Security of Internet of Things (IoT)

Amjad Mahfoud (amjad_94155@svuonline.org) *Master in Web Science - Syrian Virtual University*

***Abstract* - Internet of Things (IoT) has been a major research topic for almost a decade now, lead by the idea of connecting everything into one huge connected network giving objects the ability to communicate and interact. IoT is rapidly developing; however there are uncertainties about its security and privacy which could affect its sustainable development. This paper discusses IoT infrastructure, application, security and privacy.**

Index Terms* - *Internet Of Things, Security, Cloud Computing, Privacy.

I. Introduction

The Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals, The term, Internet of Things a system of interconnected devices was first proposed by Kevin Ashton in 1999 [1]. It is a major technological revolution that has updated the current Internet infrastructure to a concept of much more advanced computing network where all the physical objects around us will be uniquely identifiable and ubiquitously connected to each other [2] throughout a Cloud infrastructure.

II. Technical Background

A. Identification, sensing and communication technologies

‘‘Anytime, anywhere, anymedia” has been for a long time the vision pushing forward the advances in communication technologies [3].To achieve this a reduction in device size was needed to be achieved which lead to creating RFID tags, Tags are characterized by a unique identifier and are applied to objects (even persons or animals). Readers trigger the tag transmission by generating an appropriate signal, which represents a query for the possible presence of tags in the surrounding area and for the reception of their IDs.

Accordingly, RFID systems can be used to monitor objects in real-time, without the need of being in line-of-sight; this allows for mapping the real world into the virtual world. Therefore, they can be used in an incredibly wide range of application scenarios, spanning from logistics to e-health and security.

From a physical point of view a RFID tag is a small microchip attached to an antenna (that is used for both receiving the reader signal and transmitting the tag ID) in a package which usually is similar to an adhesive sticker. Dimensions can be very low: Hitachi has developed a tag with dimensions 0.4 mm 0.4 mm 0.15 mm [3].

Usually, RFID tags are passive, i.e., they do not have onboard power supplies and harvest the energy required for transmitting their ID from the query signal transmitted by a RFID reader in the proximity. In fact, this signal generates a current into the tag antenna by induction and such a current is utilized to supply the microchip which will transmit the tag ID. Usually, the gain (power of the signal received by the reader divided by the power of the signal transmitted by the same reader) characterizing such systems is very low. However, thanks to the highly directive antennas utilized by the readers, tags ID can be correctly received within a radio range that can be as long as a few meters. Transmission may occur in several frequency bands spanning from low frequencies (LF) at 124– 354 kHz up to ultra high frequencies (UHF) at 860– 960 MHz that have the longest range [3].

Sensor networks consist of a certain number (which can be very high) of sensing nodes communicating in a wireless fashion. Usually nodes report the results of their sensing to a small number (in most cases, only one) of special nodes called sinks. A large scientific literature has been produced on sensor networks in the recent past, addressing several problems at all layers of the protocol stack [3]. Design objectives of the proposed solutions are energy efficiency (which is the scarcest resource in most of the scenarios involving sensor networks), scalability (the number of nodes can be very high), reliability (the network may be used to report urgent alarm events), and robustness (sensor nodes are likely to be subject to failures for several reasons).

Today, most of commercial wireless sensor network solutions are based on the IEEE 802.15.4 standard, which defines the physical and MAC layers for low-power, low bit rate communications in wireless personal area networks (WPAN) [3]. IEEE

802.15.4 does not include specifications on the higher layers of the protocol stack, which is necessary for the seamless integration of sensor nodes into the Internet. This is a difficult task for several reasons, the most important are given below [3]:

- Sensor networks may consist of a very large number of nodes. This would result in obvious problems as today there is a scarce availability of IP addresses.
- The largest physical layer packet in IEEE 802.15.4 has 127 bytes; the resulting maximum frame size at the media access control layer is 102 octets, which may further decrease based on the link layer security algorithm utilized. Such sizes are too small when compared to typical IP packet sizes.
- In many scenarios sensor nodes spend a large part of their time in a sleep mode to save energy and cannot communicate during these periods. This is absolutely anomalous for IP networks.

Sensing RFID systems will allow to build RFID sensor networks [3], which consist of small, RFID-based sensing and computing devices, and RFID readers, which are the sinks of the data generated by the sensing RFID tags and provide the power for the network operation.

B. IoT Infrastructure

Generally, IoT has four main key levels [4] as shown in Fig. 1, which are described below

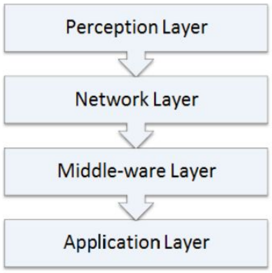

Fig. 1. Generic Architecture of IoT [4].

