to supply its power for broadcasting. Passive RFID tags rely entirely on the reader as their power source. The active and semi passive tags contain more hardware than the passive RFID tags, hence they are more expensive compared to passive tags. Therefore Active and semi-passive tags are reserved for costly items and passive tags are used for relatively cheaper items. Nevertheless , all the 3 category of tags are manufactured to be disposable, along with the disposable consumer goods on which they are placed.

These tags can be of 3 storage types

1. read-write: Data can be added or overwritten.
2. read-only: This cannot be overwritten they contain only the data that is stored in them when they were made.
3. write-once, read many(WORM): Tags can have additional data added once, but they cannot be overwritten.

The mode of communication between the reader and the tag of an RFID system is based on radio frequency (RF) technology.

A simplified RFID system is shown in Fig. 1. The tag includes the antenna within itself, which is responsible for providing communication while the reader is usually having one or two antennas. The reader which contains a trans-receiver generates a pulse of electromagnetic waves. The transponder receives the transmission which is further, rectified to get the dc power supply for the IC memory.

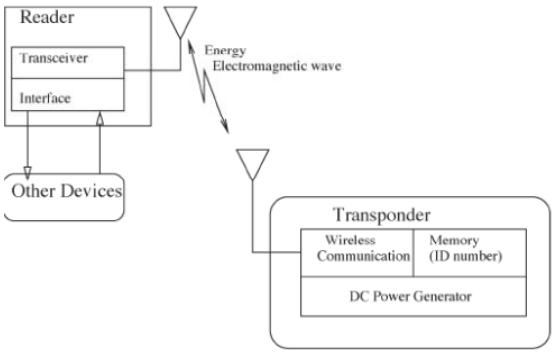

Figure 1. Simplified RFID system architecture.

The processed signal transmitted by the transponder is then received by the reader again to obtain the tag's ID number. As the RFID technology is simple, more flexible and relatively cheaper it is nowadays gaining attention in a large number of applications, such as personal identification, food production control, security guard monitoring, and inventory management.

III. STRUCTURE OF IOT BASED ON RFID

RFID is often seen as a prerequisite for the Internet of Things. The typical internet of things based on RFID is composed of three major components including RFID system, middleware system and Internet system.

a) **RFID system** consists of readers, tags and antennas. Identification of target is done with a unique Electronic Product Code (EPC) saved in RFID tag. RFID tags are wireless devices which communicate with RFID readers. Readers include transport, receiver and microprocessor responsible for reading or writing tag information. Radio-frequency signals between RFID tag and the reader are transmitted by Antennas. This layer collects information and identifies the physical world.

b) **The middleware system** is responsible for information transmission, initial processing of information, and classification of data. This layer includes key server and Object Naming Service (ONS) server.

c) **The Internet system** is responsible for analysis, processing, control and decision making of information to implement customized services ordered by users and controlling the connection between things and things. This layer includes the internet and database (PML database).

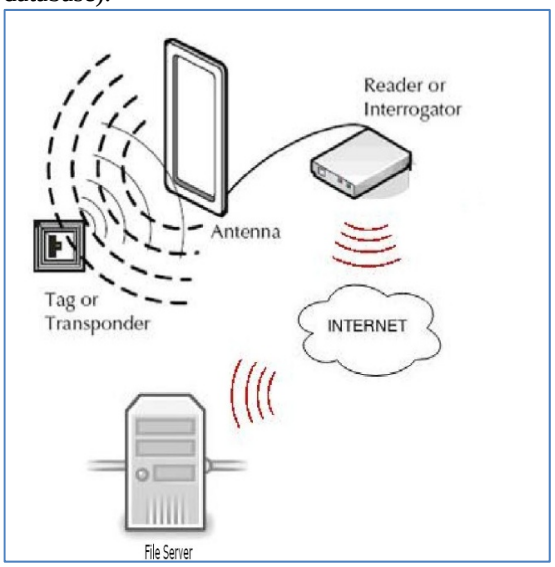

Figure 2: Working of IOT

Through the EPC code saved in RFID tag, the reader collects data from the tag. The middleware system can find the relevant information of the object by finding the corresponding IP address on the Object Naming Server on the internet through this EPC code and the information is processed and managed by the middleware system

