Advanced Smart Algorithm for Integrating RFID and IoT Security

Aseel Khalid Ahmed[a], Ammar Falih Mahdi[a], and Dmytro Khlaponin[b]

[a] *Al Rafidain University College, Palestine str., Al-Mustansirya, Baghdad, Iraq*
[b] *Kyiv National University of Construction and Architecture, Povitriflotskyi ave., 31, 03037, Kyiv, Ukraine*

Abstract

This research is an exploration into developing a system for enabling Radio Frequency Identification (RFID) labels to be connected to the Internet while taking into account their unique impediments. Additionally, this mechanism enables the tag to be extraordinarily distinct and spoken to as a communication material capable of communicating with other participants, which can facilitate and rearrange the use of the "Internet of Things" concept in the not-too-distant future. To build a mechanism capable of connecting RFID labels to the Internet. The methods taken by various researchers are investigated and dissected, enabling a better understanding of the difficulties and shortcomings associated with RFID labels connected to the Internet. The analysis and examination have resulted in the creation of another system that allows use of TCP/IP. The structure established in this paper is predicated on the capability of RFID labels to be used as procedures (TCP forms) within a host. As a result, each procedure has a procedure ID or port number, which enables various members to identify and communicate with the tag through the process ID. This is accomplished through a built-in interpretation portion that converts the RFID tag's authentic personality (ID) to a new ID that can be recognized as a TCP port number. The results of this paper show that the system worked effectively for the purpose for which it was designed. The results show that the actualized system enables RFID labels to be linked to the Internet and to be exceptionally distinct. Additionally, it enables labels to send and receive information and guidance outside of the RFID system, through the Internet, and from various members. The framework's success would provide several experts with opportunities to actualize the concept of "Internet of Things."

Keywords

Smart, network, algorithm, RFID, TCP/IP, IoT.

1. Introduction

The wheel of invention progresses steadily. Consistently in the twenty-first century, another invention, plan, or concept is introduced. By "modern inventions," I mean new devices that we use on a daily basis, such as advanced cells, table PCs, and music players. Similarly, the Internet is the vital nerve of advanced innovation. In construction of IoT network, the RFID technologies play the role of the front-end data collection via tag identification, as the basis of IoT. Hence, the adoption of RFID technologies is spurring innovation and the development of the IoT. However, in RFID system, one of the most important challenges is the collision resolution between the tags when these tags transmit their data to the reader simultaneously. We carry out our daily individual activities via the Internet, such as shopping, informing, paying bills, sponsoring, and browsing websites. Subsequently, the Internet has been involved in almost every aspect of our lives, and we have become more tried and true as a result. The combination of Internet administrations and gadgets expands the horizon for new inventions and ideas. These concepts are certain to frame significant events in the not-too-distant future. Among these vital concocted concepts is the concept of the Internet of Things. This concept revolves around establishing a link between any protest on the planet and the Internet. When a protest is connected to

Emerging Technology Trends on the Smart Industry and the Internet of Things, January 19, 2022, Kyiv, Ukraine
EMAIL: aseeleelcom@gmail.com (A. K. Ahmed); afmphd75@gmail.com (A. F. Mahdi); kmld85@gmail.com (D. Khlaponin)
ORCID: 0000-0002-1445-9600 (A. K. Ahmed); 0000-0003-0209-3477 (A. F. Mahdi); 0000-0002-7797-4319 (D. Khlaponin)

the Internet, it has the capacity to communicate with various objects. These papers may be anything from basic outline personal computers to a small issue with an integrated circuit. This hypothesis was predicated on the possibility that the Internet would serve as the main digital platform for coordinating all of these things. Nonetheless, the scientist can run into various difficulties when attempting to apply this concept. The misunderstanding does not originate on the Internet. Or perhaps the difficulties arise as a result of the posts that are to be associated with the Internet. A portion of these objects are unable to be connected to the Internet due to the requirement of interior gadgets that consider Internet connectivity. A device, such as an RFID sticker, does not have the capability of being connected to the Internet. This is because the RFID labels' outline could be improved. Or perhaps the existing outlines are shabby and inadequate. Following that, if any expert wishes to implement the "Internet of Things" concept, the most critical device to focus on is the RFID labels. There are several benefits to connecting RFID labels to the Internet. Typically, RFID marks are used to identify the articles to which they are attached. Regardless, as these labels are connected to the Internet, they can be used to identify and monitor the objects attached to them. These characteristics can be applied in a variety of fields; for example, they can be used in product fabrication to monitor and differentiate the item's status and completion level. Additionally, it could be used to monitor the shipments of goods and services between the manufacturer and the providers. Additionally, it could be used in transportation fields, such as enhancing and increasing the proficiency of open transport armadas, monitoring the movement stream on city streets, and tracking stolen automobiles. RFID marks have a wide variety of applications and are used in a wide variety of fields. The primary objective of this investigation is to look at some of the impediments that prevent RFID labels from being connected to the Internet. The techniques previously used by various researchers to attempt to link RFID labels to the Internet are examined. Finally, the analyst attempts to determine how to link RFID labels to the Internet.

