Security and Privacy Issues in IoT

Aqeel-ur-Rehman[1], Sadiq Ur Rehman[2], Iqbal Uddin Khan, Muzaffar Moiz and Sarmad Hasan

Hamdard Institute of Engineering and Technology, Faculty of Engineering Science and Technology
Hamdard University, Karachi, Pakistan
aqeel.rehman@hamdard.edu, sadiqsr@gmail.com

***Abstract*:** Internet of Things (IoT) is a global network of physical and virtual 'things' connected to the internet. Each object has unique ID which is used for identification. IoT is the emerging technology which will change the way we interact with devices. In future almost every electronic device will be a smart device which can compute and communicate with hand-held and other infrastructure devices. As most of the devices may be battery operated, due to less processing power the security and privacy is a major issue in IoT. Authentication, Identification and device heterogeneity are the major security and privacy concerns in IoT. Major challenges include integration, scalability, ethics communication mechanism, business models and surveillance. In this paper major issues related to security and privacy of IoT are focused.

***Keywords*:** Security, Privacy, IoT, Authentication, Access control, Identification.

1. Introduction

A decade ago, Kevin Ashton was the one who coined and used the term Internet of thing (IoT) for the very first time. In IoT every object whether virtual or physical is communicable, addressable and accessible through the Internet. Every object will have its own ID and has the capability to sense, compute and communicate. Pervasive nature of the objects in IoT makes data which is collected and transmitted for public and private use are very important and security of that data should be ensured. Integrity and confidentiality of transmitted data must be maintained as well as the authentication of the objects is the key aspects of IoT security and privacy.

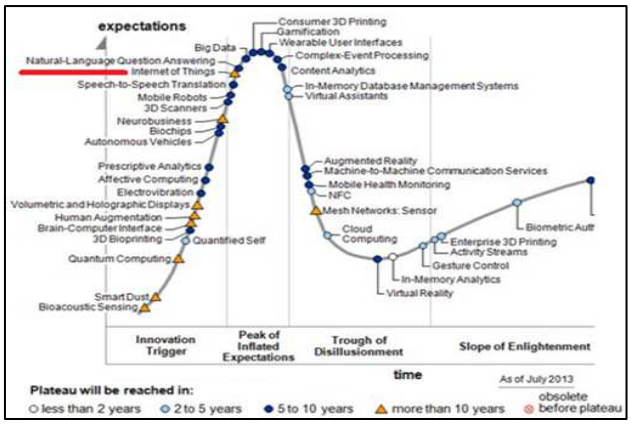

Figure 1. Gartner's 2013 Hype Cycle for Emerging Technologies [1]

Referred to Fig. 1, Hype Cycle give us the information regarding the emerging trends in which IoT marked with red line. Security and privacy is a vast topic that covers whole protocol stack. Major security issues in IoT include Authentication, Identification and device heterogeneity. With each device having its own ID, It will be very difficult to identify billions of devices. Same is the case with Authentication. Authenticating every device can be a tedious job. One of the major security concerns is device heterogeneity. There are many different types of devices in IoT and it prevents from applying single uniform security solution across the board. Every device has different security needs. Device heterogeneity can cause problems in other aspects as well.

Following is the section-wise breakup of this paper: Section 2 contains Dissimilarities in between IoT and Standard Internet. IoT technologies will be discussed in Section 3, Architectures and Applications of IoT is in Section 4. IoT protocols related to security in Section 5, Security and privacy needs of IoT along with the privacy enhancing technologies is present in Section 6. Section 7 contains major security issues. Remedy of problems regarding security and privacy issues will be covered in Section 8 and finally, Section 9 will be the Future research direction and Section 10 is going to be a Conclusion.