IV. SMART ENVIRONMENT WITH IOT

We propose the use of IOT which uses intelligent bar codes(RFID) that can talk to a networked system to track every product that you put in your shopping cart. IOT with RFIDs can be used in shopping malls. These RFID tags will communicate with an electronic reader that will detect every item in the cart. The reader will be connected to a large network that will send information on your products to the retailer and product manufacturers. Your bank will then be notified and the amount of the bill will be deducted from your account.

- At the grocery store, you buy a carton of milk. The milk containers will have an RFID tag that stores the milk's expiration date and price. When you lift the milk from the shelf, the shelf may display the milk's specific expiration date, or the information could be wirelessly sent to your personal digital assistant or cell phone.
- As you exit the store, you pass through doors with an embedded tag reader. This reader tabulates the cost of all the items in your shopping cart and sends the grocery bill to your bank, which deducts the amount from your account. Product manufacturers know that you've bought their product, and the store's computers know exactly how many of each product need to be reordered.
- Once you get home, you put your milk in the refrigerator, which is also equipped with a tag reader. This smart refrigerator is capable of tracking all of the groceries stored in it. It can track the foods you use and how often you restock your refrigerator, and can let you know when that milk and other foods spoil.
- Products are also tracked when they are thrown into a trash can or recycle bin. At this point, your refrigerator could add milk to your grocery list, or you could program the fridge to order these items automatically.
- Based on the products you buy, your grocery store gets to know your unique preferences. Instead of receiving generic newsletters with weekly grocery specials, you might receive one created just for you.

In order for this system to work, each product will be given a unique product number. MIT's Auto-ID Center is working on an **Electronic Product Code** (EPC) identifier that could replace the UPC. Every smart label could contain 96 bits of information, including the product manufacturer, product name and a 40-bit serial number. Using this system, a smart label would communicate with a network called the **Object Naming Service**. This database would retrieve information about a product and then direct information to the manufacturer's computers.

V. PROTECTING OBECT INFORMATION SENT FROM TAG

1. Killing the Tag

The manufacturer of the items can embed C1G2 UHF Tags with a Kill Password as per the EPCglobal C1G2 UHF RFID Protocol standard [3]. the tag is permanently unusable and unreadable whenever an RFID reader sends this kill password to the tag. Therefore, once a tagged item is purchased by customer, the cashier (point-of-sale) can obtain the tag's kill password from the store's EPC-Information system and kill the tag permanently.

2. Locking the Tag

The manufacturer of the items can also embed C1G2 UHF Tags with a unique 32-bit value Access Password as per the EPCglobal C1G2 UHF RFID Protocol standard [3] .The tag verifies the access password sent by the RFID reader to check if it is the same as the one embedded within itself. If the access passwords tally, the tag allows the reader to perform Read, Write, and Lock operation on it. A tag's chip

has four memory banks: Reserved, EPC, TID, and User. The Reserved memory bank is used to store the kill password and access password. The reserved memory bank is permanently locked by the manufacturer; as a result the access password can neither be read nor modified by any reader. As mentioned above, most of the tags contain only its unique EPC number and all the data associated with that EPC number is stored with the EPC-Information system(EPC-IS). Access to the EPC-IS is secure, and restricted to only authorized supply chain stakeholders. Generally, the EPC memory bank is never locked, because the EPC number is used to retrieve the data associated with that item and also to retrieve its corresponding access password (from EPC-IS). Based on the above-mentioned access password and locking features available with C1G2 UHF tags, we propose the following approach, where the tag need not be killed permanently in order to protect consumer privacy. Once a tagged item is purchased by customer, the clerk at the point-of-sale can retrieve the tag's access password from the store's EPC-IS and using this access password, the clerk can lock all the memory banks of the tag including the EPC memory bank. The customer can download and store the EPC numbers and their corresponding access passwords into her mobile/smart phone. This can be made possible via the mobile RFID-enabled mobile/smart phone communicating with the mobile RFID-module at the point-of-sale. With this proposed approach, the intruder can no longer get any information (including the EPC number) from the RFID tags that are in customer's possession, as all the memory banks of the tags are locked and intruder does not have the access passwords.