2. RFID Basics

Different kinds and varieties of RFID frameworks are composed of three fundamental components, as illustrated in (figure 1) [1]. The primary section is the RFID label that is attached to a product and is assigned a unique identifier (number) called an electronic item code (EPC) as well as details about the product. Occasionally, it can integrate sensors. The second section is the RFID. Investigators, also known as readers. The RFID investigation specialist has a single job: to provide and track RFID label interchanges. The final section is dedicated to the backend system. The backend system connects RFID examiners to external systems or software, such as a federated database or the Internet. The integrated database stores additional information, such as the cost of each RFID-tagged item.

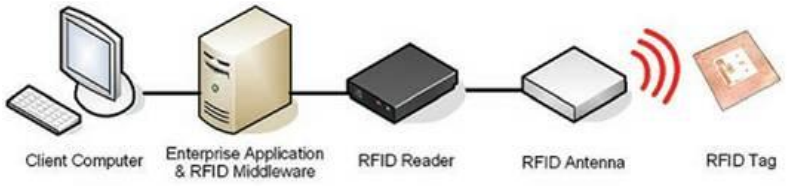


Figure 1 RFID System Diagram

3. RFID Labels

RFID labels are classified into four broad categories.

- Passive .
- Active.
- Semi passive.
- Semi active.

Do not have an installed control source in passive labels. It consists solely of a microchip and a reception apparatus, as described in (Figure 2) [2] Control of the latent mark is delegated to another source, specifically the RFID readers [3]. They obtain the necessary energy for the operation through the RFID investigator cross examination flag (Radio flag produced by the reader).

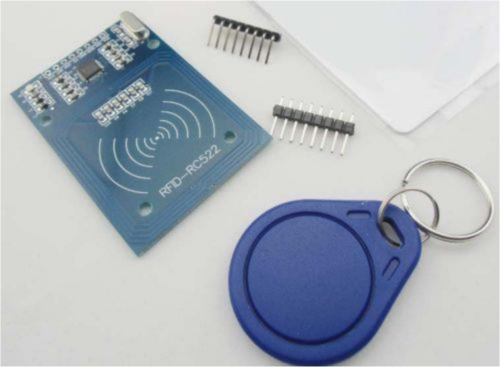


Figure 2: Passive RFID

When the tag is within the range of the radio recurrence region, the reader transmits electromagnetic waves that allow the microchip on the tag to function. When the power level in the microchip reaches the required base voltage for operation, the tag will transmit data back to the readers through similar waves [4]. Figure 3 illustrates the latent RFID framework's operational requirements. Latent RFID's correspondence range is constrained in two distinct ways. To begin, the tag must obtain extremely strong signals from the readers in order to monitor the label microchip. Additionally, is the remaining metric of strength available for a tag to react to readers. These constraints usually limit Passive RFID operation to three meters or less, depending on the frequency of the mission. Occasionally, the range can be as small as a few cm [5].

