

Ubiquitous Computing with Radio Frequency IDentification Tags

Shabbir Hassan¹, Ahmad Raza Shibli¹, Rehan Raza²

¹Department of Computer Science, Aligarh Muslim University, Aligarh, India

²Department of Computer Science and Engineering, NIT Calicut, Kerala, India

Email address:

hassan.analyst@gmail.com (Shabbir Hassan), ahmedrazashibli@gmail.com (Ahmad Raza Shibli), rhn.raza121@gmail.com (Rehan Raza)

To cite this article:

Shabbir Hassan, Ahmad Raza Shibli, Rehan Raza. Ubiquitous Computing with Radio Frequency IDentification Tags. *Mathematics and Computer Science*. Vol. 8, No. 3, 2023, pp. 73-86. doi: 10.11648/j.mcs.20230803.12

Received: July 23, 2023; **Accepted:** August 14, 2023; **Published:** August 28, 2023

Abstract: Ubiquitous computing is seen as a promising and revolutionary technological path. The goal of promoting marketable innovations and applications is addressed through intense research and developmental activities and policy strategies. This article discusses the state-of-the-art approach of the use case and the drawbacks of identification tags for radio frequency. Radio Frequency IDentification or RFID technology is a growing trend among separate automated technologies for identification. RFIDs are used in construction, engineering, chemical, manufacturing, retail, logistics, and other public industries. The importance and various advantages of RFID in different industries are therefore sometimes different. In this paper, we have performed an extensive literature survey of its current applications and the security measures that can be taken to improve the system. The paper gives an extended model of possible RFID applications in the field of mass gathering and other related applications such as crowd management and stampede management. To manage or optimize the degree of mortality rate concerning the size of the crowd, the paper proposes algorithmic approaches that can be implemented to minimize the degree of mortality. At the end of the RFID applications, other suggested applications have also been provided. Apart from the current RFID security measures, some proposed security solutions such as Tag Data Security, Maintaining Reader Integrity, Personal Privacy, and Improved Hash Lock have also been provided.

Keywords: DDOS, Digestive Tags, Bacon, EPC, Eavesdropper, Cryptanalysis, Randomized Hash Function

1. Introduction

Radio Frequency IDentification (in short RFID) may be referred to as automated identification technological innovation which uses radiofrequency and electromagnetic fields to identify items holding tags if they move toward a reader. The first use of RFID tags (often called a smart label or a transponder) can be seen in the II World War, it was done to recognize the enemy, search for missing items, monitor moving objects and fleets from geostationary satellites, enable keyless entry system and many more. In 2018, the Government of India mandated RFID tags to track the vehicle's movements. Today, many people rely upon this technology and use it to make their life easier. Besides tracking human beings, items, fleets, and animals, various other aspects make use of this technology; such tags are read in various situations and usually require a larger detection

range. RFID may be referred to as an automated identification technology that makes use of Radio Frequency Identification [1, 27] because they are highly readable in different situations and usually have larger detection ranges [3]. RFID is not a line-of-sight technique unlike a barcode reader, however, it may be considered as an automated identification technology that makes the use of radiofrequency and electromagnetic fields to detect an item attached with a tag, when the target object comes under the detection range of the reader. The reader can also fetch any confidential data (such as item number, accession number, account number, etc.) stored within the memory of the tag. The reader can also modify the content of the tag. RFID cannot be reduced to one technology. It makes the use of radiofrequency with different frequency ranges and amplitudes and hence different kinds of tags are possible that possess several characteristics and survive with various communication techniques and power supply. An RFID tag

usually works with an embedded antenna to transfer data from a tag to a reader or the interrogator (also referred to as a base station or more generally a reader). The setup is known as an inlay which is subsequently enclosed to be able to endure the conditions wherein it is going to operate. This end of the product is called the tag, Label, or Transponder [2, 4], it could be a unique identifier, Single Electronic Product Code Identifier (EPC), etc. This identifier cannot be modified, but it can be read when it is written on the digital circuit. Hence, it is referred to as write-once read multiple (WORM). Several digital chips contain additional memory units that can be used to register, change and write pieces of information as per the customer's need. Such memories range in size between a few bits and 10K bits. RFID is an automated radio frequency identification technology that

allows the system to read and write data on the reader and the tag remotely. A reader mainly consists of the following parts: a transmitter, a receiver, a control unit that mainly schedules the process, and a coupling element which is called an antenna (refer to Figure 3). To establish communication with a transponder, a reader might also have some extra interface such as RS232 USB to connect with a computer system [5, 6]. An integrated circuit (IC) is embossed within the transponder that serves as the heart of a tag. It is the transponder that plays a vital role in building an RFID system [32]. The transponder is the most significant component that stores data within it. Whereas the IC performs modulation and demodulation of the radio frequency signals, and the electronic identification is divided into two parts as shown in Figure 1.

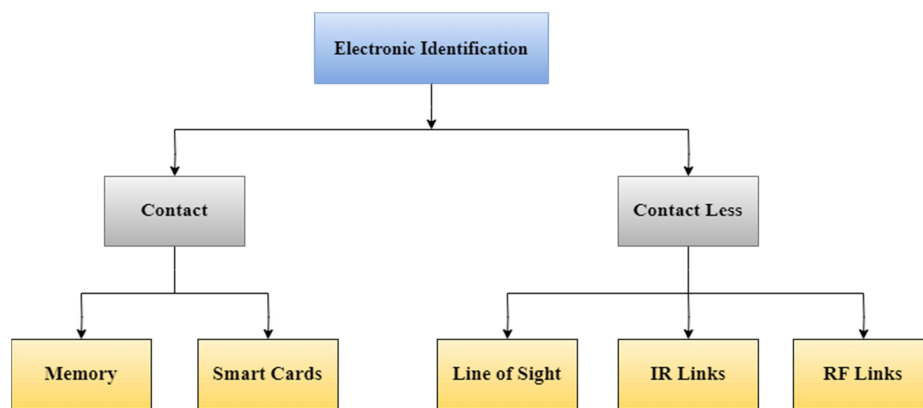


Figure 1. Taxonomy of Electronic identification.

2. RFID Tags Classification

Classification for the RFID tags is based on the existence or nonexistence of an electronic chip (EC). Surface Acoustic Wave (SAW) RFID tag is free from integrated circuits. They are simple read-only transponders that do not contain inlaid energy resources. They are also called Radio Frequency (RF) barcodes. A single-bit RFID tag is a passive system with capacitive diodes referred to as "one-bit Transponders" [6, 8]. This bit indicates whether the tag is physically native to the sphere of influence of operation generated by the interrogator or not. They are generally used to build a framework for anti-theft. The most commonly used products in the real market are RFID tags with integrated circuits that consist of an antenna and a dedicated computational unit.

3. Components of an RFID System

The component of an RFID system has been demonstrated with their essential parts and their role is shown in Figure 4. It includes mainly 5 parts.

3.1. RFID Reader or Interrogator

The RFID interrogator (sometimes also called transceivers or reading zone) comprises antennas, cables, peripherals, and

the environment where the device is mounted. The nature of an interrogation area is defined by the environment in which specular reflection, absorption, or interference with the original signal may occur. It may also be from the presence of many objects. These factors can trigger unintended readings, block the intended readings, and reduce the ability to process them. It is the interrogators that transmit radio frequency to the tag to remotely power it (in passive and semi-passive tags) to read and write data, from and to the tag. Interrogators are also responsible for establishing the bidirectional data flow between other Interrogators and tags themselves and perform analog-to-digital and digital-to-analog signal conversion [5, 9]. A general block diagram of an RFID reader is shown in Figure 3. A reader is also called a coupling device. A complex structure of an RFID tag is shown in Figure 2.

