Development in RFID (Radio Frequency Identification) Technology in Internet of Things (IOT)

HEMALATHA D[1] , AFREEN BANU E[2]

1. ME CSE Student, Vel Tech Multitech Engineering College,Chennai
2. Assistant Professor, Vel Tech Multitech Engineering College, Chennai

A***bstract*—The Internet of Things (IoT) shall be able to incorporate transparently and seamlessly a large number of different and heterogeneous end systems, while providing open access to selected subsets of data for the development of a plethora of digital services. This paper provides an overview of the Internet of Things (IoT) that is enabled by the latest developments in RFID, smart sensors, communication technologies and Internet protocols. The current revolution in Internet, mobile and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT. The radio-frequency identification (RFID) technology is one of the core technologies of IoT deployments in the healthcare environment. To satisfy the various security requirements of RFID technology in IoT, many RFID authentication schemes have been proposed in the past decade. Recently, elliptic curve cryptography (ECC)-based RFID authentication schemes have attracted a lot of attention and have been used in the healthcare environment. In this paper, we discuss the security requirements of RFID authentication schemes for the support of Internet of Things(IoT). We refer to the IoT paradigm as the means to collect data from sensors or RFID and to send control messages to actuators.***

Index Terms - Authentication, elliptic curve cryptography(ECC), Internet of Things (IoT), performance, radio-frequency identification (RFID), Security.

I. INTRODUCTION

The growing number of physical objects are being connected to the Internet at an unprecedented rate realizing the idea of the Internet of Things (IoT). A basic example of such objects includes thermostats and HVAC (Heating, Ventilation, and Air Conditioning) monitoring and control systems that enable smart homes. There are also other domains and environments in which the IoT can play a remarkable role and improve the quality of our lives. These applications include transportation, healthcare, industrial automation, and emergency response to natural and man-made disasters where human decision making is difficult. The IoT enables physical objects to see, hear, think and perform jobs by having them ―talk‖ together, to share information and to coordinate decisions.

The IoT transforms these objects from being traditional to smart by exploiting its underlying technologies such as ubiquitous and pervasive computing, embedded devices, communication technologies, sensor networks, Internet protocols and applications. Smart objects along with their supposed tasks constitute domain specific applications (vertical markets) while ubiquitous computing and analytical services form application domain independent services (horizontal markets). The IoT is a recent communication paradigm that envisions a near future in which the objects of everyday life will be equipped with micro controllers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet. The IoT concept, hence, aims at making the Internet even more immersive and pervasive.

Furthermore, by enabling easy access and interaction with a wide variety of devices such as, for instance, home appliances, surveillance cameras, monitoring sensors, actuators, displays, vehicles and so on, the IoT will foster the development of a number of applications that make use of the potentially enormous amount and variety of data generated by such objects to provide new services to citizens, companies, and public administrations.

II. IOT ARCHITECTURE

The IoT should be capable of interconnecting billions or trillions of heterogeneous objects through the Internet, so there is a critical need for a flexible layered architecture. The ever increasing number of proposed architectures has not yet converged to a reference model . Meanwhile, there are some projects like IoT-A which try to design a common architecture based on the analysis of the needs of researchers and the industry. From the pool of proposed models, the basic model is a 3-layer architecture consisting of the Application, Network, and Perception Layers. In the recent literature, however, some other models have been proposed that add more abstraction to the IoT architecture. Fig. 3 illustrates some common architectures among them is the 5-layer model (not to be confused with the TCP/IP layers) which has been used in . Next, we provide a brief discussion on these five layers:

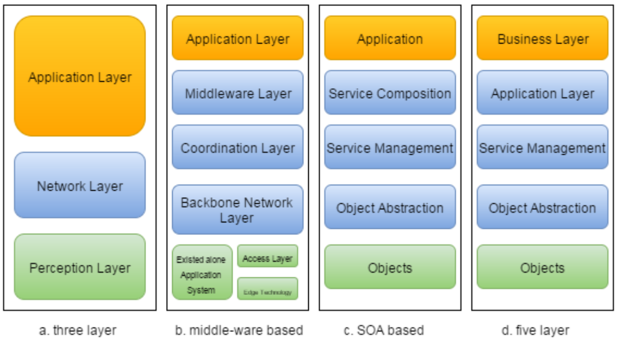

Fig.1. The IOT Architecture

A. *Objects Layer*

The first layer, the Objects (devices) or perception layer, represents the physical sensors of the IoT that aim to collect and process information. This layer includes sensors and actuators to perform different functionalities such as querying location, temperature, weight, motion, vibration, acceleration, humidity, etc. Standardized plug-and-play mechanisms need to be used by the perception layer to configure heterogeneous objects [17, 18]. The perception layer digitizes and transfers data to the Object Abstraction layer through secure channels. The big data created by the IoT are initiated at this layer.