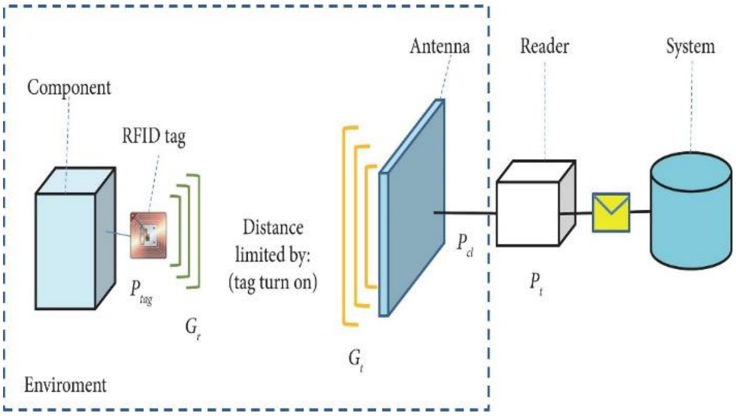


Figure 3: Working standards of Passive RFID framework

Active RFID labels are the second most prevalent form of label used today (after latent labels). The microchips and reception apparatus on dynamic labels are superior to those on inactive labels. Additionally, they incorporate unique identifiers and various gadgets, for example, sensors. Additionally, dynamic labels have their own control source, which is a battery that powers the chips within the labels. This enables the labels to respond to a weaker flag from the readers. [4] In (figure 4) [7], dynamic labels are depicted.

Figure 4: Active RFID

Semi-passive RFID tags are similar to standard detached labels, except that they contain an internal battery (figure 5) [8]. Semi-involved labels control the controller or integrated circuit using a locally accessible power source. Additionally, they can incorporate additional devices, such as sensors. Semi-passive RFID tags are similar to standard detached labels, except that they contain an internal battery (figure 5) [8]. Semi-involved labels control the controller or integrated circuit using a locally accessible power source. Additionally, they can incorporate additional devices, such as sensors.

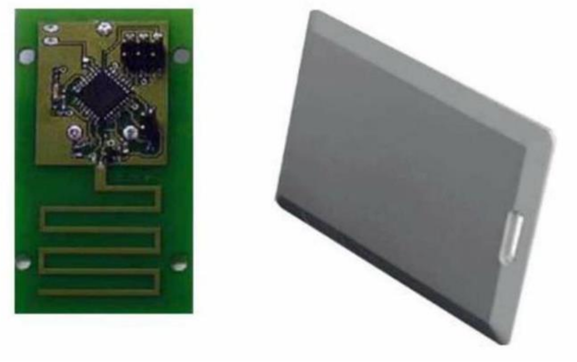


Figure 5: Semi-Passive

RFID Tags that are semi-active labels, like dynamic labels, are powered by small batteries. The batteries maintain the microchips' readiness, causing the labels to react 13 times faster [9][10][11]. Semi dynamic RFID labels include a working transmitter that is powered by an internal power source. Due to the inward power source, their transmission may be detected at a greater distance or with greater impedance than a semi-active or aloof RFID tag. Semi dynamic RFID labels are advantageous for tracking items in extremely noisy environments where aloof or semi-active labels are unable to communicate with readers [12][13]. The nanotag and burst switch are two examples of semi-dynamic RFID tags developed by the University of Pittsburgh's RFID Center of Excellence [14]. These types of labels are still in development.

4. Proposed Framework Parts

The suggested framework is composed of fundamental segments that are identical to those found in other RFID frameworks. Additionally, the system is connected to the Internet, enabling it to send and receive information and data to and from other members. The framework's key components.

5. RFID Labels (Forms)

In the proposed context, RFID labels are referred to as procedures inside the host. Each tag has a unique identifier that is detailed in the EPC code. This ID allows the tag and readers to recognize and communicate with one another. This is the normal operating environment for the RFID system. When the labels' information or data is transmitted over the Internet, the labels are no longer referred to as labels. Rather than that, these marks are now referred to as procedures inside the host. Alternate members recognize the tag as a protocol associated with that particular host. As a result, it is connected with that procedure through the port number assigned to that procedure. Finally, readers recognize each tag by its EPC number, and alternate members recognize it by its procedure number via the Network.

6. RFID Readers

In the proposed system, readers play a critical role in transmitting knowledge from one source to the next. It performs the standard function of all RFID readers, which is to interpret and communicate with the labels. On the other side, readers will use the IP address to connect to the Internet. As a result, the readers will be able to discern each procedure contained within it by using this IP address. Regardless, by combining the have's IP address and the tag's procedure number, it allows any participant to send, as well as receive, information and data to the specific tag. Finally, it allows the marks to be distinguished through the Internet. Finally, all address interpretation operations from the EPC of the labels to the procedure number and vice versa are conducted in the learners.