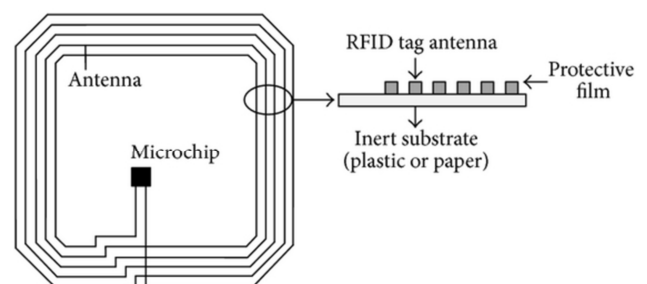


Figure 2. The internal structure of an RFID Tag.

3.2. RFID Antenna

An RFID antenna consists of a coil with one or more windings and a network that fits them. It radiates reader-generated electromagnetic waves and receives RF signals from the transponder. An RFID device can be configured to

continuously produce, or activate, the electromagnetic field via a sensor. Popular types of antennas are rod or loop antennas, which differ in configuration and function depending on the frequency used [1].

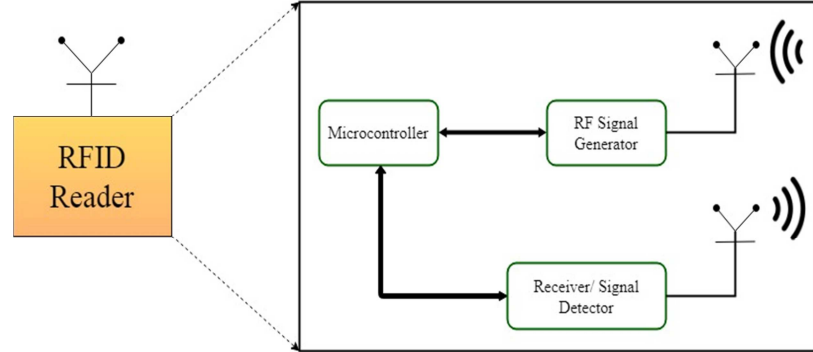


Figure 3. Schematic block diagram of an RFID reader.

3.3. RFID Tag or Transponder

An RFID tag comprises a microchip linked to an antenna that is electronically programmed with unique data. The tag accumulates and transmits signals from and to a reader. It consists of a unique serial number, along with some other essential information such as the customer's bank account number, item code, etc. Based on its application and area of use it possesses many forms and factors. RFID tags can be Active, Passive, or Battery Aided [7, 11].

filtration of data and passing on valuable information only to the organization applications. Some middleware may also be used to manage readers on a network [14, 21].

3.5. Air Interface

Air-driven interface is a platform used to transmit data and/or energy by magnetic or electromagnetic waves [38].

4. Current RFID Technology

In this section, we will explain the different components of an RFID tag, how each component work and precisely what kinds of tags exist that comprise these components. It mainly deals with the supply of power into the tag, what are the acceptable frequency ranges that it can use, what are the utilized bandwidth, etc. The part also explains a few important standards. RFID transponder or a tag mainly contains, i.e., [10].

1. Microchip
2. Antenna
3. Case
4. Battery

The size and overall look of the chip are completely dependent upon the size of the antenna that is embedded into the tag. However, its shape and size also depend upon the utilization frequency range upon which the tag is operating. It should also be noted that the size of an IC is also influenced by its operating range. It has a possible working range of about one millimeter to 30 meters [3, 13]. Besides, some tags have a rewritable store built-in where changes like serial numbers can be registered between two consecutive reads or new data. A basic RFID tag with a well-defined antenna is shown in Figure 4. As we have already mentioned, the antenna has a larger impact on the size of a tag (refer to Figure 4). The microchip is at the center of the tag, as it is a passive tag and therefore does not have an internal power supply [11, 12].

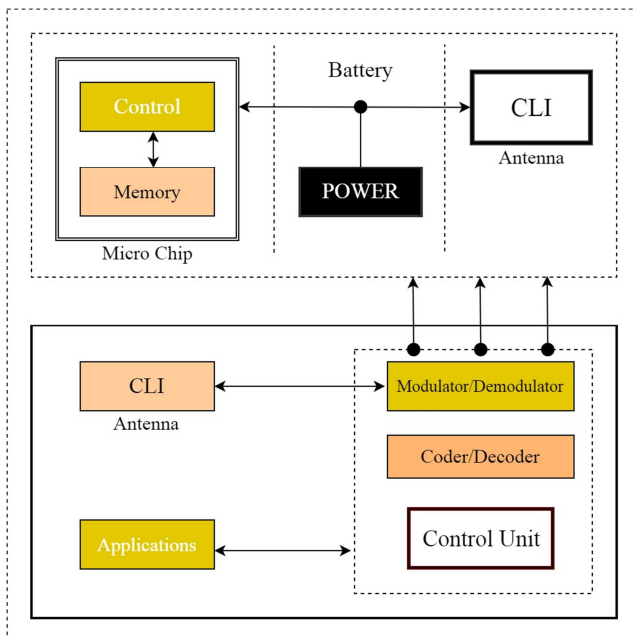


Figure 4. The basic building block of the RFID system.

3.4. Middleware

Middleware is software installed on a host that is linked to interrogators and corporate applications. Which is useful for

5. Energy Sources of an RFID

We have distinguished the RFID tags into three categories based on their relationship with *power supply*, *energy consumption*, and *performance* [2, 12].

1. Passive Tags
2. Semi-passive Tags
3. Active Tags

5.1. Passive Tags

A passive tag does not consist of any internal power resources such as a battery. However, they only depend upon the induced current emitted by the reader. When a transaction has been committed, the reader generates some induced current and the reader needs to maintain the field until the operation has not been completed. Due to the lack of any indigenous power supply, such tags are very small in size and are the cheapest that's available in the market, and more frequently used in libraries. The reading range of such tags has been restricted from about a few meters to 2mm. Moreover, their life span is unlimited because they do not contain any internal power resources which makes them robust and durable [13, 15]. A passive tag is mostly used in real-life applications that can be found in the form of a label also.

5.2. Semi-Passive Tag

The second semi-passive tags are the kind of tags that are rich in internal power resources that keeps the tags powered at all times. It has several advantages over passive tags. Since the chip inside it is always powered it can respond to a request much faster and quickly after it has been made. Since the antenna does not play an essential role to collect power, it can be optimized for backscattering and hence increasing the reading range. Since the tag does not use any energy from the field, the signal strength is much longer. Because of these positive factors, a semi-passive tag is much preferable as compared to a passive tag [16, 17, 18].

5.3. Active Tag

The third and last kind of tag is an active tag. Like a semi-passive tag, it also includes an internal power supply, which is dual, and is used for two different purposes. The first is to supply power to the IC, and the second is to transmit the signal from the antenna. Active tags that transmit signals without any query are called Bacons. The lifetime of an active tag is about 5 years. It can have a working range of up to 10 meters, which makes it ideal for locating things and serving as a landmark point in a big network [17, 19].

6. RFID Frequency Spectrum

RFID is considered a non-specific device that works in a short range. Their working range typically varies from system to system or tag to system. It can use a frequency bandwidth without any license. However, such devices must be compliant with the nearby directive [19, 22]. It is noted

that the frequency range of a tag varies from country to country.