- **Perception Layer:**
  This layer consists of different kinds of data sensors like RFID, NFC, Barcodes or any other sensor network . The basic purpose of this layer is to identify the unique objects and deal with its collected data obtained from the real world with the help of its respective sensor(s) [4].
- **Network Layer**
  The purpose of this layer is to transmit the gathered information obtained from the perception layer, to any particular information processing system through existing communication networks like Internet, Mobile Network or any other kind of reliable network [4].
- **Middleware Layer**
  This layer consists of information processing systems that take automated actions based on the results of processed data and links the system with the database which provides storage capabilities to the collected data. This layer is service-oriented which ensures same service type between the connected devices [4].
- **Application Layer**
  This layer realizes various practical applications of IoT based on the needs of users and different kinds of industries such as Smart Home, Smart Environment, Smart Transportation even Smart Cities.

B. IoT Middleware

The middleware is a software layer or a set of sub-layers interposed between the technological and the application levels. Its feature of hiding the details of different technologies is fundamental to exempt the programmer from issues that are not directly pertinent to her/his focus, which is the development of the specific application enabled by the IoT infrastructures. The middleware is gaining more and more importance in the last years due to its major role in simplifying the development of new services and the integration of legacy technologies into new ones. This exempts the programmer from the exact knowledge of the variegate set of technologies adopted by the lower layers [3].

As it is happening in other contexts, the middleware architectures proposed in the last years for the IoT often follow the Service Oriented Architecture (SOA) approach. The adoption of the SOA principles allows for decomposing complex and monolithic systems into applications consisting of an ecosystem of simpler and well-defined components. The use of common interfaces and standard protocols gives a horizontal view of an enterprise system. Thus, the development of business processes enabled by the SOA is the result of the process of designing work-flows of coordinated services, which eventually are associated with objects actions. This facilitates the interaction among the parts of an enterprise and allows for reducing the time necessary to adapt itself to the changes imposed by the market evolution [3].

A SOA approach also allows for software and hardware reusing, because it does not impose a specific technology for the service implementation [3].

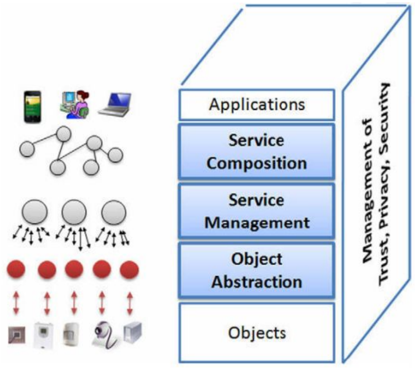

Fig. 2. SOA-based architecture for the IoT middleware.

C. IoT Types

There are four types of IoT in general, as discussed below:

- **Centralized IoT.** A Centralized Internet of Things (Fig. 3 A). In this scenario, the data acquisition networks (i.e. networks of things such as mobile phones, radiation sensors, and cars) are passive: their only task is to provide data. All this data will be retrieved by a single central entity, which will process it into information, combine it, and provide it to its customers. Consequently, if users want to make use of IoT services, they must connect through the Internet to the interfaces provided by this central entity. Note that there are various strategies to implement this approach. For example, the central entity can be instantiated using a simple server or a cluster of devices forming a cloud. Also, its interfaces can provide both raw and preprocessed data, enabling the creation of more complex 3rd party services [5].
- **Collaborative IoT.** While in this approach the 'intelligence' of the network is still located within the central entities (data acquisition networks still behave as passive entities, users access the information through the central entity interfaces), the main difference with a centralized IoT is its compliance with the collaboration principle. As a result, there are various central entities that can exchange data and/or information with each other, generating new services or enriching existing ones (Fig. 1B). For example, IoT service providers that analyze the radiation in the atmosphere of different cities can collaborate in order to provide a snapshot of the radiation levels in the whole country [5].
- **Connected Intranets of Things.** In this approach, data acquisition networks (Intranets of Things) can actually process local information, and also provide it not only to central entities but also to local and remote users (Fig. 1C). However, there are no underlying mechanisms (e.g. discovery services, ontologies) that facilitate the collaboration between entities. As a result, the information mainly flows from the intranets to a central entity, which will be able to provide a holistic point of view of the whole system. For example, IoT-enabled hospitals need to access the services of a central IoT entity to obtain global information (e.g. overall bed occupancy). Note, however, that if the central entities fail, the local services (e.g. the vital signs records of local patients) can still be accessed [5].
- **Distributed IoT.** In this vision, all entities can have the ability to retrieve, process, combine, and provide information and services to other entities (Fig. 1D). Intranet of things (ranging from personal area networks (PANs) to smart city infrastructures) evolve from isolated entities to fully interconnected systems, not only providing services at a local level but also collaborating with each other and with other IoT architectures towards common goals. Observe that it is also possible to integrate higher-level cloud-based services or other centralized entities (e.g. data repositories) within this architecture, but they are not required. Following the e-health example highlighted above, the IoT of a hospital can

interact with the IoT located in the household of a patient, or even with the PANs of the personnel located inside the premises. Moreover, all hospitals can easily collaborate so as to obtain the overall bed occupancy [5].