B. *Object Abstraction layer*

Object Abstraction transfers data produced by the Objects layer to the Service Management layer through secure channels. Data can be transferred through various technologies such as RFID, 3G, GSM, UMTS, WiFi, Bluetooth Low Energy, infrared, ZigBee, etc. Furthermore, other functions like cloud computing and data management processes are handled at this layer.

C. *Service Management Layer*

Service Management or Middleware (pairing) layer pairs a service with its requester based on addresses and names. This layer enables the IoT application programmers to work with heterogeneous objects without consideration to a specific hardware platform. Also, this layer processes received data, makes decisions, and delivers the required services over the network wire protocols.

D. *Application Layer*

The application layer provides the services requested by customers. For instance, the application layer can provide temperature and air humidity measurements to the customer who asks for that data. The importance of this layer for the IoT is that it has the ability to provide high-quality smart services to meet customers‘ needs. The application layer covers numerous vertical markets such as smart home, smart building, transportation, industrial automation and smart healthcare.

E. *Business Layer*

The business (management) layer manages the overall IoT system activities and services. The responsibilities of this layer are to build a business model, graphs, flowcharts, etc. based on the received data from the Application layer. It is also supposed to design, analyze, implement, evaluate, monitor, and develop IoT system related elements. The Business Layer makes it possible to support decision-making processes based on Big Data analysis. In addition, monitoring and management of the underlying four layers is achieved at this layer. Moreover, this layer compares the output of each layer with the expected output to enhance services and maintain users‘ privacy.

III. IOT ELEMENTS

Understanding the IoT building blocks helps to gain a better insight into the real meaning and functionality of the IoT. In the following sections we discuss six main elements needed to deliver the functionality of the IoT as illustrated in Fig. 4. Table II shows the categories of these elements and examples of each category.

A. *Identification*

Identification is crucial for the IoT to name and match services with their demand. Many identification methods are available for the IoT such as electronic product codes (EPC) and ubiquitous codes (uCode) [21]. Furthermore, addressing the IoT objects is critical to differentiate between object ID and its address. Object ID refers to its name such as —T1‖ for a particular temperature sensor and object‘s address refers to its address within a communications network. In addition, addressing methods of IoT objects include IPv6 and IPv46LoWPAN [22, 23] provides a compression mechanism over IPv6 headers that makes IPv6 addressing appropriate for low power wireless networks. Distinguishing between object‘s identification and address is imperative since identification methods are not globally unique, so addressing assists to uniquely identify objects. In addition, objects within the network might use public IPs and not private ones. Identification methods are used to to provide a clear identity for each object within the network.

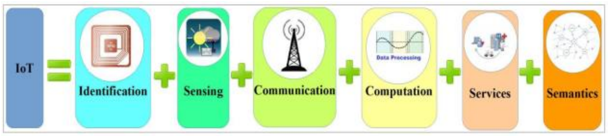

Fig 2. The IOT Elements

B. Sensing

The IoT sensing means gathering data from related objects within the network and sending it back to a data warehouse, database, or cloud. The collected data is analyzed to take specific actions based on required services. The IoT sensors can be smart sensors, actuators or wearable sensing devices. For example, companies like Wemo, revolv and SmartThings offer smart hubs and mobile applications that enable people to monitor and control thousands of smart devices and appliances inside buildings using their smartphones [24-26]. Single Board Computers (SBCs) integrated with sensors and built-in TCP/IP and security functionalities are typically used to realize IoT products (e.g., Arduino Yun, Raspberry PI, BeagleBone Black, etc.). Such devices typically connect to a central management portal to provide the required data by customers.

C. Communication

The IoT communication technologies connect heterogeneous objects together to deliver specific smart services. Typically, the IoT nodes should operate using low power in the presence of lossy and noisy communication links. Examples of communication protocols used for the IoT are WiFi, Bluetooth, IEEE 802.15.4, Z-wave, and LTE-Advanced. Some specific communication technologies are also in use like RFID, Near Field Communication (NFC) and *ultra-wide bandwidth* (UWB). RFID is the first technology used to realize the M2M concept (RFID tag and reader). The RFID tag represents a simple chip or label attached to provide object‘s identity. The RFID reader transmits a query signal to the tag and receives reflected signal from the tag, which in turn is passed to the database. The database connects to a processing center to identify objects based on the reflected signals within a (10 cm to 200 m) range [27]. RFID tags can be active, passive or semi-passive/active. Active tags are powered by battery while passive ones do not need battery. Semi-passive/active tags use board power when needed.