1. Low Frequency [125-134] kHz
2. High Frequency [1.75 to 13.56] kHz
3. Ultra-High Frequency (433MHz) [860-890] MHz

6.1. Low-Frequency

The Low Frequency (LF) band operates between the frequency range of 30 to 300 kHz. Precisely it works at 125 kHz to 134 kHz depending on the framework and the country in which it is used. LF tags are based on inductive coupling technology where the tag is powered by the current induced by the RFID reader as shown in Figure 5. LF tags are generally passive and do not require any internal power supply [39]. Low-frequency RFID tags have long wavelengths that can even penetrate solid metal surfaces (normally, HF and UHF tags cannot be used for metal substances). It can also work with high-water ecosystems, liquids, and solid malarial. As LF tags are based on inductive coupling technology, their read range is, therefore, limited to 0-10 cm and useful for animal detection [20]. For a variety of cases, this restricted range can be used to provide an improved degree of protection i.e. the RFID device can only function when the tag is close to the user. It can be used for sharing confidential information or for car ignition, where a reader inside the vehicle will insert the RFID tag into the key and read it. The device can only operate while close to the vehicle [21].

6.2. High Frequency

The High Frequency (HF) band operates between frequencies ranges 3 to 30 MHz precisely it works from 1.75 MHz to 13.56 MHz [21]. HF tags are based on Near Field coupling technology (refer to Figure 5) where the tag is powered by the current induced by the RFID reader. Such tags are usually passive and do not need a battery or power source [22].

They have anti-collision capabilities that allow multiple tags to be read simultaneously by one reader. The range of these systems is usually under 1 meter hence they are used for Access Control, Passports, and Payment Cards, in Libraries, Inventory Systems, and Product Tracking [7, 8]. High-frequency tags often work pretty well with metal items. HF RFID systems are used in a wide range of applications including ticketing, purchases, library monitoring, patient flow monitoring, and general applications for data transmission [40].

6.3. Ultra-High Frequency

The Ultra High Frequency (UHF) band operates between the frequency range of 300 MHz to 1 GHz. Precisely it works at 433 MHz and between 860 to 960 MHz [23]. A UHF tag is based on the principle of far-field radiative coupling or backscatter coupling (refer to Figure 6) and offers much more read range as compared to an LF and HF tag. The high rate of data transfer makes it ideal for applications that need to read multiple items at once, such as goods boxes passing through a door into a warehouse or racers crossing an end line. The UHF RFID tag read range is approx 50 feet that are

In the case of UHF readers, tags are placed apart from each other. Hence coupling between the reader and the tags is a far-field coupling. For energizing the RFID tag a far-field antenna uses capacitive coupling (or propagation coupling). Capacitive coupling occurs when the antenna of the RFID

reader propagates RF energy outward and the tag is energized with that energy as shown in Figure 6. The tag then sends a portion of the RF energy back to the reader's antenna as a reaction known as backscatter coupling or FAR FIELD [14].

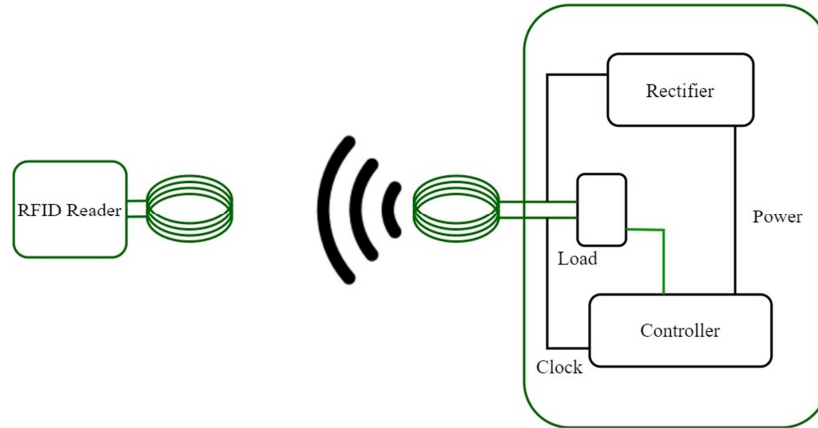


Figure 6. Far-Field coupling of an RFID system.

Once activated the tag gets instructions from the reading unit and responds by sending its serial number. In most cases, the tag does not have plenty of energy to produce its electromagnetic field, instead, it uses backscattering to modulate (reflect/absorb) the field sent by the reading unit.

Since almost all liquids digest electromagnetic fields and almost all metals reflect those fields the reading of the tags in the presence of those materials is complicated. During each reading cycle, the reader has to continuously power the tag.

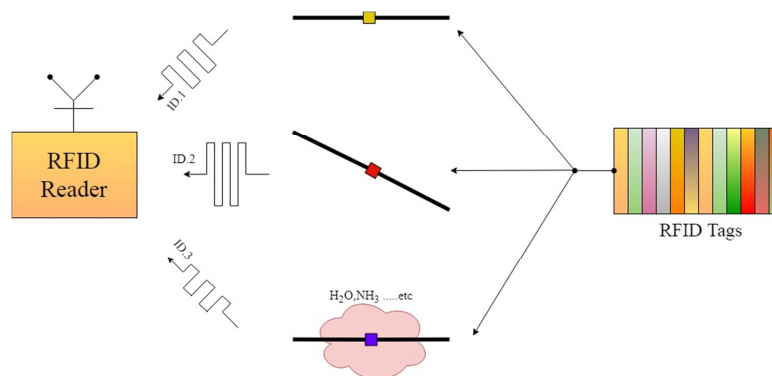


Figure 7. Working principle of an RFID system.

The produced field is called a continuous wave, and because the intensity of the field decreases with the square of the distance, the readers have to use a rather greater power source [13, 14]. That field overpowers any response a tag could give, which is why tags reply on side channels that are placed directly below and above the frequency of the continuous wave as shown in Figure 7.

8. Application of RFID Tags

In this section, we have discussed some existing and proposed RFID applications.

8.1. Current RFID Applications

Today RFID technology is considered as enabling

technology in the field of information technology to achieve automation of supply chain management, tracking assets, consignment tracking, animal monitoring, and access control in a contactless fashion, they are listed in Table 2 [1]. RFID is also widely used in the field of medical science for the diagnosis of diseases. Currently, RFID technology is not widespread, but some stores and marts like K-Mart, Wal-Mart, Target, Best Buy, etc. use them extensively [7]. Today IT has discovered that emerging RFID technology can help keep their records at the highest level and reduce loss of stock items, limit burglary, detect shoplifters, and enhance the billing process. One of the special classes of passive RFID tags is powder/dust digestive tags [33, 24]. Digestive tags are used for observing the human digestive system. RFID digestive tags have no side effects and can be

deliberately broken down. Such tags are encapsulated within a soft degradable material called gelatine, it may take a few moments to dissolve in the stomach of the patient. And hence they are biodegradable. The RFID digestible tags very help full for monitoring the digestive system of a human being, operating hip and knee joints, and inspecting some internal organs. Digestive tags do not work properly when they are exposed to gastric acid for a specific period [31]. However, RFID applications are not limited to such an extent, moreover, it has a wide range of applications in other fields too. On the basis and requirement of the business process,

this technique can be adopted in various forms [24]. We can categorize the applications into two major classes: the first one is the system having a short range of communication. When a tag and a reader have to be very close such as in Electronic Immobilization, RFID Cashless payment, access control, etc. The second one is medium for extensive application, here the range could be considerably longer like fleet tracking systems, Toll collection [25]. Innovative manufacturing, modern antenna designs, and increased memory will create smart tags long-lasting which will protect our data with modern cloud-based technologies.