2. Dissimilarities in between IoT and Standard Internet

There is an obvious difference between IoT and conventional internet (referred to Table 1). The first key difference is in the deployment of these both. IoT network is commonly set-out on network with the characteristics of slow processing, limited memory and less power. This types of networks are usually know as Low power and Lossy Networks (LLNs) which encounters high data loss

Table 1. Extended Comparison between Traditional Network and IoT [2]

Topic	Traditional Internet	IoT
Who creates contents?	Human	Machine
How is the content combined?	Using explicitly defined links	Through explicitly defined operations
What is the value	Answer questions	Action and timely information
What was done so far?	Both content creation (HTML) and content consumption (search engine)	Mainly content creation
Type of Connections	Point-to-point and Multipoint	Only Multipoint
Digital Data	Readily available	Does not generate unless augmented or manipulated
Technology Concept based on	Both Physical-fist and Digital-first	Physical-first

3. IoT Technologies

Some of the core technologies of IoT includes Radio Frequency Identification known as RFID, NFC which is called as Near Field Communication and WSN which the full form of Wireless Sensor Networks. Extended table for the IoT Technologies taken from [12] is present in Table 2 and Table 3, show the comparison of different IoT Wireless Technology.

3.1 Radio Frequency Identification (RFID)

The major technology used in IoT is Radio Frequency Identification and works as discussed in [3, 4]. In [5], details regarding components of RFID are mentioned. RFID is of two categories, Active RFID and Passive RFID. Due to advancement in RFID technology, IoT became a reality. All objects in IoT are equipped with identifiers and smart tags which makes them manageable with the help of computers. IoT objects have microprocessor or smart chip that give the object capability to sense information from environment around it, compute and then communicate information to other objects or to humans. A detail concept regarding RFID working technologies are presented in [6]. Ultra-lightweight RFID authentication protocol has been discussed in [7] with the proposed attacks and their security claims along with the pitfalls in the designs on ultra-lightweight authentication protocol.

3.2 Wireless Sensor Networks (WSN)

When there is a need for remote sensing application and information gathering, WSN is commonly used. These networks are cost effective, good in efficiency and consume low power [8]. Comparing RFID and WSN, both have features that are common in each other. However, WSN have the edge due to its intelligent and processing potentials. In [9], challenges that should be resolved to determine the strength of WSNs are mentioned. Moreover, in [10] Deterministic Algorithm has been proposed which can be used to solve problem of coverage for commonly known regions with the help of WSNs

3.3 Near Field Communication (NFC)

This is the core technology of IoT which came into use when there is a need to communicate within the distance of few centimeters with the low power and data rate requirement. Such technology supports, especially for the case of internet of things, numerous services for example smart cards, transport, access control etc. [11]

Table 2. Extended Table for the IoT Technologies [12]

Communication Technologies
NFC, RFID, Bluetooth, ZigBee, ZWave, IEEE802.15.4, WiFi, 3G/ 4G, LTE, , WiMAX, Weightless, DASH7, PLC, QR Code, Ethernet
Prototype Hardware
Raspberry Pi, Hackberry, Arduino Yun, Arduino Uno, PCDuino, the Rascal, Cubie Board, BeagleBone Black,
Identification Techniques
IPv6, AIDC, RFID, QR Code, barcode etc.
IoT Architectures
3-Layer, 5-th layer, IoT-A, BeTaaS, OpenIoT, IoT@Work, IOT-I etc.
Operating System
Tiny OS, Contiki, Mantis, Nano-RK, LiteOS, FreeRTOS,
Protocol
IPV6, 6LOWPAN, UDP, Chirp, DTLS, XMPP-IoT, SSI, NanoIP , MQTT

In conclusion we can say that different communication technologies (see Table 3) are being used depending upon the application and their factors like range, data, security, power consumption, battery life requirement. WiFi standard IEEE 802.11 ah [13] and LoRa [14] with the standard IEEE 802.15g are considered to be the most recent technologies for IoT. The good thing about them is they are having feature of extended range, with acceptable data rate.

4. Architectures and Applications of IoT

Internet of Things cover the vast range technologies, due to this reason it is not possible to consider one single IoT architecture as a reference architecture that can be used for all IoT operations. Therefore, the probability of having different reference architectures to be merge-up for creating required IoT architecture is very high, this means there is no standard architecture of IoT and different architectures are used according to the requirements. Architecture that provides easiness in deployment and makes the usage more desirable is considered to be an ideal architecture of IoT[15].