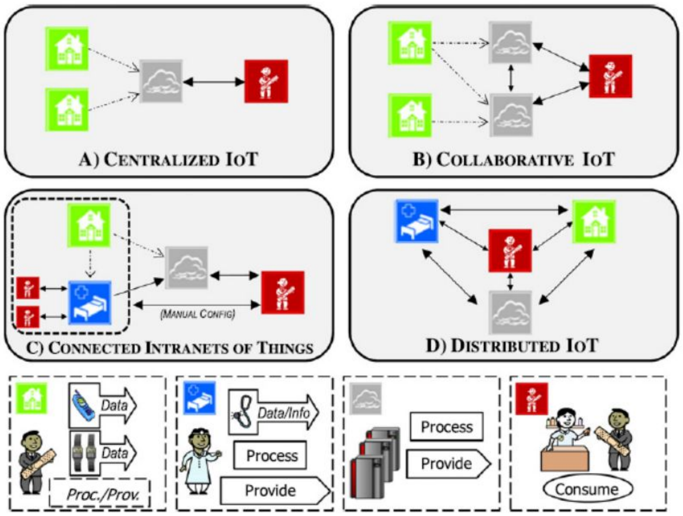

Fig. 3. Overview of the centralized and distributed approaches[5].

III. IoT Usage and Applications

Potentialities offered by the IoT make possible the development of a huge number of applications, of which only a very small part is currently available to our society. Many are the domains and the environments in which new applications would likely improve the quality of our lives: at home, while travelling, when sick, at work, when jogging and at the gym, just to cite a few. These environments are now equipped with objects with only primitive intelligence, most of times without any communication capabilities. Giving these objects the possibility to communicate with each other and to elaborate the information perceived from the surroundings imply having different environments where a very wide range of applications can be deployed. These can be grouped into the following domains:

- **Transportation**
  Advanced cars, trains, buses as well as bicycles along with roads and/or rails are becoming more instrumented with sensors, actuators, and processing power. Roads themselves and transported goods are also equipped with tags and sensors that send important information to traffic control sites and transportation vehicles to better route the traffic, help in the management of the depots, provide the tourist with appropriate transportation information, and monitor the status of the transported goods. Below, the main applications in the transportation and logistics domain are described [3].
- **Logistics**
  Real-time information processing technology based on RFID and NFC can realize real-time monitoring of almost every link of the supply chain, ranging from commodity design, raw material purchasing, production, transportation,storage, distribution and sale of semi-products and products, returns' processing and after-sales service..It is also possible to obtain products related information, promptly, timely, and accurately so that enterprises or even the whole supply chain can respond to intricate and changeable markets in the shortest time. The application result is that the reaction time of traditional enterprises is 120 days from requirements of customers to the supply of commodity while advanced companies that make use of these technologies (such as Walmart and Metro) only needs few days and can basically work with zero safety stock [39,40]. Additionally, real-time access to the ERP program helps the shop assistants to better inform customers about availability of products and give them more product information in general [3].
- **Assisted driving**
  Cars, trains, and buses along with the roads and the rails equipped with sensors, actuators and processing power may provide important information to the driver and/or passengers of a car to allow better navigation and safety. Collision avoidance systems and monitoring of transportation of hazardous materials are two typical example functions. Governmental authorities would also benefit from more accurate information about road traffic patterns for planning purposes. Whereas the private transportation traffic could better find the right path with appropriate information about the jam and incidents. Enterprises, such as freight companies, would be able to perform more effective route optimization which allows energy savings. Information about the movement of the vehicles transporting goods together

with information about the type and status of the goods can integrated to provide important information about the delivery time, delivery delays, and faults. This information can be also combined with the status of the warehouses in order to automate the refilling of the magazines [3].