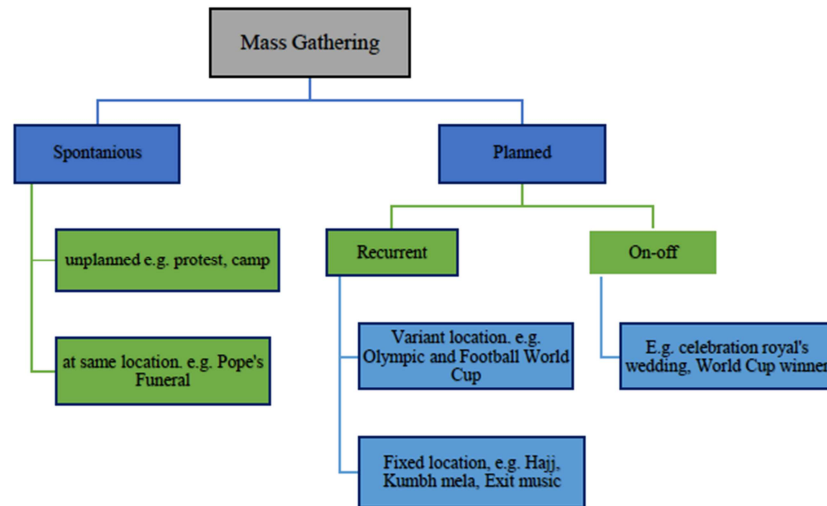


Figure 8. Classification of Mass Gathering (MGs).

Table 2. Application of RFID Tags.

#	RFID Application	RFID Tag Technology
1	Supply Chain Automation	In supply chain management, UHF passive tags are used for consignment tracking.
2	Asset Tracking	Tracing objects in the office, where the house, labs, etc. we use HF and UHF passive tags. Since radio frequencies are absorbed by metal, therefore, a special mechanism is followed to track metallic items.
3	Sporting Events	It is also used to calculate the exact running time in an athlete's ground, tags are simply attached to the shoes of athletes and are a start when athletes start a race.
4	People Tracking	UHF tags are also used to make a system that ensures the presence and absence of victims, convicts, or a worker.
5	RFID Cashless/Wireless	To achieve a wireless digital transaction of funds, pay a bill without cash, and credit the digital account, RFID plays a vital and secure role. [13].
6	Payment	Used for Biometric authentication, monitoring patient activity, tracking drugs or a confidential item, and doing diagnosis by using a Digestive tag is very applicable.
7	Medical Applications	UHF also provides a way to track an item in a real-time inventory by having computerized cataloging of items in a store or a warehouse.
8	Warehouse	In highways, both UHF passive and UHF active tags play a vital role to collect toll tax.
9	Toll Collection	Unlocking a system through a key, RFID technology can be implemented to authenticate the key which is a real one to have a secure ignition of a vehicle.
10	Electronic Immobilization	To track particular kinds or species of animals in a herd, LF tags are used [1].
11	Animal Monitoring	To grant access control in an office, firm, or within a locker in a bank, both Low and High-frequency passive tags are used.

8.2. Proposed RFID Applications in Mass Gathering

The 'context' type of event and risk assessment primarily drives Mass Gathering Management (MGs). There are several potential threats, large and small, predictable and unexpected, that may occur immediately before, during, or after an event or a MGs. A detailed taxonomy of mass gathering is shown in Figure 8.

The type of event will guide the risk assessment and the preparation: Some other applications of RFID tags in mass crowd management are found. Crowd Control and Management, designed to prevent and manage crushes, stampedes, and other disasters. These systems may detect such events beforehand and use cloud computing, fog computing [48] WSN technology [49] smart Digital Street, IP cameras, RFID, voice alarm, light alarm, GPS and

smartphones, and the Internet of Things (IoT) [50].

8.3. Proposed Algorithm

To manage or optimize the degree of mortality rate concerning the size of the crowd, there is only one way to manage, and it is to follow some algorithm that allocates a group of people to some resource on a pre-defined condition, such that the allocation and request are not cyclic and haphazard. Following are some algorithmic approaches that can be implemented to minimize the degree of mortality.

Step I: Hieratical of Processing and Control

Step 1.1: Divide the crowd build-up locations into clusters and continuously allocate the crowd data to the Fog network from the sensor networks for speed processing and further decision-making.

Step 1.2: Every Fog Node will be linked to the center of fogs to monitor the integration between the nodes and ensure data processing before moving it to the cloud. Then it is conducted thorough data analysis to identify new information that would be very useful for disaster prediction and prevention and plan to manage the outcome of a catastrophe if it arises.

Step II: Collecting and Sensing Data

Step 2.1: Attach all passive RFID tags (the low-cost tags) in the form of cards or bracelets to individual bodies to fetch their current location and decide crowd size in each cell/cluster.

Step 2.2: Connect the tag's reader to the Fog node, or distribute several readers in each cell and the host will be in the fog. Tag identification can be used to access other details.

Step 2.3: Deploy different WSNs for sensing parameters, conditions, and circumstances in each cell, to sense temperature, pressure, and neighboring density in each cell of the cluster.

Step 2.4: If GPS and cellular networks are not working, use aircraft or WSN readers drone.

Step 2.5: Use IP-Cameras to predict the possibility of fore coming tragedy in each cell. Tragedy detection can be done by comparing new footage with the previous one.

Step 2.6: Extract people's behavior and degree of panic with these images and take remedial steps if required. Using photos to assess people's moods and take remedial measures should there be any evidence of illness or discomfort.

Step 2.7: In case of a tragedy, send route, precautionary and remedial information to people's mobile or any handheld gadget.

Step III: Decision-Making and Notification

Step 3.1: Create smart streets in disaster-prone areas by installing alarm/light/sound alerts install crowd lifter wagons to lift people/vehicles in case of a deadlock.

Step 3.2: Send light/sound/vibration alert to people about the fore coming tragedy and guide them to follow a safe sequence (a path, waiting for another is to be free, or voluntarily releasing an allocated resource or a request) to avoid a deadlock condition within a cell.

Step 3.3: In case of communication failure or unreachable circumstances, use a surveillance drone to communicate with

a targeted cell of the cluster.

Step IV: Sensitive Data Computation

Step 4.1: Sensors and other management tools can collect, store, clean, refine, and analyze data obtained from sensors. All of this will take place on the cloud, where deep learning and data mining will identify new relationships to better handle future events.

Step 4.2: The performance of this or any other program is proportional to user-management cooperation. In particular, the admin must take note of alerts and updates within the specified time frame and follow their instructions at critical moments.

8.4. Other Possible Applications

1. The Indian Railways have to use RFID tags to track wagons, coaches, and locomotives to ensure efficient and transparent service.
2. RFID tags may be attached to the shirt collar of the school uniform in such a way that it cannot be counterfeited and replicated. When students enter the school's premises, their attendance will automatically be marked by the concept of proximity sensors of the tag, and a notification will be sent to their parents as well as school administrations.

In case of a class bunk or any premises crossing condition, the embedded tag (uniform or shirt worn by the students) will come out from the reader's range. Followed by this situation, a notification will be sent to the school's administration and also to the parent to alert the trespassing of school premises and appropriate action will be taken.

3. In the same way (as said in the point above), the Government of India should also use this technology in their prisons to track and monitor prisoners' activity.
4. RFID technology can also be used in the railway's coach compartments to identify the lifting of luggage. When passengers board a train, he/she must register their luggage identification number (provided by the Indian railway at the time of reservation of seats) to the installed RFID system in each compartment (just like switching on and off a light or fan). It means passengers should simply pair the luggage with the embedded RFID system of their compartment. After a successful pairing, the passenger may enjoy a fear-less journey because when a thief will try to de-attach (steal the luggage) the luggage, the tag or label attached to the luggage will come out of the reader's range, followed by this an alarming sound/light will be triggered in the compartment.

To identify the thief, we can also close the exit door and coach connecting doors of the coach followed by this alert if needed.

9. Security on RFID System

In this section, we have discussed some existing and proposed security solutions for an RFID system.