After purchasing the RFID tagged items from the store, the retailer terminal allows the shop manager to download and store the EPC numbers and their corresponding access passwords into the mobile RFID-enabled mobile/smart phone. Shop manager uses the Smartphone's 3G/4G/Wi-FI network to establish an HTTPS (Hypertext Transfer Protocol Secure) connection [5] with the shop server, in order to send the EPC numbers and their access passwords. Based on the EPC numbers, the shop server identifies the appropriate EPC-IS and uses the access passwords as proof of purchase, downloads the related information (product description, size, weight, manufacturing date, expiry date, directions to use, ingredients, warranty certificate, etc.) associated with the EPC numbers. The EPC-IS must provide only the information, which is relevant to the consumer who purchased the items. Therefore, by the time shop manager has purchased tagged items, the shop server is ready with all the information about the items. After obtaining the EPC numbers from Shop managers mobile RFID-device, the shop server now needs to contact the appropriate EPC-IS to download the related information associated with the EPC numbers. As per the EPCglobal Architecture Specification [2], there exists an Object Naming Service (ONS), which can assist the shop server in locating the EPC-IS. The retailer at the point-of-sale gives away the access passwords to only those consumers who purchased the tagged items. The EPC-IS already has the list of EPC numbers and their corresponding access passwords, therefore when the shop server sends the access passwords to the EPC-IS it proves that shop manager/shop server indeed purchased the tagged items.

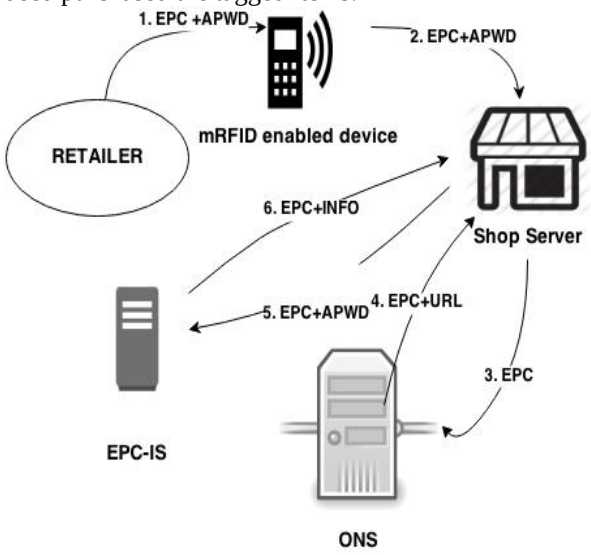

Figure 3. Secure Communication between mobile- RFID-device, shop server and EPC-IS.