- **Mobile ticketing.**
  Posters or panels providing information (description, costs, schedule) about transportation services can be equipped with an NFC tag, a visual marker and a numeric identifier. The user can then get information about several categories of options from the web by either hovering his mobile phone over the NFC tag, or pointing the mobile phone to the visual markers. The mobile phone automatically gets information from the associated web services (stations, numbers of passengers, costs, available seats and type of services) and allows the user to buy the related tickets [3].
- **Monitoring environmental parameters.**
  Perishable goods such as fruits, fresh-cut produce, meat, and dairy products are vital parts of our nutrition. From the production to the consumption sites thousands of kilometers or even more are covered and during the transportation the conservation status (temperature, humidity, shock) need to be monitored to avoid uncertainty in quality levels for distribution decisions. Pervasive computing and sensor technologies offer great potential for improving the efficiency of the food supply chain [3].
- **Augmented maps**
  Touristic maps can be equipped with tags that allow NFC-equipped phones to browse it and automatically call web services providing information about hotels, restaurants, monuments and events related to the area of interest for the user,
- **Healthcare domain**
  Many are the benefits provided by the IoT technologies to the healthcare domain and the resulting applications can be grouped mostly into: tracking of objects and people (staff and patients); identification and authentication of people; automatic data collection and sensing [3].
- **Tracking**
  Tracking is the function aimed at the identification of a person or object in motion. This includes both real-time position tracking, such as the case of patient-flow monitoring to improve workflow in hospitals, and tracking of motion through choke points, such as access to designated areas. In relation to assets, tracking is most frequently applied to continuous inventory location tracking, and materials tracking to prevent 780 left-ins during surgery, such as specimen and blood products [3].
- **Identification and authentication**
  It includes patient identification to reduce incidents harmful to patients (such as wrong drug/dose/time/procedure), comprehensive and current electronic medical record maintenance (both in the in- and out-patient settings), and infant identification in hospitals to prevent mismatching. In relation to staff, identification and authentication is most frequently used to grant access and to improve employee morale by addressing patient safety issues. In relation to assets, identification and authentication is predominantly used to meet the requirements of security procedures, to avoid thefts or losses of important instruments and products[3].
- **Data collection**
  Automatic data collection and transfer is mostly aimed at reducing form processing time, process automation (including data entry and collection errors), automated care and procedure auditing, and medical inventory management. This function also relates to integrating RFID technology with other health information and clinical application technologies within a facility and with potential expansions of such networks across providers and locations [3].
- **Sensing**
  Sensor devices enable function centered on patients, and in particular on diagnosing patient conditions, providing real-time information on patient health indicators. Application domains include different telemedicine solutions, monitoring patient compliance with medication regiment prescriptions, and alerting for patient well-being. In this capacity, sensors can be applied both in in-patient and out-patient care. Heterogeneous wireless access-based remote patient monitoring systems can be deployed to reach the patient everywhere, with multiple wireless technologies integrated to support continuous biosignal monitoring in presence of patient mobility [3].

Many other applications exists please refer to [3] for more

IV. IoT Issues

Although the enabling technologies make the IoT concept feasible, a large research effort is still required. In this section, we review the issues that are still in research, for more details please refer to [3]

- **Standards**
  There are several standardization efforts but they are not integrated in a comprehensive framework
- **Mobility support**
  There are several proposals for object addressing but none for mobility support in the IoT scenario, where scalability and adaptability to heterogeneous technologies represent crucial problems
- **Naming**
  Object Name Servers (ONS) are needed to map a reference to a description of a specific object and the related identifier, and vice versa
- **Transport protocol**
  Existing transport protocols fail in the IoT scenarios since their connection setup and congestion control mechanisms may be useless; furthermore, they require excessive buffering to be implemented in objects
- **Traffic characterization and QoS support**
  The IoT will generate data traffic with patterns that are expected to be significantly different from those observed in the current Internet. Accordingly, it will also be necessary to define new QoS requirements and support schemes
- **Authentication**
  Authentication is difficult in the IoT as it requires appropriate authentication infrastructures that will not be available in IoT scenarios. Furthermore, things have scarce resources when compared to current communication and computing devices. Also man-in-the-middle attack is a serious problem
- **Data integrity**
  This is usually ensured by protecting data with passwords. However, the password lengths supported by IoT technologies are in most cases too short to provide strong levels of protection
- **Privacy**
  A lot of private information about a person can be collected without the person being aware. Control on the diffusion of all such information is impossible with current techniques
- **Digital forgetting**
  All the information collected about a person by the IoT may be retained indefinitely as the cost of storage decreases. Also data mining techniques can be used to easily retrieve any information even after several years

V. Security And Privacy

People will resist the IoT as long as there is no public confidence that it will not cause serious threats to privacy. All the talking and complains following the announcement by the Italian retailer Benetton on the plan to tag a complete line of clothes (around 15 million RFIDs) has been the first, clear confirmation of this mistrust towards the use that will be done of the data collected by the IoT technologies. Public concerns are indeed likely to focus on a certain number of security and privacy issues[3].