9.1. Attack Ranges of an RFID System

This section introduces various ranges that turn out to be interesting, concerning the security of an RFID system. Transmission ranges that are discussed above may become intruder range in many cases, it has also seemed that a range that has been declared a safe range may be used to collect information about the tag, or even an eavesdropper can break the security of RFID system within such ranges and frequencies. The following are the five crucial ranges that are discussed and should be taken into account while designing an RFID system [9, 29].

a. Nominal Reading Range

According to the standard, a nominal range is a suitable range for an RFID tag for which it can make communication. A sender can easily communicate along with their all-defined protocol effectively [36].

b. Cad Reading Range

This range has some advantages over the above one, in Rogue Reading Range a modified sender can establish a connection with tags in a very lucid manner, and can also perform some modifications such as propagating any type of signals with more power and frequencies as allowed by the standard. It may also have a high-gain antenna or an array of antennae too [30].

c. Tag to Reader Eavesdropping Range

Listening to a private conversation is a serious issue, in terms of privacy it is called eavesdropping. In this issue, there is a chance that an unintended reader may listen to the transmitted signals when a tag wants to make some response to an intended reader [28]. But it has to be noted that, it's only the passive tags that can involve in such eavesdropping activity. The tag to Reader Eavesdropping Range is always larger than the rough scanning range; this is because the reader need not powered the tag because of the read range limitations [37].

d. Reader to Tag Eavesdropping Range

Misbehaving readers trying to listen to the conversation or the signal emitted by a reader to a tag (or simply a system) which is an authentic one. Since the authentic reader produces a very strong signal to power the intended tag in the network, the misbehaving tag read this transmitted signal from a few kilometers away from the system. It should be noted that here the eavesdropping reader (i.e. the misbehaving reader) is passive in nature and can pose a greater detection range than the previous one. An inappropriate reader who is prepared to track a Tag-to-Reader communication should also track Reader-to-Tag communication, and the whole communication can be completely transcribed [41].

e. Detection Range

In this range, one can easily detect a tag or a reader. However, we cannot capture any intelligible information within this range. A reader can detect signals that are far from a tag, and their detection range may be used in the Department of Defense that needed item-level tagging [10, 42].

9.2. Attacks Against RFID Systems

This section explains varieties of several attacks that could penetrate the RFID tags and the exploits that an RFID system may suffer from. Many attacks targeting RFID communication are not limited to a single layer. In this category, the attacks that affect multiple layers of the OSI model are the physical layer, networks layer, applications layer, and other strategic layers. It covert networks, infrastructure denial, and study of traffic, and as a result, it reveals the channel utilization, physical information, traffic records, and other sensitive information. Thus, crypto side-channel attacks are especially included in this layer. We define these attacks as well as ways of defending against them. We primarily offer eight attacks against RFID tags as mentioned below.

a. Sniffing and Eavesdropping

To abstain from the implementation of expensive algorithms, lack of resources for encryption & decryption, abstain from sharing the keys, etc., most of the system prefers to have text communication and becomes the victim of a powerful attack called Sniffing [23, 24]. By using a Sniffing attack one can retrieve a lot of information from a conversation. Even a simple RFID tag does not have any protection wall against such attacks that are acted by a misbehaving reader. Hence eavesdroppers may use the stolen information to threaten the intended recipients [37].

b. Tracking

As we have seen earlier, the tracking activity can collect and correlate stolen information as much as possible; tracking seems very effective when item-level tagging presents everywhere simultaneously, and hence one can easily create a precise profile of a customer. Tracking leads to a robust loss of privacy.

c. Spoofing

A blank tag is used to copy the secured stolen information of a targeted tag while the tag has been authenticated by an intended reader. This happens because many tags in the market do not support prior authentication while establishing a secure connection with their intended recipients. This is the main reason that an attacker can steal and alter its secured information lucidly by saving the stolen data into a new blank tag, they use it for future undesirable purposes [43]. After the new tag has been initialized with stolen information, the attacker then replaces the new tag with an identical tag whose cost is much higher. The retagged item is then authenticated at the billing desk and the attacker just had to pay only for a cheaper one [21].

d. Replay

After seizing the conversation between a tag and an intended reader, the attacker then waits for a while, after that, a response made by an intended tag has been saved by the attacker, and then reused while receiving a query from the intended reader. For instance, the conversation made by a proximity card with their Entrance Access Reader (EAR) is recorded, and then played again at the end of the authentication session has lapsed. Another situation arises

when someone can record a response made by a car on an automated toll collection outlet and then use it (the stolen response) when it passes through a checkpoint to be exempted from paying toll tax [22, 25]. These attacks can be resolved by implementing the Challenge-Response Protocol (CRP).

e. Denial of Service

There are several forms in which this attack works. One of them is performed by clogging the frequencies utilized by the RFID system, thus making conversation difficult. This attack is also termed Unauthorized tag Disabling. The prime objective of the attacker is to turn an RFID tag into a form, such that the intended tag is assumed in a state that is not functioning properly. This results in the tag becoming either temporarily or permanently injured. When a tag completely wraps into a metal foil, it is isolated permanently and cannot make a request or a response. Isolation also results in the RFID system not receiving enough energy to respond to a request or reply to a query [44]. This technique is often used by attackers to disable Electronic Article Surveillance (EAS) tags. A more manual intensive attack has seemed as an anti-RFID activist may attach an arbitrary label on intended items, and hence the RFID system then gather garbage data, and attackers achieve their target to discredit and defame the RFID technology because it breaks the privacy [26, 35].

f. Malware and Virus

We all are fully aware of the attack of a virus on IT appliances and systems, RFID is also not free from this threat. RFID viruses are the traditional SQL injection that tries to exploit the targeted database [11, 23]. Virus directly targets the backend database of the RFID system since all the information read from tags is stored in the database.

g. Covert Channels

Attackers can exploit RFID tags to establish unauthorized channels of communication to covertly transfer information. Adversaries can take advantage of the unused storage memory of multiple RFID tags to securely transfer data in a manner that is hard to detect [45]. A collection of RFID tags implanted in human bodies, for example, whose main function would be to identify an individual, may secretly disclose private information relating to medical details or social activities.

h. Traffic Analysis

RFID communication is vulnerable to attacks from traffic analysis. An eavesdropper can intercept communications, and extract information from a pattern of communication. Even if the RFID correspondence is secured by encryption and authentication methods, it is still vulnerable to attacks on traffic analysis. The greater the number of messages intercepted, the more successful a traffic analysis would be [46]. A complete summarized list of more often vulnerable attacks with their corresponding examples is listed in Table 3.

Table 3. Application of RFID Tags.

Vulnerability	Description
Cost	The manufacturing cost of an RFID tag and implementation of an RFID system may restrict the degree of privacy as well as security control.
Counterfeiting or Decoy	Reading confidential data from an RFID tag is quite possible and creating an identical duplicate tag
Denial of service (DOS)	Attackers try to disrupt the communication between the tag and the reader. One way to achieve this service of attack is to connect several tags in the system. This will result in the reader being unable to differentiate the different tags.
Eavesdropping	Eavesdropper trying to listen to a private conversation between the reader and the tag.
Physical Attack	Tampering with RFID tags may leave them invalid (e.g., fault induction, timing, and power analysis attacks)
Spoofing	The attacker creates a new tag and tries to replace it with the targeted real tag.
Traffic Analysis	In this technique, an attacker tries to scale the data transfer rate to analyze the exact location of the targeted tag.