7. Smart Middleware Framework

The middleware system stores information and data about the objects associated with the marks. The information could be stored inside the tag, assuming the tag is capable of storing it. At times, the middleware system fulfills the reader's duties, which include maintaining communication with the outside world and acting as an interpreter for the labels' ID. This may occur when compact readers are used in systems or when the readers lack sufficient memory to perform all of the tasks independently. RFID tags (forms)

In the proposed context, RFID labels are referred to as procedures inside the host. Each tag has a unique identifier that is defined in the EPC code plan. This ID allows the tag and readers to recognize and communicate with one another. This is the normal operating environment for the RFID system. When the labels' information or data is transmitted over the Internet, the labels are no longer referred to as labels. Rather than that, these marks are now referred to as procedures inside the host. Alternate members recognize the tag as a protocol associated with that particular host. It is associated with that procedure in this manner by using the port number associated with that procedure. Finally, each tag is identified by its EPC number by readers and by its procedure number by alternate members via the Internet.

The execution of the "Internet of Things" concept is predicated on the awe-inspiring fact that any object can be connected to the Internet. Not only can these things be connected to the Internet, but they can also communicate with one another through the Internet. This concept is realized in the proposed system, which allows alternate representatives to be any question as long as they are connected to the Internet and capable of communicating with other questions through the Internet. The products can include a personal computer, a host, a sensor, or even an RFID tag). There are two fundamental characteristics of alternate participants. To begin, it should be capable of performing the interpretation instrument. Second, it should be capable of implementing the correspondence convention. With these characteristics, any protest can be correlated with and effectively trade information and data over the Internet with the proposed system. The middleware system stores information and data about the objects associated with the marks. The information could be stored inside the tag, assuming the tag is capable of storing it. At times, the middleware system fulfills the reader's duties, which include maintaining communication with the outside world and acting as an interpreter for the labels' ID. This may occur when compact readers are used in systems or when the readers lack sufficient memory to perform all of the tasks independently. RFID tags (forms)

In the proposed context, RFID labels are referred to as procedures inside the host. Each tag has a unique identifier that is defined in the EPC code plan. This ID allows the tag and readers to recognize and communicate with one another. This is the normal operating environment for the RFID system. When the labels' information or data is transmitted over the Internet, the labels are no longer referred to as labels. Rather than that, these marks are now referred to as procedures inside the host. Alternate members recognize the tag as a protocol associated with that particular host. It is associated with that procedure in this manner by using the port number associated with that procedure. Finally, each tag is identified by its EPC number by readers and by its procedure number by alternate members via the Internet.

The execution of the "Internet of Things" concept is predicated on the awe-inspiring fact that any object can be connected to the Internet. Not only can these things be connected to the Internet, but they can also communicate with one another through the Internet. This concept is realized in the proposed system, which allows alternate representatives to be any question as long as they are connected to the Internet and capable of communicating with other questions through the Internet. The products can include a personal computer, a host, a sensor, or even an RFID tag). There are two fundamental characteristics of alternate participants. To begin, it should be capable of performing the interpretation instrument. Second, it should be capable of implementing the correspondence convention. With these characteristics, any protest can be correlated with and effectively trade information and data over the Internet with the proposed system.

8. The Operation of the Proposed Smart Working Framework

The proposed working framework's rule structure is divided into two fundamental stages. It is fundamental to understand job standards. The primary stage depicts the actions carried out by the other participant and the manner in which information is communicated to the have. The second stage clarifies the activities and methods used to prepare the information in the host (readers) and is antagonistic to the objective process (tag). The main stage begins when an external PC (a different member) attempts to submit data to the objective tag. Before the outside PC can send the data to its destination, it must complete a few tasks. The first task is to use the interpretation component to convert the EPC code of the tag to another 16-bit address called the procedure number. The process number is used to direct data to the appropriate objective procedure (tag) within the target have. The second operation, the TCP layer header, which contains the procedure number in the port number field, is exemplified by information that should have been conveyed. The exemplified frame is referred to as portions. In the third operation, these parts are embodied by the Internet layer's header, which includes the goal's IP address. At the moment, information is exemplified by the headers f the device layer and is referred to as information parcels. Finally, these packets have been connected to the Internet. Figure 6 illustrates one of the existing working guidelines in its entirety.