Security:
The IoT is extremely vulnerable to attacks for several reasons. First, often its components spend most of the time unattended; and thus, it is easy to physically attack them. Second, most of the communications are wireless, which makes eavesdropping extremely simple. Finally, most of the IoT components are characterized by low capabilities in terms of both energy and computing resources (this is especially the case for passive components) and thus, they cannot implement complex schemes supporting security.More specifically, the major problems related to security concern authentication and data integrity. Authentication is difficult as it usually requires appropriate authentication infrastructures and servers that achieve their goal through the exchange of appropriate messages with other nodes. In the IoT such approaches are not feasible given that passive RFID tags cannot exchange too many messages with the authentication servers. The same reasoning applies (in a less restrictive way) to the sensor nodes as well. In this context, note that several solutions have been proposed for sensor networks in the recent past. However, existing solutions can be applied when sensor nodes are considered as part of a sensor network connected to the rest of the Internet via some nodes playing the roles of gateways. In the IoT scenarios, instead, sensor nodes must be seen as nodes of the Internet, so that it becomes necessary to authenticate them even from nodes not belonging to the same sensor

network. In the last few years, some solutions have been proposed for RFID systems, however, they all have serious problems as described in [3].

Finally, none of the existing solutions can help in solving the proxy attack problem, also known as the man-in-the-middle attack. Consider the case in which a node is utilized to identify something or someone and, accordingly, provides access to a certain service or a certain area (consider an electronic passport for example, or some keys based on RFID). The attack depicted in Fig. 5 could be successfully performed.

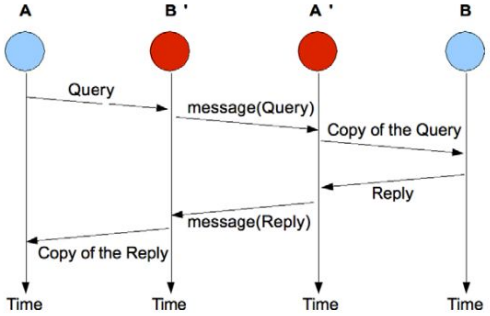

Fig. 4. Man in the middle attack.

Privacy

The concept of privacy is deeply rooted into our civilizations, is recognized in all legislations of civilized countries and, as we already said, concerns about its protection have proven to be a significant barrier against the diffusion of the technologies involved in the IoT. People concerns about privacy are indeed well justified. In fact, the ways in which data collection, mining, and provisioning will be accomplished in the IoT are completely different from those that we now know and there will be an amazing number of occasions for personal data to be collected. Therefore, for human individuals it will be impossible to personally control the disclosure of their personal information.

Furthermore, the cost of information storage continues to decrease and is now approaching 10^(-9) euro per byte. Accordingly, once information is generated, will most probably be retained indefinitely, which involves denial of digital forgetting in people perspective. It follows that the IoT really represents an environment in which privacy of individuals is seriously menaced in several ways. Furthermore, while in the traditional Internet problems of privacy arise mostly for Internet users (individuals playing an active role), in the IoT scenarios privacy problems arise even for people not using any IoT service. Accordingly, privacy should be protected by ensuring that individuals can control which of their personal data is being collected, who is collecting such data, and when this is happening. Furthermore, the personal data collected should be used only in the aim of supporting authorized services by authorized service providers; and, finally, the above data should be stored only until it is strictly needed.

VI. Security Goals

The major security goals of IoT are to ensure proper identity authentication mechanisms and provide confidentiality about the data. The Security triad, a distinguished model for the development of security mechanisms, implements the security by making use of the three areas which are Data confidentiality, integrity and availability as shown in the Fig. 5. A breach in any of these areas could cause serious issues to the system so they must be accounted for. The three areas are described below:

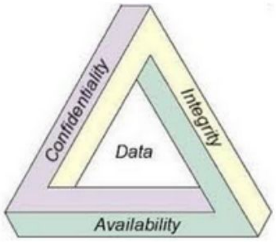

Fig.5. The Security Triad

A. Data Confidentiality

Data confidentiality is identical to providing freedom to user from the external interference. It is the ability to provide confidence to user about the privacy of the sensitive information by using different mechanisms such that its disclosure to the unauthorized party is prevented and can be accessed by the permitted users only. There are many security mechanisms to provide confidentiality of the data including, but not limited to, Data Encryption in which the data is converted into ciphertext form which makes it difficult to access for the users having no proper authorizations, the Two-step verification, which provides authentication by two dependent components and allows the access only if both the components pass the authentication test and the most common Biometric Verification in which every person is uniquely identifiable. For the IoT based devices, it ensures that the sensor nodes of the sensor networks don't reveal their data to the neighboring nodes, similarly the tags don't transmit their data to an unauthorized reader [4].