9.3. Current Security Solutions of RFID System

It explains the strategies that are used to beat all those attacks that make an RFID tag vulnerable. After that, this section discussed all those attacks which are taken against the RFIS system. Since RFID equipment turns into more stylish and product stage tagging guarantees greater control and a big reduction in supply chain management, firms also used to tag their product to protect their manufacturing product from unauthorized access. To get a large profit, firms also made it mandatory for almost all products that are shipped to a corporation. For instance, Wall-Mart, Examiner and Glory, and the US Defence Department called upon respective suppliers to promote product-level tagging [23, 25]. Even so, besides the goods and the objects, animal tagging is pretty popular in big farming for monitoring the activity of an animal in a herd. Additionally, the tagging of human beings has also been seen. Anti-RFID activists develop some situations to exhibit feasible exploits if any measures are not

used [35]. The best-known one is the felonious scanning of tags to generate the end user's profile. Some other situations are, scanning the drugs of one that contains conjecture just to identify what disease the individual might be suffering. Or even a robber can scan a group of people and identify the person who is carrying precious items [21, 46].

9.4. Possible Security Solution for RFID System

The protection and privacy concerns surrounding RFID are discussed in many ways. They can be grouped into:

1. Tag Data Security
2. Maintaining Reader Integrity
3. Personal Privacy
4. Improved Hash Lock

9.4.1. Solutions for Tag Data Security

In this section we have discussed some points related to the security of RFID tag data, they are:

- a. Password Protection on Tag Memory

We may use a long alphanumeric password to encrypt the tag's embedded data, which prevents anyone from reading the tags without the intended owner's consent. Nevertheless, if all tags have identical passwords, the data become essentially public when the tag does not have any password. However, there may be millions of passwords that must be indexed every day, but a brute comparison will be required to meet the valid tag data and its associated metadata.

b. Physical Locking of Tag Memory

The tag provider may protect the sensitive tag data such as a unique identifier, and session ID into the tags before releasing it. In other words, we must embed the essential prerequisite information of the tag data during the production time and set the memory type of the tag as read-only, so that no further modifications are to be done. By doing so, we can verify that, whether the tag is original or not. The only problem associated with this approach is that the tag's data further cannot be updated. However, this problem can be resolved by having an additional memory attached to the tag.

c. Authentication of the "manufacturer" in tag memory

We should encrypt the tag data by using a private key which is referred to as the digital sign process of the tag, and save the encrypted data into additional auxiliary memory associated with the manufacturer's name. Which will serve as a reference to the public key and for the algorithm used in a non-encrypted fashion. To check the validity of the encrypted data, a reader must compare the manufacturer's name and other non-encrypted information on the tag to check whether the fetched information is matching with the information provided by the intended manufacturer or not. However, if the RFID reader wants to update the embedded tag information with a new one, then there must require a key management technique to establish the session.

9.4.2. Solutions for RFID Readers' Integrity

In this section we have discussed some points related to the security of reader's data, they are:

a. Reader Protection

A Reader may deny tag responses as per the anomalies found in response time, attenuation, frequency fluctuations, irregular response, and other factors that do not match the tag's intended physical properties [26]. This technique may avoid traffic delays, spoofing, and eavesdropping on the tag's reader communication. A reader may also generate a frequency of variant bandwidth and program the tag to respond only at a pre-defined value of the bandwidth of the reader. By doing so, third parties (except for a valid tag) cannot sense the frequency emitted by the reader. Hence the system can be protected from a side-channel attack.

b. Read Detectors

Custom firmware can be mounted in an RFID system to monitor unauthorized requests of a read. Such read detectors can be used to detect an unauthorized read or write request for tag data [28].

9.4.3. Solutions for Personal Privacy

In this section we have discussed some points related to the security of reader's data, they are:

a. Kill the tag

We can completely "disable" an RFID tag by executing a "kill" command to the read-only content of the tag data. This will ensure that the tag will never be re-activated. Executing the "kill" command will disconnect the tag connection from their antenna, as a result, it cannot be detected even if it comes close to the reading range. By doing so, we can protect the sensitive data (such as bank details, ATM PIN, etc.) of a customer who has purchased the product. However, there may be some cases where tags may not be killed. For example, when a customer wants to return or exchange a purchased product, then the retailer will have to re-activate the tag to fetch the sold information [47].

b. Faraday Cage

An RFID tag with metal mesh or a foil jar can be used to block radio waves of a certain frequency and is referred to as a "Faraday Cage" [28]. Set the intended reader with a pre-defined frequency to communicate with the tag. By doing so, we can curb the concurrent tag detection to avoid the correlation attack [29].

c. Active Jamming

Active jamming of RF signals refers to the use of a radio signal device to intentionally confuse any RFID user. This form of physical defense could also unintentionally disrupt the surrounding RFID systems [12, 45]. The use of such a device, though, could be unconstitutional, based on the system's transmitting capacity and the government laws, as all surrounding RFID devices are at risk of severe disruption if the jamming power is too high.

9.4.4. Improved Hash Lock

A hash lock is a customized hash function that is used to ensure the communication between a tag and the reader has been established or not. It is being used to achieve the state of locking and unlocking of request and response flags to secure and achieve atomicity in connection. But the issue of the privacy leak and the middle RFID attack are easily encountered in this technique [44]. This section proposed a novel approach called *Random Hash Function 'H'* to improve the performance of the existing hash function $h(x)$. We have implemented the 'H' in two variants/overloaded signatures, the $H(\bullet) \forall \bullet \in \{TagID_i\}$ and the $H(\bullet, \mu) \forall \mu \in \{ReaderID_k\}$ is used to solve these problems. The proposed method works fine and can be implemented in a system having at most 25000 tags. In the subsequent section (sections (a), (b), and (C) of 9.4.4) the working principle of the Random Hash Function H, Reader Certification of H, and update state mechanism of TagID and ReaderID has been discussed. However, the proposed method has some limitations with large networks of tags, which are discussed in section 9.4.4.1.

a. Working Principle

In this approach, the unique identification number of tags (TagID) and readers (ReaderID) are maintained by each other. It means the tag will have the ReaderID of a reader and vice versa. Suppose there are several readers and many tags present in a network, and a reader sends a request to get a

ReaderID, then the reader may get the same or different ReaderID in response. On getting the same ReaderID, there is no problem so far, but if the reader gets a different ReaderID as a response, then we will verify the identity of this reader. Since each tag is associated with some ReaderID, thus we will maintain a lookup Table (refer to Figure 9) of TagID corresponding to their intended ReaderID. So, on

getting a different ReaderID as a response, the control immediately transfers (refer to edge 1.2 of Figure 9) on the lookup Table to get a TagID to correspond to the response ReaderID (R101 in this case). So it is the tags that will decide whether a reader has verified or not. The complete scenario is shown in Figure 9.

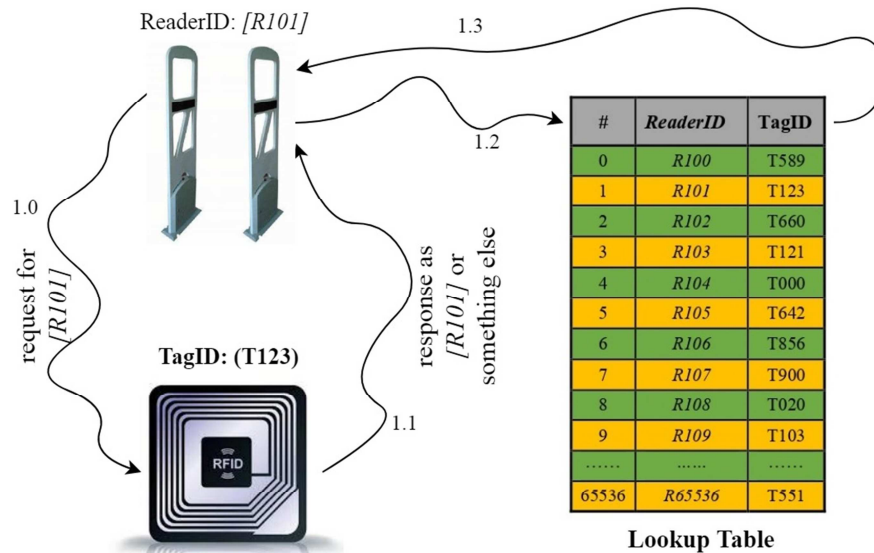


Figure 9. Working principle of the randomized hash function 'H'