Table 3. IoT Wireless Technology Comparison

	Bluetooth (BLE)	**ZigBee**	**Wi-Fi**	**Wi-Max**	**LoRa**	**LTE**	**Z-Wave**
Standards	IEEE 802.15.1 IoT Interconnect	IEEE 802.15.4	IEEE 802.11 ah	IEEE 802.16	IEEE 802.15g	3GPP	Z-Wave alliance
Network Type	P2P	Mesh	WLAN	MAN	LPWAN	GERAN /UTRAN	Mesh
Power Consumption	10 mW	30mA TX1, Standby 3# 956; A (low)	400+mA TX1 Standby 20mA (High)	N/A	Very low power	5W / 1 W	Very low power
Data rate (Mbps)	1	0.25	Min 150 kbps	70	250 kbps	0.1-1 Gb/s	0.1
Range	35 m	10-100 m	1 Km	50 km	100 Km	28 Km/ 10 Km	30 m
Spectrum	2.4 GHz	2.4 GHz	2.4-5 GHz	2 – 11 GHz	868-915 MHz	700-2600 MHz	908.42 MHz

IoT architecture is in evolutionary process. The data volume is extensively high in IoT as compare to the traditional

internet. Some key elements which includes flexibility, QoS, privacy, reliability, security, universality, interoperability etc. should always be kept in mind while developing a new architecture for IoT.

In [16] [17], a generic architecture model has been proposed with the concerns like scalability, reliability, and QoS are under discussion. At a moment, there are two proposed layered based IoT architectures namely 3-layer and 5-layered architecture.

3-layer architecture model was the very first model that has been accepted/ obtained for IoT purpose. This 3-layer architecture model is based on Perception, Network and the Application Layer respectively. The functionality of these layers are as follows, Perception layer, responsible for identification of object and information gathering. Moreover, the devices like camera, two dimensional bar coder reader, GPS, Tags of RFID etc. are incorporated on this layer. Network layer is counted as an essential layer and work as a neural network for IoT. Processing and transmission of data that has been received from perception layer is the key responsibility of this layer. Moreover, this layer is comprises of convergence network, intelligent processing, management of network and information centers. It is the responsibility of Application layer to combine both IoT's social division and industrial requirements. The main objective of this layer is to give informational service consisting of three parts that are IoT client side, data storage and data inquiry module.

The 3-layered explains the detailed structure of IoT from the technical perspective. Various Experts and Scholars believes that Internet of Things is a cloud-castle vision approach due to lack of management and business methodology and therefore more focus need to be done for the better approach towards management and business models. As compared to Internet technology, IoT network can be controlled and managed and is more similar to communication network. In order to study the correct IoT system, structure, the internet and communication network need to be analyzed and combine the features of both networks to achieve the goal of having more improved and decent IoT architecture

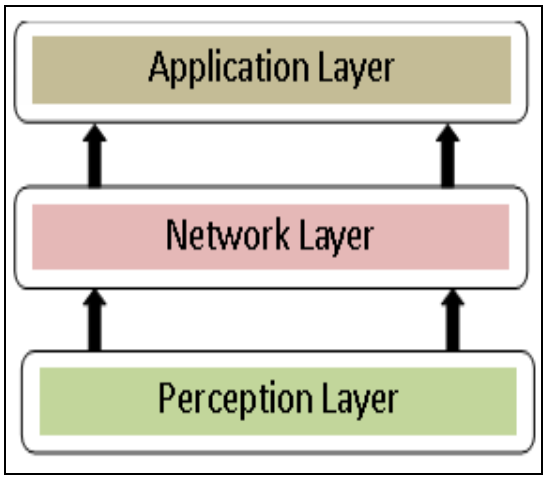

Figure 2. 3-Layered Architecture of IoT

Since the IoT 3-layer architecture (see Fig. 2) which was proposed earlier lacks expected IoT development. Therefore, a much well-defined 5-layer architecture model is proposed. This architecture model is highly recommended by experts with the strong believe that it will illustrate all IoT features accordingly. The architecture contains 5 layers (see Fig. 3) known as Perception Layer, Transport Layer, Processing Layer, Application and Business Layer