The NFC protocol works at high frequency band at 13.56 MHz and supports data rate up to 424 kbps. The applicable range is up to 10 cm where communication between active readers and passive tags or two active readers can occur [28].The UWB communication technology is designed to support communications within a low range coverage area using low energy and high bandwidth whose applications to connect sensors have been increased recently [29].

Another communication technology is WiFi that uses radio waves to exchange data amongst things within 100 m range [30]. WiFi allows smart devices to communicate and exchange information without using a router in some *ad hoc* configurations. Bluetooth presents a communication technology that is used to exchange data between devices over short distances using short-wavelength radio to minimize power consumption [31]. Recently, the Bluetooth *special interest group* (SIG) produced Bluetooth 4.1 that provides Bluetooth Low Energy as well as high-speed and IP connectivity to support IoT [32]. The IEEE 802.15.4 standard specifies both a physical layer and a medium access control for low power wireless networks targeting reliable and scalable communications [33]. LTE (Long-Term Evolution) is originally a standard wireless communication for high-speed data transfer between mobile phones based on GSM/UMTS network technologies [34]. It can cover fast-travelling devices and provide multicasting and broadcasting services. LTE-A (LTE Advanced) [35] is an improved version of LTE including bandwidth extension which supports up to 100 MHz, downlink and uplink spatial multiplexing, extended coverage, higher throughput and lower latencies.

D. Computation

Processing units (e.g., microcontrollers, microprocessors, SOCs, FPGAs) and software applications represent the ―brain‖ and the computational ability of the IoT. Various hardware platforms were developed to run IoT applications such as Arduino, UDOO, FriendlyARM, Intel Galileo, Raspberry PI, Gadgeteer, BeagleBone, Cubieboard, Z1, WiSense, Mulle, and T-Mote Sky.

Furthermore, many software platforms are utilized to provide IoT functionalities. Among these platforms, Operating Systems (RTOS) are vital since they run for the whole activation time of a device. There are several Real-Time Operating Systems (RTOS) that are good candidates for the development of RTOS-based IoT applications. For instance, the Contiki RTOS has been used widely in IoT scenarios. Contiki has a simulator called Cooja which allows researcher and developers to simulate and emulate IoT and wireless sensor network (WSN) applications [36]. TinyOS [37], LiteOS [38] and Riot OS [39] also offer light weight OS designed for IoT environments. Moreover, some auto industry leaders with Google established the Open Auto Alliance (OAA) and are planning to bring new features to the Android platform to accelerate the adoption of the Internet of Vehicles (IoV) paradigm [40]. Some features of these operating systems are compared. Cloud Platforms form another important computational part of the IoT. These platforms provide facilities for smart objects to send their data to the cloud, for big data to be processed in real-time, and eventually for end-users to benefit from the knowledge extracted from the collected big data. There are a lot of free and commercial cloud platforms and frameworks available to host IoT services. Some of these services are introduced in section VII.B.

E. Services

Overall, IoT services can be categorized under four classes: Identity-related Services, Information Aggregation Services, Collaborative-Aware Services and Ubiquitous Services. Identity-related services are the most basic and important services that are used in other types of services. Every application that needs to bring real world objects to the virtual world has to identify those objects. Information Aggregation Services collect and summarize raw sensory measurements that need to be processed and reported to the IoT application. Collaborative-Aware Services act on top of Information Aggregation Services and use the obtained data to make decision and react accordingly. Ubiquitous Services, however, aim to provide Collaborative-Aware Services *anytime* they are needed to *anyone* who needs them *anywhere*. With this categorization, we review some applications of the IoT in the following paragraphs. The ultimate goal of all IoT applications is to reach the level of ubiquitous services. However, this end is not achievable easily since there are a lot of difficulties and challenges that have to be addressed. Most of the existing applications provide identity-related, information aggregation, and collaborative-aware services. Smart healthcare and smart grids fall into the information aggregation category and smart home, smart buildings, intelligent transportation systems (ITS), and industrial automation are closer to the collaborative-aware category.

Smart home IoT services contribute to enhancing the personal life-style by making it easier and more convenient to monitor and operate home appliances and systems (e.g., air conditioner, heating systems, energy consumption meters, etc.) remotely. For example, a smart home can automatically close the windows and lower the blinds of upstairs windows based on the weather forecast. Smart homes are required to have regular interaction with their internal and external environments [44]. The internal environment may include all the home appliances and devices that are Internet-connected while the external environment consists of entities that are not in control of the smart home such as smart grid entities.