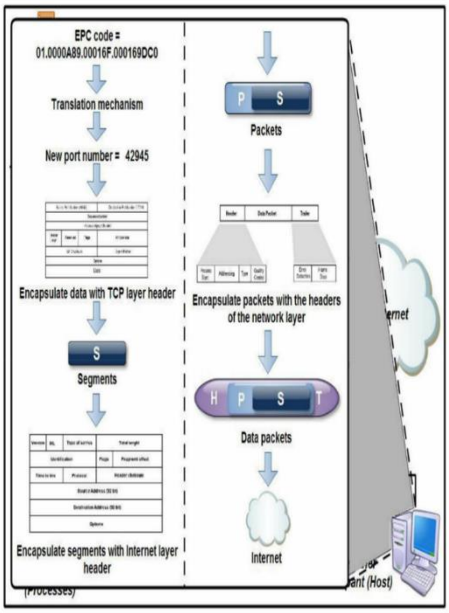


Figure 6: part one of proposed working principle

When the data packet enters the destination host, the second stage starts. At this stage, the data packet can be handled in one of two ways. The first approach is focused on the separation of data packets based on their size. Active tags' data packets are significantly larger than passive tags' data packets.

The difference in size is due to the fact that passive tags do not transmit or receive a large volume of data. The types of data that passive tags monitor are limited to read, write, and destroy instructions. On the contrary, the active tags control a variety of data types, including instructions and/or information. Such data, which may include product information, must be stored in the tag memory. As a result, these tags are larger in size. After classifying the data packets, the next decision is which operations to perform. Depending on the tag sort, various operations are performed on different data packets (passive or active).

9. Operation Performed on the Data Packet with Passive RFID

Following identification of the data packet based on its size, the data packet with the smallest size (passive data packet) is processed within the reader. The process begins when the host (reader) begins opening the data packets' encapsulation before they enter the TCP layer. At that step, it will extract the data and the destination process's address (tag), which is the process number for this specific data. Following that, the host performs address conversion on the process number, converting the 16-bit address to its original 64-bit – 256-bit format. Finally, the host executes the process's read, write, or destroy instructions. The primary operation of passive data packets is shown in (figure 7). If the host is asked to send the data or information about the tag back to the other participant, the host will conduct all previous operations in reverse order. However, in some situations, additional information about the product attached to the tag may be required.

This additional data can be stored in a middleware device separate from the host (reader). Before initiating the operation sequence, the host will request the necessary data from the middleware device.

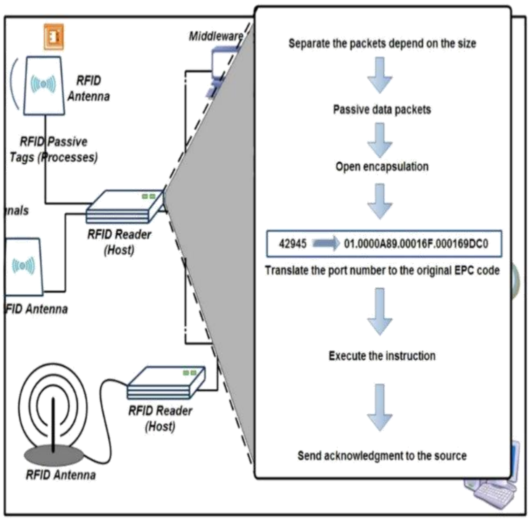

Middleware
RFID Antenna
RFID Passive Tags (Processes)
nals
RFID Reader (Host)
FID Antenna
RFID Reader (Host)
RFID Antenna
Separate the packets depend on the size
Passive data packets
Open encapsulation
42945
01.0000A89.00016F.000169DC0
Translate the port number to the original EPC code
Execute the instruction
Send acknowledgment to the source

Figure 7: The operation of passive data packets

10.Operation Performed on the Data Packet of the Active RFID

The operation performed on active RFID data packets is distinct from the operation performed on passive RFID data packets. After the host (reader) determines the packet's size and distinguishes active from passive packets, the active data packets are sent or guided to the tag. The tag performs the operations of opening the encapsulation, translating the address, and executing the instruction. Active data packets are routed to the tag for processing, as active tags provide ample memory and processing power to perform these operations. Additionally, active RFID tags are capable of implementing a more compact variant of the communication protocol, such as the UTP protocol, in order to perform the required operations for receiving and assembling data packets. In this case, the host acts as a router, routing the data packets to their intended destinations. [16].