B. *Data Integrity*

During the communication, data could be altered by the cybercriminals or could be affected by various other factors that are beyond human control including the crash of server or an electromagnetic disturbance. Data Integrity refers to the protection of useful information from the cybercriminals or the external interference during transmission and reception with some common tracking methods, so that the data cannot be tampered without the system catching the threat [13]. The methods to ensure the accuracy and originality of data includes methods like Checksum and Cyclic Redundancy Check (CRC) which are simple error detector mechanisms for a portion of data. Moreover, continuous syncing of the data for backup purposes and the feature like Version control, which keeps a record of the file changes in a system to restore the file in case of fortuitous deletion of data can also ensure the integrity of data such that the data on IoT based devices is in its original form when accessed by the permitted users [4].

C. *Data Availability*

One of the major goals of IoT security is to make data available to its users, whenever needed. Data Availability ensures the immediate access of authorized party to their information resources not only in the normal conditions but also in disastrous conditions. Due to dependency of companies on it, it is necessary to provide firewalls to countermeasure the attacks on the services like Denial-of-service (DoS) attack which can deny the availability of data to the user-end. Data Availability also ensure the prevention of bottleneck situations which prevent the flow of information. The Redundancy and Failover backup methods provide duplication of the system components in conditions of system failure or various system conflictions to ensure reliability and availability of data [4].

IoT architectures are supposed to deal with an estimated population of billions of objects, which will interact with each other and with other entities, such as human beings or virtual entities. And all these interactions must be secured somehow, protecting the information and service provisioning of all relevant actors and limiting the number of incidents that will affect the entire IoT. However, protecting the Internet of Things is a complex and difficult task. The number of attack vectors available to malicious attackers might become staggering, as global connectivity (''access anyone'') and accessibility (''access anyhow, anytime'') are key tenets of the IoT. The threats that can affect the IoT entities are numerous, such as attacks that target diverse communication channels, physical threats, denial of service, identity fabrication, and others. Finally, the inherent complexity of the IoT, where multiple heterogeneous entities located in different contexts can exchange information with each other, further complicates the design and deployment of efficient, interoperable and scalable security mechanisms [5].

IV. Analysis of attacker models and threats

In order to understand how the different approaches presented earlier should be secured in the future, it is firstly necessary to enumerate and analyze the attacker models. These models have been defined in a way that they can be applied to both centralized and distributed IoT approaches. Note, however, that the concept of 'perimeter' in the Internet of Things is a bit fuzzy: an attacker can control part of the network, but due to the inherent distributed nature of the IoT, it is nearly impossible for an attacker to fully control the whole system. As a result, an attacker can be both 'internal' and 'external' at the same time [5]. These attacker models, categorized by threats, are introduced below:

- **Denial of service (DoS).** There are a wide number of DoS attacks that can be launched against the IoT. Beyond traditional Internet DoS attacks that exhaust service provider resources and network bandwidth, the actual wireless communication infrastructure of most data acquisition networks can also be targeted (e.g. jamming the channels).
- **Physical damage.** This threat can be seen as a subset of the DoS threat. In this attacker model, active attackers usually lack technical knowledge, and can only hinder the provisioning of IoT services by destroying the actual 'things'. This is a realistic attack in the IoT context, because things might be easily accessible to anyone (e.g. a street light). If that is not possible, the attacker can simply target the hardware module in charge of creating the 'virtual persona' of the thing.

- **Controlling.** As long as there is an attack path, active attackers can try to gain partial or full control over an IoT entity. The scope of the damage caused by these attackers depends mainly on (a) the importance of the data managed by that particular entity, (b) the services that are provided by that particular entity

VI. Security Challenges

There have been many achievements in the research field of IoT, however there are still some open challenges that needs to be addressed for the ubiquity of this technology. In this section some of the threats in each architectural layer that needs special attention are discussed.

Perception Layer Challenges [4]

Perception layer consists of different sensor technologies like RFID which are exposed to many kinds of threats which are discussed below:

- *Unauthorized Access to the Tags.* Due to the lack of proper authentication mechanism in a large number of RFID systems, tags can be accessed by someone without authorization. The attacker cannot just read the data but the data can be modified or even deleted as well.
- *Tag Cloning.* Since tags are deployed on different objects which are visible and their data can be read and modified with some hacking techniques therefore they can be easily captured by any cybercriminal who can create a replica of the tag and hence compromising it in a way that the reader cannot distinguish between the original and the compromised tag.
- *Eavesdropping.* Because of the wireless characteristics of the RFID it becomes very easy for the attacker to sniff out the confidential information like passwords or any other data flowing from tag-to-reader or reader-to-tag which makes it vulnerable because the attacker can make it to use in despicable ways.
- *Spoofing.* Spoofing is when an attacker broadcasts fake information to the RFID systems and makes it to assume its originality falsely which makes it appearing from the original source. This way attacker gets full access to the system making it vulnerable.
- *RF Jamming.* RFID tags can also be compromised by kind of a DoS attack in which communication through RF signals is disrupted with an excess of noise signals.