Smart buildings **connect** ***building automation systems*** (BAS) to the Internet [45]. BAS allows to control and manage different building devices using sensors and actuators such as HVAC, lighting and shading, security, safety, entertainment, etc. Furthermore, BAS can help to enhance energy consumption and maintenance of buildings. For example, a blinking dishwasher or cooling/heating system can provide indications when there is a problem that needs to be checked and solved. Thus, maintenance requests can be sent out to a contracted company without any human intervention.

Smart healthcare plays a significant role in healthcare applications through embedding sensors and actuators in patients and their medicine for monitoring and tracking purposes. The IoT is used by clinical care to monitor physiological statuses of patients through sensors by collecting and analyzing their information and then sending analyzed patient‘s data remotely to processing centers to make suitable actions. For example, Masimo Radical-7 monitors the patient‘s status remotely and reports that to a clinical staff [55]. Recently, IBM utilized RFID technology at one of OhioHealth's hospitals to track hand washing after checking each patient [56-58].

Smart grids [44, 59] utilize the IoT to improve and enhance the energy consumption of houses and buildings. Employing the IoT in smart grids helps power suppliers to control and manage resources to provide power proportionally to the population increase. For example, smart grids use the IoT to connect millions or billions of buildings‘ meters to the network of energy providers. These meters are used to collect, analyze, control, monitor, and manage energy consumption. The IoT enables energy providers to improve their services to meet consumers‘ needs. Also, utilizing the IoT in the smart grid reduces the potential failures, increases efficiency and improves quality of services.

TABLE 1
BUILDING BLOCKS AND TECHNOLOGIES OF THE IOT

IoT Elements		**Samples**
Identification	**Naming**	EPC, uCode
	Addressing	IPv4, IPv6
Sensing		Smart Sensors, Wearable sensing devices, Embedded sensors, Actuators, RFID tag
Communication		RFID, NFC, UWB, Bluetooth, BLE, IEEE 802.15.4, Z-Wave, WiFi, WiFiDirect, , LTE-A
Computation	**Hardware**	SmartThings, Arduino, Phidgets, Intel Galileo, Raspberry Pi, Gadgeteer, BeagleBone, Cubieboard, Smart Phones
	Software	OS (Contiki, TinyOS, LiteOS, Riot OS, Android); Cloud (Nimbits, Hadoop, etc.)
Service		Identity-related (shipping), Information Aggregation (smart grid), Collaborative-Aware (smart home), Ubiquitous (smart city)

A *smart city* which could be seen as an application of ubiquitous services, aims to improve the quality of life in the city by making it easier and more convenient for the residents to find information of interest. In a smart city environment, various systems based on smart technologies are interconnected to provide required services (health, utilities, transportation, government, homes and buildings).

F. Semantics

Semantic in the IoT refers to the ability to extract knowledge smartly by different machines to provide the required services. Knowledge extraction includes discovering and using resources and modeling information. Also, it includes recognizing and analyzing data to make sense of the right decision to provide the exact service [62]. Thus, semantic represents the brain of the IoT by sending demands to the right resource. This requirement is supported by Semantic Web technologies such as the Resource Description Framework (RDF) and the Web Ontology Language (OWL). In 2011, the *World Wide Web consortium* (W3C) adopted the *Efficient XML Interchange* (EXI) format as a recommendation.

IV. APPLICATIONS

There are several application domains which will be impacted by the emerging Internet of Things. The applications can be classified based on the type of network availability, coverage, scale, heterogeneity, repeatability, user involvement and impact [21]. We categorize the applications into four application domains: (1) Personal and Home; (2) Enterprize; (3) Utilities; and (4) Mobile. This is depicted in Fig. 1, which represents Personal and Home IoT at the scale of an individual or home, Enterprize IoT at the scale of a community, Utility IoT at a national or regional scale and Mobile IoT which is usually spread across other domains mainly due to the nature of connectivity and scale. There is a huge crossover in applications and the use of data between domains. For instance, the Personal and Home IoT produces electricity usage data in the house and makes it available to the electricity (utility) company which can in turn optimize the supply and demand in the Utility IoT. The internet enables sharing of data between different service providers in a seamless manner creating multiple business opportunities.

A few typical applications in each domain are given.