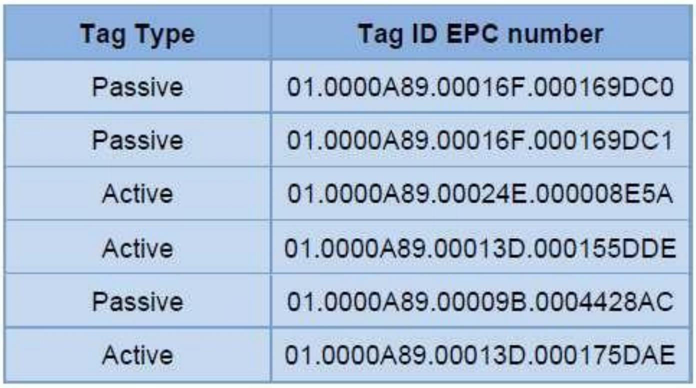
However, one drawback of this approach is that the reader must broadcast these packets. This means that each active tag will decrypt the packet's encapsulation. Only when the correct/target tag enters the packet will the reader receive acknowledgement. Otherwise, the reader would send a message to the source informing it of the mistake. The second approach is based on the tag's unique identifier. The reader performs all operations necessary for opening the encapsulation and translating the addresses of all received data packets in this process (passive and active).

Following that, the reader will execute the instruction associated with that tag. This is close to how passive data packets operate. Both of the suggested approaches require the source to obtain confirmation from the host that the data has arrived at its destination and the instructions have been correctly executed. Otherwise, the source would receive a response from the host indicating that the execution failed.

11.Testing and Results

After establishing the system's operations and primary translation mechanism, it's time to evaluate the system's ability to link RFID tags to the Internet using six separate RFID tags belonging to two distinct categories (Passive and Active). The tags used in the test are specified in (Table 1), which includes the tag type and EPC number for each tag.

Table 1: Testing RFID tags and its EPC code



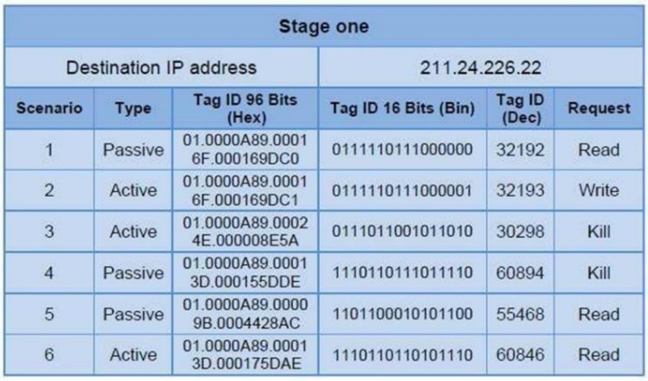
Tag Type	Tag ID EPC number
Passive	01.0000A89.00016F.000169DC0
Passive	01.0000A89.00016F.000169DC1
Active	01.0000A89.00024E.000008E5A
Active	01.0000A89.00013D.000155DDE
Passive	01.0000A89.00009B.0004428AC
Active	01.0000A89.00013D.000175DAE

The system's testing is split into two distinct phases. Each stage addresses and clarifies the changes to the format of the tag identifier or EPC code. Additionally, each stage specifies the form of instructions that will be transmitted and received by the source and destination hosts.

11.1 Step One

In step one, data is transferred from an external host to the host. The data is in the form of a request, which instructs the host to conduct a specific operation on the processes running on it and to respond to the external host. The process begins when an external host sends the host a request for information about a specific process running within it, in the form of instructions containing the process ID. However, before the external host can make a request, it must convert the EPC code of the tag to an Internet-compatible format. This step is carried out using the translation process discussed previously. This mechanism will transform the tag's identity from its original (96 Bits) hexadecimal representation to the current decimal representation in three stages. It will convert the EPC code from hexadecimal to binary numbers in the first phase. The second step entails initiating the translation process in order to select sixteen bits from the created binary numbers using the schema (0, 0, 5, and 11). The numbers in the schema correspond to a 0 bit header field, a 0 bit EPC manager field, a 5 bit object type field, and an 11 bit serial number field. This produces a 16-bit binary number that is ready for use. The third phase converts the 16-bit binary number to a decimal value that can be injected into the destination port region of the communication protocol's TCP header (the third phase is only used for demonstration purposes in the simulation system)[15]. Finally, the data representing the request instructions will be encapsulated with the tag's new ID (process) and transmitted to the host. The outcomes of all operations are summarized in Table 2.