Network Layer Challenges [4]

Network layer consists of the Wireless Sensor Network (WSN) which transmits the data from the sensor to its destination with reliability. The related security issues are discussed below:

- *Sybil Attack.* Sybil is a kind of attack in which the attacker manipulates the node to present multiple identities for a single node due to which a considerable part of the system can be compromised resulting in false information about the redundancy
- *Sinkhole Attack.* It is a kind of attack in which the adversary makes the compromised node look attractive to the nearby nodes due to which all the data flow from any particular node is diverted towards the compromised node resulting in packets drop i.e. all the traffic is silenced while the system is fooled to believe that the data has been received on the other side. Moreover this attack results in more energy consumption which can cause DoS attack.
- *Sleep Deprivation Attack.* The sensor nodes in the Wireless Sensor Network are powered with batteries with not so good lifetime so the nodes are bound to follow the sleep routines to extend their lifetime. Sleep Deprivation is the kind of attack which keeps the nodes awake, resulting in more battery consumption and as a result battery lifetime is minimized which causes the nodes to shut down.
- *Denial of Service (DoS) Attack.* The kind of attack in which the network is flooded with a useless lot of traffic by an attacker, resulting in a resource exhaustion of the targeted system due to which the network becomes unavailable to the users.
- *Malicious code injection.* This is a serious kind of attack in which an attacker compromises a node to inject malicious code into the system which could even result in a complete shutdown of the network or in the worst case, the attacker can get a full control of the network.
- *Man-in-the-Middle Attack.*
  This is a form of Eavesdropping in which target of the attack is the communication channel due to which the unauthorized party can monitor or control all the private communications between the two parties hideously. The unauthorized party can even fake the identity of the victim and communicate normally to gain more information.

Middleware Layer Challenges[4]

This layer is composed of data storage technologies like cloud computing. The security challenges of this layer are discussed below:

- *Unauthorized Access.* Middleware Layer provides different interfaces for the applications and data storage facilities. The attacker can easily cause damage to the system by forbidding the access to the related services of IoT or by deleting the existing data. So an unauthorized access could be fatal for the system.
- *DoS Attack.* It is similar to the DoS attack discussed in the previous two layers i.e. it shuts down the system which results in unavailability of the services.
- *Malicious Insider.* This kind of attack occurs when someone from the inside tampers the data for personal benefits or the benefits of any 3rd party. The data can be easily extracted and then altered on purpose from the inside.

Application Layer Challenges [4]

The related security issues of this layer are described below:

- *Malicious Code Injection.* An attacker can leverage the attack on the system from end-user with some hacking techniques that allows the attacker to inject any kind of malicious code into the system to steal some kind of data from the user.
- *Denial-of-Service (DoS) Attack.* DoS attacks nowadays have become sophisticated, it offers a smoke screen to carry out attacks to breach the defensive system and hence data privacy of the user, while deceiving the victim into believing that the actual attack is happening somewhere else. This put the non-encrypted personal details of the user at the hands of the hacker.
- *Spear-Phishing Attack.* It is an email spoofing attack in which victim, a high ranking person, is lured into opening the email through which the adversary gains access to the credentials of that victim and then by a pretense retrieves more sensitive information.
- *Sniffing Attack.* An attacker can force an attack on the system by introducing a sniffer application into the system, which could gain network information resulting in corruption of the system.

Security at Different Layers

There are many researches being carried out to provide a reliable well-defined security architecture which can provide confidentiality of the data security and privacy. W. Zhang et al. [8] proposed an architecture for the security against the possible threats, as shown in Fig. 6

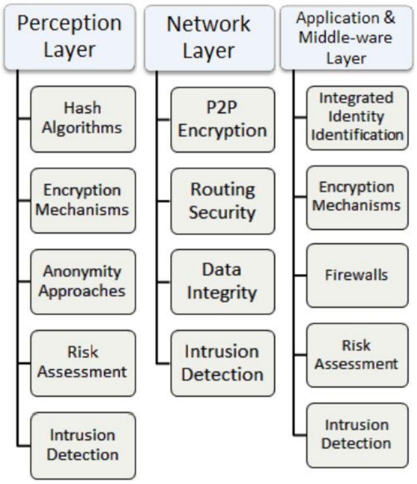

Fig.6. Security Architecture of IoT

Perception Layer

Perception Layer is the bottom layer of the IoT architecture which provides various security features to the hardware. It serves four basic purposes which are Authentication, Data Privacy, Privacy of sensitive information and Risk Assessment which are discussed below:

- *Authentication*. Authentication is done using Cryptographic Hash Algorithms which provides digital signatures to the terminals that could withstand all the possible known attacks like Side-channel attack, Brute force attack and Collision attack etc.
- *Data Privacy.* Privacy of the data is guaranteed by symmetric and asymmetric encryption algorithms such as RSA, DSA, BLOWFISH and DES etc which prevents an unauthorized access to the sensor data while being collected or forwarded to the next layer. Due to their low power consumption benefit, they can be easily implemented into the sensors.
- *Privacy of sensitive information.* As for hiding the sensitive information, anonymity of the location and identity is obtained using K-Anonymity approach which ensures the protection of the information like identity and location etc of the user.
- *Risk Assessment.* It is a fundamental of IoT security which discovers the new threats to the system. It could help preventing the security breaches and determining the best security strategies. An example of it is the Dynamical Risk Assessment method for IoT.

  Even with such security measures, if an intrusion is detected in the system, an automated Kill-command from the RFID reader is sent to the RFID tag which prevents an unauthorized access to the RFID tag data.

Network Layer

The network layer which could be both wired or wireless is exposed to various kinds of attacks. Due to the openness of the wireless channels, communications can be monitored easily by some hackers. The network layer security is further divided into three types which are discussed below [4]:

- *Authentication.* With the help of a proper authentication process and point to point encryption, illegal access to the sensor nodes to spread fake information could be prevented. The most common kind of attack is the DoS attack which impacts the network by driving a lot of useless traffic towards it through a number of botnets fueled by the system of interconnected devices.
- *Routing Security.* After the Authentication process, routing algorithms are implemented to ensure the privacy of data exchange between the sensor nodes and the processing systems. There have been many researches carried out for the routing ways including Source Routing , in which data to be transmitted is stored in the form of packets which is then sent to the processing system after being analyzed by the intermediate nodes, And the Hop-by-Hop routing in which only address of the data destination is known. The security of routing is ensured by providing multiple paths for the data routing which improves the ability of the system to detect an error and keep performing upon any kind of failure in the system.
- *Data Privacy.* The safety control mechanisms monitors the system for any kind of intrusion and finally Data integrity methods are implemented to make sure that the data received on the other end is the same as the original one.

Middleware and Application Layer

This layer amalgamates the Middle-ware and Application layer to form an integrated security mechanism. The security categorization is discussed below:

- *Authentication.* Firstly it goes through the authentication process which prevents the access to any miscreant user by integrated identity identifications. This is exactly similar to that of the identification process in either of the layers except that this layer encourages authentications by some certain cooperating services which means users can even choose the associated information to be shared with the services. The major technologies used in this layer are Cloud computing and Virtualization, both of which are ripe to various attacks. The cloud technology can be easily compromised, one of the worst threat is the insider threat. Similarly Virtualization is exposed to DOS and data theft etc. A lot of research is needed in both domains to provide secure environment.
- *Intrusion Detection.* Its intrusion detection techniques provide solutions for various security threats by generating an alarm on occurrence of any suspicious activity in the system due to the continuous monitoring and keeping a log of the intruder’s activities which could help to trace the intruder. There are different existing intrusion detection techniques including the data mining approach and anomaly detection.

- *Risk Assessment.* The risk assessment gives justification for the effective security strategies and provides improvements in the existing security structure.
- *Data Security*. Data security is ensured by various encryption technologies which prevent the data stealing threats. Moreover, to prevent other malicious activities from the miscreant users, AntiDos firewalls and up to date spywares and malwares are introduced.

References

[1] Kevin Ashton, That Internet of things thing, It can be accessed at: http://www.rfidjournal.com/articles/view?4986

[2] D. Singh, G. Tripathi, A.J. Jara, A survey of Internet-of Things: Future Vision, Architecture, Challenges and Services, in Internet of Things (WF-IoT), 2014

[3] Atzori, L., Iera, A. and Morabito, G., 2010. The internet of things: A survey. *Computer networks*, *54*(15), pp.2787-2805.

[4] Farooq, M.U., Waseem, M., Khairi, A. and Mazhar, S., 2015. A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, *111*(7).

[5] Roman, R., Zhou, J. and Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), pp.2266-2279.

[6] Liu, C., Zhang, Y., Zeng, J., Peng, L. and Chen, R., 2012, May. Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology. In *Natural Computation (ICNC), 2012 Eighth International Conference on*(pp. 874-878). IEEE.

[7] Bello, O., Zeadally, S. and Badra, M., 2017. Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT). *Ad Hoc Networks*, *57*, pp.52-62.

[8] W. Zhang, B. Qu, Security Architecture of the Internet of Things Oriented to Perceptual Layer, in International Journal on Computer, Consumer and Control (IJ3C), Volume 2, No.2 (2013)