Personal and home

The sensor information collected is used only by the individuals who directly own the network. Usually WiFi is used as the backbone enabling higher bandwidth data (video) transfer as well as higher sampling rates (Sound). Ubiquitous healthcare [8] has been envisioned for the past two decades. IoT gives a perfect platform to realize this vision using body area sensors and IoT back end to upload the data to servers. For instance, a Smartphone can be used for communication along with several interfaces like Bluetooth for interfacing sensors measuring physiological parameters. So far, there are several applications available for Apple iOS, Google Android and Windows Phone operating systems that measure various parameters. However, it is yet to be centralized in the cloud for general physicians to access the same. An extension of the personal body area network is creating a home monitoring system for elderly care, which allows the doctor to monitor patients and the elderly in their homes thereby reducing hospitalization costs through early intervention and treatment [22,23]. Control of home equipment such as air conditioners, refrigerators, washing machines etc., will allow better home and energy management. This will see consumers become involved in the IoT revolution in the same manner as the Internet revolution itself [24,25]. Social networking is set to undergo another transformation with billions of interconnected objects [26,27]. An interesting development will be using a Twitter like concept where individual ‘Things’ in the house can periodically tweet the readings which can be easily followed from anywhere creating a TweetOT. Although this provides a common framework using cloud for information access, a new security paradigm will be required for this to be fully realized [28].

Enterprize

We refer to the ‘Network of Things’ within a work environment as an enterprize based application. Information collected from such networks are used only by the owners and the data may be released selectively. Environmental monitoring is the first common application which is implemented to keep track of the number of occupants and manage the utilities within the building (e.g., HVAC, lighting). Sensors have always been an integral part of the factory setup for security, automation, climate control, etc. This will eventually be replaced by a wireless system giving the flexibility to make changes to the setup whenever required. This is nothing but an IoT subnet dedicated to factory maintenance. One of the major IoT application areas that is already drawing attention is Smart Environment IoT [21,28]. There are several testbeds being implemented and many more planned in the coming years. Smart environment includes subsystems and the characteristics from a technological perspective are listed briefly. It should be noted that each of the sub domains cover many focus groups and the data will be shared. The applications or use-cases within the urban environment that can benefit from the realization of a smart city WSN capability. These applications are grouped according to their impact areas. This includes the effect on citizens considering health and well being issues; transport in light of its impact on mobility, productivity, pollution; and services in terms of critical community services managed and provided by local government to city inhabitants.

Utilities

The information from the networks in this application domain is usually for service optimization rather than consumer consumption. It is already being used by utility companies (smart meter by electricity supply companies) for resource management in order to optimize cost vs. profit. These are made up of very extensive networks (usually laid out by large organization on a regional and national scale) for monitoring critical utilities and efficient resource management. The backbone network used can vary between cellular, WiFi and satellite communication. Smart grid and smart metering is another potential IoT application which is being implemented around the world [38]. Efficient energy consumption can be achieved by continuously monitoring every electricity point within a house and using this information to modify the way electricity is consumed. This information at the city scale is used for maintaining the load balance within the grid ensuring high quality of service. Video based IoT [39], which integrates image processing, computer vision and networking frameworks, will help develop a new challenging scientific research area at the intersection of video, infrared, microphone and network technologies. Surveillance, the most widely used camera network applications, helps track targets, identify suspicious activities, detect left luggage and monitor unauthorized access. Automatic behavior analysis and event detection (as part of sophisticated video analytics) is in its infancy and breakthroughs are expected in the next decade as pointed out in the 2012 Gartner Chart Water network monitoring and quality assurance of drinking water is another critical application that is being addressed using IoT. Sensors measuring critical water parameters are installed at important locations in order to ensure high supply quality. This avoids accidental contamination among storm water drains, drinking water and sewage disposal. The same network can be extended to monitor irrigation in agricultural land. The network is al so extended for monitoring soil parameters which allows informed decision making concerning agriculture.