b. Reader Certification

Before responding to a reader, the readers and tags decide the certification process, and let the reader obtain the TagID. As the reader's ReaderID is completely stored in the tag's auxiliary memory, the responsible reader gets identified by tag through this ReaderID. Since a tag does not reply without the prior permission of a reader, thus an eavesdropper cannot monitor the session activity. Moreover, this method of controlling the authority is based on PRNG so it would also help the opponent to disguise their attempt. If a reader request has been received by the RFID tag, a random number k is generated and transmitted to the reader, on receiving it, the reader sends it back to the reader database, which computes whether the $H(\text{TagID}) = H(\text{ReaderID}, \text{QUEUE})$ and sends $H(\text{TagID})$ back to the reader, the reader transmits $H(\text{TagID})$ to the mark. RFID tags also measure $H(\text{ReaderID}, \text{NEW})$, but tags then compare an $H(\text{TagID})$ and whether the reader values are equal or not. The reader passes the certification if equal, and the label will give it some relevant TagID information; if not equal, the reader is not certified to be shielded. *Get TagID: is responded to the Hash Authentication reader (TagID) after reader certification.* If the $H(\text{TagID})$ value is obtained by the reader, the reader interacts with the backend database and searches for the data $H(\text{TagID}, H(\text{TagID}))$, and the readers get the TagID. The eavesdropper does not know the value of the $H(\text{TagID})$ even though the mark sends its value because it cannot decide the relationship between TagID and $H(\text{TagID})$.

c. TagID and ReaderID Update

During the transformation of an item from one place to another place, the intended reader (before transfer) also shift from the old to a new place. Now, the new reader starts to access the $H(\text{TagID})$ value of the moving tag and continuously saves it to the Hash Table (or lookup Table) of the database. The Hash Table contains a list of ReaderID corresponding to each TagID and starts comparing for a valid match. After getting a proper match (when a valid ReaderID is obtained TagID for a moving tag), this new ReaderID is assigned and transferred to the new reader. When this reader receives the New ReaderID, then we will XOR the ReaderID and OldReaderID together and the XOR value is sent to the RF tag. By doing so, we can get the following advantages.

Since an opponent eavesdropper can produce $H(\text{TagID})$ during the certification process, it is unable to validate it, as we have to continuously change the hash value $H(\text{TagID})$ at each time of the certification, the older value of certification is becoming meaningless for the newer one. When the certification process is over, the tag will output a hash value $H(\text{TagID})$ instead of a TagID. Since a hash function $H(\bullet)$ is a one-way trapdoor function, thus their reverse engineering is impossible. So even if an opponent gets the $H(\text{TagID})$ (a hash value) then he cannot convert it into the corresponding TagID. In short, even after successful eavesdropping between a tag and a reader, the TagID cannot be determined.

Limitation of $H(\bullet)$ and $H(\bullet, \mu)$

Due to the space and time complexity of the proposed Random Hash Function 'H', the approach is found suitable for a network having at most 25000 tags connected to

exchange data concurrently.

10. Conclusion and Future Work

The paper highlights the theory and practical need for an RFID system, its design, architecture, working principles, and application along with the associated limitations. Although the wide use of RFID is still stuck by various limitations and unresolved issues. To develop and implement efficient sensor-based IT solutions, we have provided the possible use-case and implementation of the RFID system in more possible aspects. Besides the current applications, to manage the degree of fatality concerning crowd size, *a novel approach has been proposed (in sub-section 8.3), that will help in managing any mass gathering, risk assessment, and detecting the fore coming tragedy.* In this section, other possible RFID applications are for the Indian railway to manage and track the current location of the train, and provide passenger luggage protection inside the railway coach. Apart from this, school student/employee tracking and other confined methodologies have been proposed. When RFID systems are more commonly deployed, security becomes a major concern and till now several cryptographic attacks have been reported like DOS, DDOS, replay and monitoring, side-channel attacks, etc. We have discussed some other use cases where attacks are easily made to reveal the sensitive data and internal state of the system. To improve the results of the existing security solution, a novel approach for tag and reader data protection has been provided in section 9. *The section provides an astute algorithmic approach called a randomized hash function which uses a lookup table to implement the proposed algorithm (refer to section 8.3) and seems to be more secure against the above-mentioned well-known cryptographic attacks.*

References

- [1] Camacho-Cogollo, Javier Enrique, Isis Bonet, and Ernesto Iadanza. "RFID technology in health care." *Clinical Engineering Handbook*. Academic Press, 2020. 33-41.
- [2] Elbasani, Ermal, Pattamaset Siriporn, and Jae Sung Choi. "A Survey on RFID in Industry 4.0." *Internet of Things for Industry 4.0*. Springer, Cham, 2020. 1-16.
- [3] Papapostolou, Apostolia, and Hakima Chaouchi. "Exploiting multi-modality and diversity for localization enhancement: WiFi & RFID usecase." 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications. IEEE, 2019.
- [4] Monico, Dominick L. "Low cost long distance RFID reading." U. S. Patent No. 6, 259, 369. 10 Jul. 2001.
- [5] Dastoori, K., B. Makin, and S. Bappoo. "The effectiveness of passive RFID Tags in the presence of charged particles." *Journal of Electrostatics* 67.2-3 (2009): 468-472.
- [6] Liu, Yali, Martianus Frederic Ezerman, and Huaxiong Wang. "Double verification protocol via secret sharing for low-cost RFID Tags." *Future Generation Computer Systems* 90 (2019): 118-128.
- [7] Mitra, Mala. "Privacy for RFID systems to prevent tracking and cloning." *International Journal of Computer Science and Network Security* 8.1 (2008): 1-5.
- [8] Jeong, Soyeon, et al. "Read/Interrogation Enhancement of Chipless RFIDs Using Machine Learning Techniques." *IEEE Antennas and Wireless Propagation Letters* 18.11 (2019): 2272-2276.
- [9] Al-Shaery, Ali M., Mohamed O. Khozium, Norah S. Farooqi, Shroug S. Alshehri, and Mohammad Adnan MB Al-Kawa. "Problem solving in crowd management using heuristic approach." *IEEE Access* 10 (2022): 25422-25434.
- [10] Hussain, Muzammil, and Arshad Hashmi. "SECURITY THREATS IN IOT VIA LAYERED ARCHITECTURE." *International Journal of Future Generation Communication and Networking* 12.5 (2019): 173-185.
- [11] Shariq, Mohd, and Karan Singh. "A vector-space-based lightweight rfid authentication protocol." *International Journal of Information Technology* 14, no. 3 (2022): 1311-1320.
- [12] Sklovsky, Vladimir, Ruben R. Formoso, and Lyle A. Gastra. "Method and system for monitoring secure application execution events during contactless RFID/NFC communication." U. S. Patent No. 10, 311, 427. 4 Jun. 2019.
- [13] Ke, Qiao, Jakub Silka, Michał Wiecezorek, Zongwen Bai, and Marcin Woźniak. "Deep neural network heuristic hierarchization for cooperative intelligent transportation fleet management." *IEEE Transactions on Intelligent Transportation Systems* 23, no. 9 (2022): 16752-16762.
- [14] Gao, Ming, and YuBin Lu. "URAP: A new ultra-lightweight RFID authentication protocol in passive RFID system." *The Journal of Supercomputing* 78, no. 8 (2022): 10893-10905.
- [15] Shariq, Mohd, Karan Singh, Pramod Kumar Maurya, Ali Ahmadian, and David Taniar. "AnonSURP: an anonymous and secure ultralightweight RFID protocol for deployment in internet of vehicles systems." *The Journal of Supercomputing* (2022): 1-26.
- [16] Alajami, Abdussalam A., Guillem Moreno, and Rafael Pous. "A ROS Gazebo Plugin Design to Simulate RFID Systems." *IEEE Access* 10 (2022): 93921-93932.
- [17] Ahsan, Kamran, Hanifa Shah, and Paul Kingston. "RFID applications: An introductory and exploratory study." *arXiv preprint arXiv: 1002.1179* (2010).
- [18] Welbourne, Evan, et al. "Building the internet of things using RFID: the RFID ecosystem experience." *IEEE Internet computing* 13.3 (2009): 48-55.
- [19] Nunes-Silva, P., et al. "Applications of RFID technology on the study of bees." *Insectes sociaux* 66.1 (2019): 15-24.
- [20] Nikooghadam, Mahdi, Hamid Reza Shahriari, and Saeid Tousi Saeidi. "HAKECC: Highly efficient authentication and key agreement scheme based on ECDH for RFID in IOT environment." *Journal of Information Security and Applications* 76 (2023): 103523.
- [21] Kumar, Vikas, Rahul Kumar, Akber Ali Khan, Vinod Kumar, Yu-Chi Chen, and Chin-Chieh Chang. "RAFI: robust authentication framework for IoT-based RFID infrastructure." *Sensors* 22, no. 9 (2022): 3110.