Table 2: RFID tag types, IDs and the requested instructions



Stage one					
Destination IP address			211.24.226.22		
Scenario	**Type**	**Tag ID 96 Bits (Hex)**	**Tag ID 16 Bits (Bin)**	**Tag ID (Dec)**	**Request**
1	Passive	01.0000A89.0001 6F.000169DC0	0111110111000000	32192	Read
2	Active	01.0000A89.0001 6F.000169DC1	0111110111000001	32193	Write
3	Active	01.0000A89.0002 4E.000008E5A	0111011001011010	30298	Kill
4	Passive	01.0000A89.0001 3D.000155DDE	1110110111011110	60894	Kill
5	Passive	01.0000A89.0000 9B.0004428AC	1101100010101100	55468	Read
6	Active	01.0000A89.0001 3D.000175DAE	1110110110101110	60846	Read

Additionally, Table 2 contains the results of the proposed system's evaluation. The destination IP address is shown at the top of the stack. There is only one IP address since all tags (processes) are linked to a single reader during this study's test (host). As a result, all processes run on a single host with the same IP address. The columns of the table denote the various fields. The first column indicates the number of situations that the proposed method is capable of testing. The second column indicates the type of tag used to evaluate the device (passive or active). The third column contains the tag's original identity, which is encoded in 96 bits of hexadecimal data. The fourth column contains the tag's ID in 16-bit binary format. The fifth column contains the tag's latest decimal ID. The external host will use the new ID to communicate with the destination host about the specified operation. Additionally, the host can use it to understand and classify the mechanism contained inside. In additionally, the new ID enables the execution of specified instructions from an external host associated with the specified procedure, as well as the transmission of the response to the source. Finally, the final column includes the unique requests that must be made on that particular tag (process). The second stage occurs when the external host transmits the data packet to the Internet in order for it to reach its destination (Host).

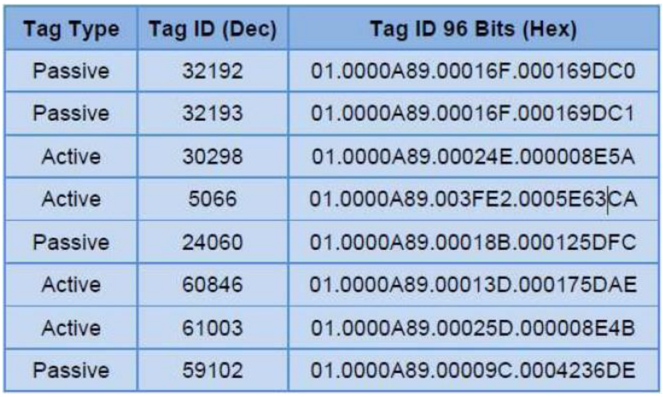
11.2 Step Two

Stage Two starts when the external host's data packets meet their destination or (Host). When this packet reaches its destination, the host performs the necessary operations to de capsulate it. Regrettably, the host received the target process's ID as a decimal number. Meanwhile, the host (reader) has a list of tag IDs from the translation mechanism, which performs translation on the tag IDs (processes) within its range.

The reader memory stores the tag IDs in an internal table. As a result, when the host receives the target process's ID, it performs a simple comparison with the ID stored in its internal table. If the received ID corresponds to an entry in the internal table, the host will execute the requested instruction. When the host has completed the requested instruction's execution, it will send a response to the source (external host).

This response may include an acknowledgment, details, or information from the tag (process) about which the source inquired. On the other hand, if the target ID is not found in the internal table, the host sends an error message to the source (external host). The available tags in this host are listed in Table 3, along with the tag form, the hexadecimal ID for the tag, and the decimal ID for the tag.

Table 3: Available tags in the range of the host (reader)



Tag Type	Tag ID (Dec)	Tag ID 96 Bits (Hex)
Passive	32192	01.0000A89.00016F.000169DC0
Passive	32193	01.0000A89.00016F.000169DC1
Active	30298	01.0000A89.00024E.000008E5A
Active	5066	01.0000A89.003FE2.0005E63CA
Passive	24060	01.0000A89.00018B.000125DFC
Active	60846	01.0000A89.00013D.000175DAE
Active	61003	01.0000A89.00025D.000008E4B
Passive	59102	01.0000A89.00009C.0004236DE

The interpretation of the results demonstrates that the device performed correctly in accordance with the instructions. Regardless of the response type, the device always responded to the external host and executed the external host's requested instructions. As a result, the system's internal operations and engineered processes were performed with reliability and integrity. The proposed system established a communication channel between the RFID tags and the external host successfully (user). This framework has accomplished the primary objective of its design and implementation, which was to link RFID tags to the Internet using the "Internet of Things" model.