Mobile

Smart transportation and smart logistics are placed in a separate domain due to the nature of data sharing and backbone implementation required. Urban traffic is the main contributor to traffic noise pollution and a major contributor to urban air quality degradation and greenhouse gas emissions. Traffic congestion directly imposes significant costs on economic and social activities in most cities. Supply chain efficiencies and productivity, including just-in-time operations, are severely impacted by this congestion causing freight delays and delivery schedule failures. Dynamic traffic information will affect freight movement, allow better planning and improved scheduling. The transport IoT will enable the use of large scale WSNs for online monitoring of travel times, origin–destination (O–D) route choice behavior, queue lengths and air pollutant and noise emissions. The IoT is likely to replace the traffic information provided by the existing sensor networks of inductive loop vehicle detectors employed at the intersections of existing traffic control systems. They will also underpin the development of scenario-based models for the planning and design of mitigation and alleviation plans, as well as improved algorithms for urban traffic control, including multi-objective control systems. Combined with information gathered from the urban traffic control system, valid and relevant information on traffic conditions can be presented to travelers [41]. The prevalence of Bluetooth technology (BT) devices reflects the current IoT penetration in a number of digital products such as mobile phones, car hands-free sets, navigation systems, etc. BT devices emit signals with a unique Media Access Identification (MAC-ID) number that can be read by BT sensors within the coverage area. Readers placed at different locations can be used to identify the movement of the devices. Complemented by other data sources such as traffic signals, or bus GPS, research problems that can be addressed include vehicle travel time on motorways and arterial streets, dynamic (time dependent) O–D matrices on the network, identification of critical intersections, and accurate and reliable real time transport network state information [37]. There are many privacy concerns by such usages and digital forgetting is an emerging domain of research in IoT where privacy is a concern [42]. Another important application in mobile IoT domain is efficient logistics management [37]. This includes monitoring the items being transported as well as efficient transportation planning. The monitoring of items is carried out more locally, say, within a truck replicating enterprize domain but transport planning is carried out using a large scale IoT network.

V. RFID COMMUNICATION IN IOT

Radio-frequency identification (RFID) is one of the most important technologies used in the IoT as it can store sensitive data, wireless communication with other objects, and identify/ track objects automatically. RFID technology was first used in the Identify Friend or Foe (IFF) aircraft system during World War II. Compared to the traditional barcode, RFID could be applied to objects with rough surfaces, can provide both read/write capability, requires no line-of-sight contact with RFID readers, and can read many RFID tags simultaneously. All these benefits make RFID a superior technology compared to the traditional barcode system.

VI. RFID-BASED HEALTHCARE SYSTEM

In the healthcare environment, RFID technology is being used within IoT and common applications including location tracking of medical assets, newborn and patient identification, medical treatment tracking and validation, patient location and procedure management at a wellness center, and surgical process management. Fig. 3 demonstrates a typical healthcare system using RFID technology.

The rapid deployment of RFID technologies in the healthcare environment also means that we need to ensure the reliable and secure access and management of sensitive healthcare information as it is delivered over RFID systems connected to the IoT infrastructure.

Mutual authentication in RFID systems is a strong requirement that must be met to ensure secure communication between RFID tags and the server. The RFID authentication scheme should be efficient and secure against various attacks.

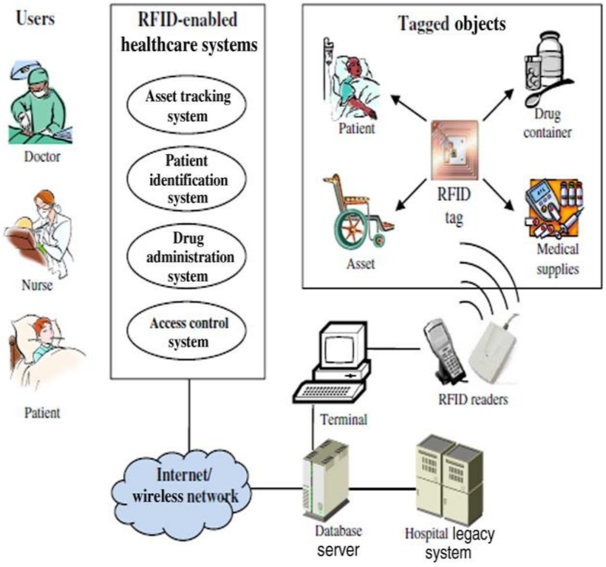

Fig.3. Typical RFID-based healthcare system.

In the past decade, many RFID authentication schemes have been proposed for a wide range of applications especially in healthcare system.

VII. RFID AUTHENTICATION SCHEME

According to cryptographic primitives used in those schemes, RFID authentication schemes can be broadly classified into nonpublic-key cryptosystem (NPKC)-based schemes and public-key cryptosystem (PKC) based schemes.

The NPKC-based RFID authentication schemes have better performance because no complex operations are needed. Therefore, many NPKC-based RFID authentication schemes, such as NP cyclic redundancy code (CRC) checksumbased schemes, simple bit-wise operations (such as XOR, AND, and OR)-based schemes, one-way hash functions-based schemes, and symmetric encryption algorithms-based schemes, have been proposed for various practical applications such as goods management, books management, identity verification, public security, road traffic administration, and electronic healthcare. Recently, the authors demonstrated that the PKC-based RFID authentication schemes are necessary for secure communication in RFID systems because many security attributes cannot be implemented by NPKC-based schemes.