- [22] Tewari, Aakanksha, and B. B. Gupta. "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID Tags." *The Journal of Supercomputing* 73.3 (2017): 1085-1102.
- [23] Shen, Han, et al. "Efficient RFID authentication using elliptic curve cryptography for the internet of things." *Wireless Personal Communications* 96.4 (2017): 5253-5266.
- [24] Shuyu, Chen, and Yan Limin. "A low-overhead PUF for anti-clone attack of RFID tags." *Microelectronics Journal* 126 (2022): 105497.
- [25] Hernandez-Castro, Julio Cesar, et al. "Cryptanalysis of the David-Prasad RFID ultralightweight authentication protocol." *International Workshop on Radio Frequency Identification: Security and Privacy Issues*. Springer, Berlin, Heidelberg, 2010.
- [26] Wang, Xingmiao, Kai Fan, Kan Yang, Xiaochun Cheng, Qingkuan Dong, Hui Li, and Yintang Yang. "A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living." *Computer Communications* 186 (2022): 121-132.
- [27] Bowers, John H., and Thomas J. Clare. "Rfid Tags which are virtually activated and/or deactivated and apparatus and methods of using same in an electronic security system." U. S. Patent No. 6, 025, 780. 15 Feb. 2000.
- [28] Feldhofer, Martin. "An authentication protocol in a security layer for RFID smart Tags." *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (IEEE Cat. No. 04CH37521)*. Vol. 2. IEEE, 2004.
- [29] Sadiku, Matthew NO, Abayomi J. Ajayi-Majebi, and Philip O. Adebo. "Ubiquitous Manufacturing." In *Emerging Technologies in Manufacturing*, pp. 215-231. Cham: Springer International Publishing, 2023.
- [30] Mertler, Craig A., and Rachel Vannatta Reinhart. *Advanced and multivariate statistical methods: Practical application and interpretation*. Taylor & Francis, 2016.
- [31] Glidden, Rob, et al. "Design of ultra-low-cost UHF RFID Tags for supply chain applications." *IEEE Communications Magazine* 42.8 (2004): 140-151.
- [32] Gope, Prosanta, Yuening Wang, Zengpeng Li, and Biplab Sikdar. "QR-PUF: Design and Implementation of A RFID-based Secure Inpatient Management System Using XOR-Arbiter-PUF and QR-Code." *IEEE Transactions on Network Science and Engineering* (2022).
- [33] Vena, Arnaud, et al. "Design of chipless RFID Tags printed on paper by flexography." *IEEE Transactions on Antennas and Propagation* 61.12 (2013): 5868-5877.
- [34] Leong, Kin Seong, Mun Leng Ng, and Peter H. Cole. "Investigation on the deployment of HF and UHF RFID Tag in livestock identification." *2007 IEEE Antennas and Propagation Society International Symposium*. IEEE, 2007.
- [35] Brito, Jerry. "Relax, don't do it: Why RFID privacy concerns are exaggerated and legislation is premature." *UCLA JL & TECH*. 2004 (2004): 5.
- [36] Kim, Do-Yun, et al. "Effects of reader-to-reader interference on the UHF RFID interrogation range." *IEEE Transactions on Industrial Electronics* 56.7 (2019): 2337-2346.
- [37] Kortvedt, Henning, and S. Mjolsnes. "Eavesdropping near field communication." *The Norwegian Information Security Conference (NISK)*. Vol. 27. 2009.
- [38] Hussien, Naseer Ali, et al. "Smart Shopping System with RFID Technology Based on Internet of Things." *International Journal of Interactive Mobile Technologies (IJIM)* 14.04 (2020): 17-29.
- [39] Brand, Timothy K. "Antenna system and method for reading low frequency Tags." U. S. Patent No. 6, 750, 771. 15 Jun. 2014.
- [40] Egbert, William C. "Ultra high frequency radio frequency identification Tag." U. S. Patent No. 7, 215, 295. 8 May 2017.
- [41] Mohammad, Gouse Baig, Shitharth Shitharth, Salman Ali Syed, Raman Dugyala, K. Sreenivasa Rao, Fayadh Alenezi, Sara A. Althubiti, and Kemal Polat. "Mechanism of internet of things (IoT) integrated with radio frequency identification (RFID) technology for healthcare system." *Mathematical Problems in Engineering* 2022 (2022): 1-8.
- [42] Whitesmith, Howard William, Timothy John Palmer, and Alan Edward Ball. "RFID detection system." U. S. Patent No. 6, 577, 238. 10 Jun. 2013.
- [43] Khan, Muhammad Ayaz, Subhan Ullah, Tahir Ahmad, Khwaja Jawad, and Attaullah Burio. "Enhancing Security and Privacy in Healthcare Systems Using a Lightweight RFID Protocol." *Sensors* 23, no. 12 (2023): 5518.
- [44] Fu, Yongqing, Chun Zhang, and Jingchao Wang. "A research on Denial of Service attack in passive RFID system." *2010 International Conference on Anti-Counterfeiting, Security and Identification*. IEEE, 2010.
- [45] Puica, Elena. "Improving Supply Chain Management by Integrating RFID with IoT Shared Database: Proposing a System Architecture." In *IFIP International Conference on Artificial Intelligence Applications and Innovations*, pp. 159-170. Cham: Springer Nature Switzerland, 2023.
- [46] Mtita, Collins, Maryline Laurent, and Jacques Delort. "Efficient serverless radio-frequency identification mutual authentication and secure Tag search protocols with untrusted readers." *IET Information Security* 10.5 (2016): 262-271.
- [47] Ngai, Ka Ming, et al. "Human stampedes: a systematic review of historical and peer-reviewed sources." *Disaster medicine and public health preparedness* 3.4 (2019): 191-195.
- [48] Turksonmez, Halit, and Mehmet Hilal Ozcanhan. "ENHANCING SECURITY OF RFID-ENABLED IOT SUPPLY CHAIN." *Malaysian Journal of Computer Science* 36, no. 3 (2023): 289-307.
- [49] Grace, R. Kingsy, and S. Manju. "A Comprehensive Review of Wireless Sensor Networks Based Air Pollution Monitoring Systems." *Wireless Personal Communications* 108.4 (2019): 2499-2515.
- [50] Wei, Guo-heng, Yan-lin Qin, and Wei Fu. "An improved security authentication protocol for lightweight RFID based on ECC." *Journal of Sensors* 2022 (2022).