12. Conclusion

The idea of the "Internet of Things" is groundbreaking. This idea can pave the way for us to alter our behaviors and the way we currently do things. This philosophy is based around the idea of connecting any object on Earth to the Internet. As a result, RFID tags must be linked to the Internet due to their small size, low cost, and environmental friendliness. However, some criteria for RFID tags do not meet the minimum requirements for Internet connectivity. As a result, the researcher suggested a new system design that would link RFID tags to the Internet. Additionally, the device allows remote users to interact with these tags as self-contained entities. The proposed system's processes underwent several stages before they were able to meet the criteria for linking RFID tags to the Internet. These phases began with the formulation of a novel concept that is diametrically opposed to any other concept proposed by other researchers for linking the tags. Later, an investigation of the issue resulted in the design of a new method based on the analysis's findings. Finally, the system's implementation involves checking it against a variety of situations involving various types of tags.

13. Acknowledgements

We extend our deep thanks to our college, Al-Rafidain University College, for its continuous support for the wheel of research and scientific development, represented by its Dean, Dr. Mahmoud Abu Shaer.

14. References

[1] Atlas RFID store.com (2011), “RFID Tags from Atlas” http://www.atlasrfidstore.com/tags_RFID_chips_s/14.htm [25-Nov-2011].

[2] Brock D. (2001), “The Compact Electronic Product Code™ – a 64-bit Representation of the Electronic Product Code™”. Technical Report MIT-AUTOID-WH-008, Auto-ID Center, November 2001.

[3] P., Venugopal K. R. (2010), "Protocol to Simulate Application of RFID Technology in Public Transportation System", 1st International Conference on Parallel, Distributed and Grid Computing, IEEE. CISCO (2008),” Wi-Fi Location-Based Services 4.1 Design Guide”, Cisco Systems, OL-11612-0, USA.

[4] Dominikus S. and Schmidt J. (2010), "Connecting Passive RFID Tags to theInternet of Things", IAIK, Graz University of Technology.

[5] Engels D. (2003), “The Use of the Electronic Product Code”, institute of technology, Massachusetts, technical report, MIT-AUTOID-TR-009, May 2003.

[6] Engels D.W. (2003), “EPC-256: The 256-bit Electronic Product Code™ Representation”. Technical Report MIT-AUTOID-TR-010, Auto-ID Center, February 2003.

[7] Fleisch E. (2010), “What is the Internet of Things: An Economic Perspective", ETH Zurich / University of St. Gallen, Auto-ID Labs White Paper WPBIZAPP- 053.

[8] Goodrum P. M., McLaren M. A. and Durfee A. (2005), “The application of active radio frequency identification technology for tool tracking on construction job sites”, University of Kentucky, United States, AUTCON-00715.

[9] Kinoshita S., Ohkubo M., Hoshino F., Morohashi G., Shionoiri O. and Kanai A. (2005), “Privacy Enhanced Active RFID Tag”, NTT Information Sharing Platform Laboratories, Japan.

[10] Liu F., Ning H., Yang H., Xu Z. and Cong Y. (2006), ”RFID-based EPC System and Information Services in Intelligent Transportation System”, International Conference on ITS Telecommunications

[11] Nguyenl H. Q., Choi J. H., Kang M., Ghassemlool Z., Kim D. H., Lim S. K., Kang T. G. and Lee C. G. (2010), "A MATLAB-based simulation program for indoor visible light communication system", IEEE.

[12] NKK Abdulhakeem Amer A. , Omeed Kamal Khoursheed., 2017, “Design an Wireless Sensing Network by utilizing Bit Swarm enhancements”, International Journal of Computer Science and Network Security , IJCSNS 17

[13] Savi Technology (2002), “Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility”, White paper by Savi Technology.

[14] A Amer A.,2018,” IMPROVE THE PERFORMANCE OF THE CNPV PROTOCOL IN VANET NETWORKS”, A Amer A. International Journal of Civil Engineering and Technology (IJCIET) (9) (11)

[15] Lee S. D., Shin M. K. and Kim H. J. (2007), "EPC vs. IPv6 mapping mechanism", ICACT2007, ICACT, Korea, PP. 1243 - 1245.

[16] Leiner B. M., Cerf V. G., Clark D. D., Kahn R. E., Kleinrock L., Lynch D. C., Postel J., Roberts L. G. and Wolff S. S. (1997), "The Past and Future History of the Internet" , Communications of the ACM, Vol. 40, No. 2, pp. 102 – 10.