With the development of microelectronic technology, some complex PKC algorithms have been directly implemented into RFID chips.

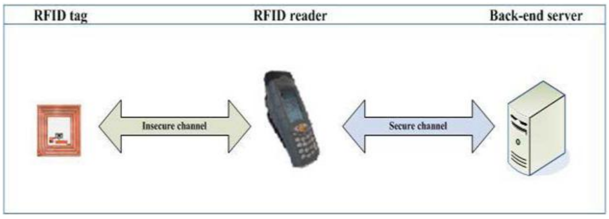

Fig. 4. Architecture for an RFID authentication scheme.

In contrast to PKC algorithms, the elliptic curve cryptography (ECC) system is more suitable for RFID system because it can provide similar security level but with a shorter key size and has low computational requirements. The low processing overhead associated with ECC makes it suitable for use with RFID tags because they have limited computing power.

Recent research results, have demonstrated that the ECC algorithm with 160 bits key size has the same security level as the RSA algorithm with 1024 bits key size. The ECC algorithms have been implemented on very compact RFID chips. Based on these implementations, many ECC-based RFID authentication schemes have been proposed for practical applications. In particular, Zhao and Zhang and Qi proposed two efficient ECC-based RFID authentication schemes that can be applied to the healthcare environment. Experimental results show that these ECC-based RFID authentication schemes are suitable for enhancing security in the healthcare environment.

VIII SYSTEM ARCHITECTURE AND SECURITY REQUIREMENTS OF RFID AUTHENTICATION

A. System Architecture

The basic architecture (shown in Fig. 2) for an RFID authentication scheme includes three entities: the RFID tag, the RFID reader, and the server. To achieve authentication between the tag and the server, some secret data are preshared between them when the system is set up.

The communication channel between the RFID tag and the RFID reader is not secure because they exchange data wirelessly and an adversary could intercept the data easily. The communication channel between the RFID read and the server is secure because a secure channel is established between them through a preshared secret key and some security mechanism.

1) ***RFID tag*****:** A tag is composed of a microchip, an antenna, and a dedicated hardware for cryptographic operations. It can store secret data for authentication and it communicates with the RFID reader. Usually, the RFID tag's computing capacity and memory storage are very limited. RFID tags could be divided into three types: passive tag, semiactive tag, and active tag [65]. The passive tag gets power through wireless signals from the reader. The semiactive tag is equipped with a small battery and gets power from it. The passive and the semiactive tags use backscatter modulation to send messages. The active tag is equipped with a small battery and a radio transceiver. It can communicate directly with the reader.

2) ***RFID reader*****:** An RFID reader is composed of a radio transmitter, a radio receiver, a control unit, and a memory unit. The main function of an RFID reader is to enable the RFID tag and the server to exchange messages between each other and achieve mutual authentication. Usually, the RFID reader's computing capacity is higher compared to that of the RFID tag.

3) ***Server*****:** A server is a trusted entity. To achieve the goal of mutual authentication, it stores all the RFID tag's identification information in its database when the system is set up. Using the stored identification information, the server could determine the validity of the tag. Usually, the server's computing capability and memory capacity are high.

B. Security Requirements for RFID Communication

RFID authentication is one of the most important steps to ensure secure communication in the RFID system. However, messages transmitted between the RFID tag and the RFID reader are exposed to many kinds of security threats.

Previous research efforts on RFID security have identified the following security requirements that must be satisfied to ensure secure
RFID communications in addition to a robust and efficient authentication scheme.

1) ***Mutual authentication*****:** It is essential that mutual authentication among the RFID tag, the RFID reader, and the server should be achieved before a session starts. In our system architecture, the communication channel between the RFID reader and the server is secure. In this case, only mutual authentication between the RFID tag and the server is required.

2) ***Confidentiality*****:** It is essential that the secret information (such as identity and password) stored in the RFID tag cannot be retrieved by the adversary when it is transmitted through the communication channels. The adversary could impersonate the tag to the server if access to the secret information is possible. The information must be encrypted before transmission.

3) ***Anonymity*****:** It is essential that an RFID authentication scheme should provide anonymity. The adversary will violate the owner's privacy and trace his/her action if the tag's identity becomes known. The tag's identity must be encrypted as part of the mutual authentication process.

4) ***Availability*****:** It is essential that the authentication process of an RFID authentication scheme be executed during the lifecycle of the RFID tag. To provide anonymity, the RFID tag and the server in most of RFID authentication schemes update the secret information shared between them when the authentication scheme is executed. If an adversary destroys the synchronization of the update, theauthentication scheme will be invalid.