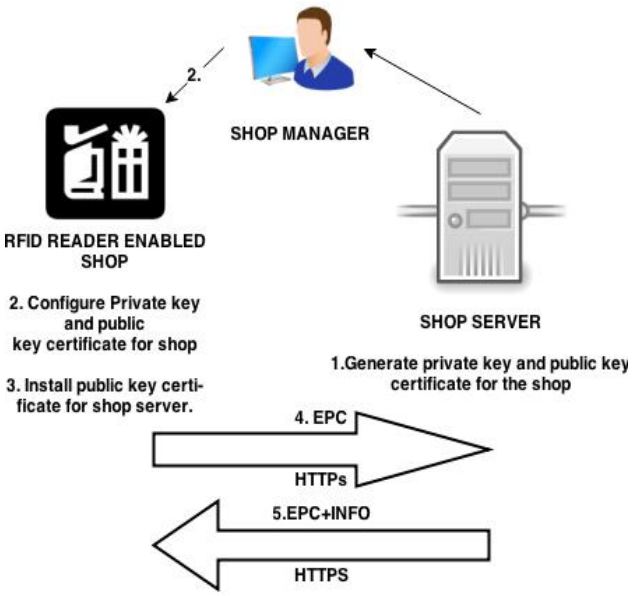

Figure 4. Secure Communication between the Shop objects and shop server.

The RFID reader in the Shop does not get any EPC numbers from the newly added items in the shop as their memory banks are all locked. In such a situation, the RFID reader communicates with the shop server and requests all the RFID tag access passwords that have been downloaded by the server (from EPC-IS) but not yet activated in the smart shop. The shop server then sends all those access to the RFID reader in the shop and the reader checks each of these passwords with every locked tag until a particular tag responds with its EPC number. With this approach a tag can be unlocked without knowing its EPC number initially. This approach can be easily understood by looking at the Figure 4.

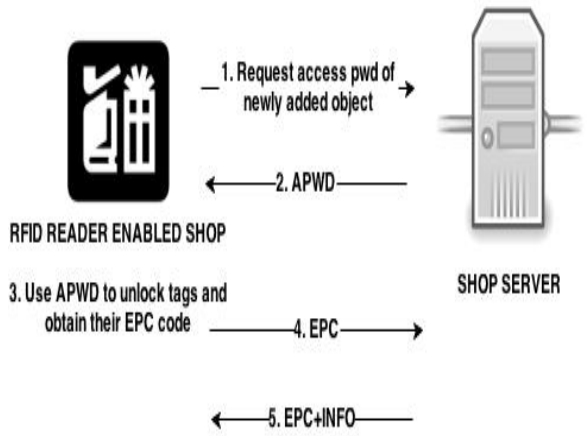

Figure 5. Unlocking RFID tags using an RFID Reader-enabled Device

VI. CONCLUSION

In this paper we considered IOT-based 'Smart Environment' scenarios that based on RFID. We identified some of the security and privacy threats and identified the need for protecting consumer privacy and proposed a "Kill Password" and "Access Password" approach to provide authentication, data confidentiality, and data integrity at the various levels of communication.

REFERENCES

[1] Shao Xiwen, "Study on Security Issue of Internet of Things based on RFID," Proc. IEEE 2012 Fourth International Conference on Computational and Information Sciences(ICCIS), IEEE Press, Aug.2012, pp. 566–569, doi:10.1109/ICCIS.2012.301.

[2] S. Mohammadi, and S. G. Mesgarha, "Autonomous Movement in Car with The Base of RFID", *World Academy of Science, Engineering and Technology*, Vol. 58, pp. 580-583, 2011.

[3] W. Gueaieb, and M.S. Miah, "An Intelligent Mobile Robot Navigation Technique Using RFID Technology". *IEEE Transactions on Instrumentation and Measurement*, Vol. 57, Issue. 9, September 2008.

[4] Xiao Nie;Xiong Zhong "Security In the Internet of Things Based on RFID: Issues and Current Countermeasures" in Proc. 2nd International Conference on Computer Science and Electronics Engineering ICCSEE 2013. International Conference, 2013.pp.1181-1184.

[5] A. Amanna, A. Agrawal and M. Manteghi, "Active RFID For Enhanced Railway Operations", *Proceedings of the ASME 2010 Rail Transport Division Fall Conference, RTDF2010*, Roanoke, USA, October, 2010.

[6] Tao Yan, Qiaoyan Wen,"A Secure Mobile RFID Architecture for the Internet of Things",Proc. IEEE Information Theory and Information Security (ICITIS), IEEE Press, Dec. 2010,pp.616-619,doi:10.1109/ICITIS.2010.5689514.