5) ***Forward security*****:** It is essential that an RFID authentication scheme provides forward security. In many RFID authentication schemes, the adversary could trace back the past location of the tag if the secret information from the RFID tag is successfully retrieved by the adversary. This will seriously violate the owner's privacy.

6) ***Scalability*****:** It is essential that an RFID authentication scheme should be scalable. To authenticate the RFID tag, the server in the RFID system has to find the matching record from its database. If the computational workload of the searching algorithm increases significantly as the number of RFID tags increases, the system will not scale.

7) ***Attack resistance*****:** To guarantee secure communication within the RFID system, the RFID authentication process should be secure against various attacks including thereplay attack, the tag masquerade attack, the server spoofing attack, the man-in-the-middle attack, the tag cloning attack, and the modification attack.

IX. CONCLUSION

RFID authentication is one of the most critical security services for IoT implementations in the healthcare environment. We have presented an in-depth survey of recently proposed ECC-based RFID authentication schemes.

We identified some of the security requirements that an RFID authentication scheme should satisfy. We found that only three recently proposed ECC-based RFID authentication schemes are able to satisfy all the security requirements.

With recent advances in modern cryptography, it is wellknown that we must be able to prove that a cryptographic scheme is provably secure using a security model. However, none of the ECC-based

RFID schemes reviewed in this work proposed a suitable security model for RFID systems to demonstrate that these proposed schemes are provably secure. Most of them are still vulnerable to different types of malicious attacks. To ensure secure communication (using ECC-based techniques) in an RFID system, it is necessary to construct a suitable security model for ECC-based RFID schemes first. Then, we need to design ECC-based RFID authentication schemes, which are provably secure in the security model.

ACKNOWLEDGEMENT

The authors would like to thank the Vel Tech Multitech Engineering College for the support in realization of the project. The authors are also grateful to the anonymous reviewers for their valuable comments, which helped us to improve the quality and presentation of this paper and to the faculties of Vel Tech Multitech Engineering College for their invaluable support in deploying the system and in providing experimental data and technical documentation concerning the project.

REFERENCES

[1] Andrea Zanella, Senior Member, IEEE, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Senior Member, IEEE, Michele Zorzi, Fellow, IEEE,” Internet of Things for Smart Cities”, 2014.

[2] Debiao He and Sherali Zeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography”, IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 1, FEBRUARY 2015.

[3] Charles Deans, School of Computing and Information Technology, University of Technology, Jamaica, “The Design of an Intelligent Urban Transportation System in Jamaica based on the Internet of Things”, IEEE SoutheastCon 2015, April 9 - 12, 2015 - Fort Lauderdale, Florida.

[4] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues”, IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 3, THIRD QUARTER 2015.

[5] Sriram N. Premnath and Zygmunt J. Haas, *Fellow, IEEE, “*Security and Privacy in the Internet-of-Things Under Time-and-Budget-Limited Adversary Model*”,* IEEE WIRELESS COMMUNICATIONS LETTERS, VOL. 4, NO. 3, JUNE 2015.

[6] E. A. K. amd N. D. Tselikas and A. C. Boucouvalas, “Integrating RFIDs and smart objects into a unified Internet of Things architecture,” *Adv. Internet Things*, vol. 1, no. 1, pp. 5–12, 2011.

[7] R. Girau, M. Nitti, and L. Atzori, “Implementation of an experimental platform for the Social Internet of Things,” in *Proc. IEEE 7th Int. Conf. Innov. Mobile Internet Serv. Ubiq. Comput. (IMIS’13)*.

[8] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira, “Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation”, The Future Internet, Lecture Notes in Computer Science Volume 6656, pp. 431-446, 2011.

[9] J. Hui and P. Thubert. “Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks.” RFC6282. s.l. : IETF, 2011.

[10] N. Bui and M. Zorzi. “Health Care applications: A solution based on the Internet of Things.” In ISABEL, Barcelona, Spain, Oct. 2011.

HEMALATHA D received the BE degree in 2015 from the Anna University and pursuing ME in the department of Computer Science in Vel Tech Multitech Engineering College affiliated by Anna University, Chennai, India. Her main research interests include Internet of Things, Cloud Computing and Data Mining.

AFREEN BANU E is an Assistant Professor in the department of Computer Science in Vel Tech Multitech Engineering College affiliated by Anna University, Chennai, India. Her main research interests include Internet of Things, Cloud Computing and Big Data.