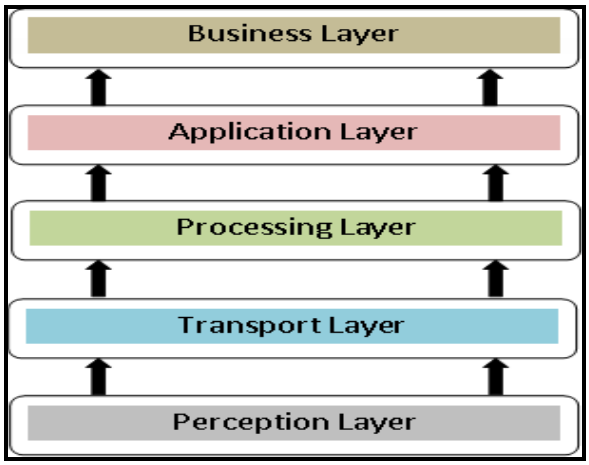

Figure 3. 5-Layered Architecture of IoT

The layer which is responsible for the identification of physical properties (e.g. location, temperature etc.) with the help of using various sensors used in IoT and performing conversion of signal to digital signal according to the transmission network is *Perception layer*. Sensing technology is the major technique for this layer which includes technologies like RIFD, GPS, 2-D barcode and so on.

The *Transport Layer* which is often called Network Layer in 5 layer architecture used for the purpose of transporting the received data to the processing centre. This transportation takes place through different network. IPv6 is considered to be the key protocol for this layer and FTTx, 3G, Wifi, Bluetooth, ZigBee, infrared technology are the important techniques used on this layer.

In *Processing Layer*, all the data transmit from the transport layer is further store, process and analysed. Database, intelligent processing, cloud computing, ubiquitous computing, etc. are considered to be the prime approaches on this layer. Experts believe that the future development and research of Internet of Things can be done on processing layer.

Application Layer's tasks are very much depended on the data from processed layer. The goal of application layer is to create the distinct IoT applications. Intelligent transportation, logistics management, identity authentication etc. are the examples of IoT applications. Application layer is also responsible for providing applications to industrial usage.

The *Business Layer* performs managing task like management of applications and business model. Realising and charge management of different application is not only a task of this layer but also the research on two model namely business and profit [17].

Based on this approach, the IoT cannot be efficient without the research of a long term development on Business model.

The business layer is also responsible about the user's privacy and all research related to IoT applications [18].

There are also some special purpose IoT architectures which are present in [17, 19, 20, and 21]. Multimedia traffic security architecture is discussed in [22]. Clock synchronization architecture of network for IoT is in [23] and is used to eliminate the issues of managing IoT nodes. There are three level in this architecture, adaptation level, organization level and region level. Architecture model for

trusted security systems is presented in [24]. There are some more architecture [25, 26, and 27] which are used for special purposes, the negative point regarding these architectures is that they cannot be treated as standard architectures.

Table 4. EU FP7 research IoT architectures and security requirements [30]

	IoT Architectures			
Requirements	IoT-A	BeTaaS	OpenIoT	IoT@Work
Network security				
…Confidentiality	✓	✓	✓	✓
…Integrity	✓	✓	✓	✗
…Authenticity	✓	✓	✓	✓
…Availability	✗	✗	✗	≈
Identity management				
…Authentication	✓	✓	✓	✓
…Authorization	✓	✓	✓	✓
…Accountability	✗	✗	✗	✓
…Revocation	✓	✗	✗	✓
Privacy				
…Data privacy	≈	✗	✗	≈
…Anonymity	✗	✗	✗	✓
…Pseudonymity	✓	✗	✗	✓
…Unlinkability	✓	✗	✗	✗
Trust				
…Device trust	✓	✓	✓	✗
…Entity trust	✓	✗	✓	✗
…Data trust	✗	✓	✗	✗
Resilience				
…Robustness	✓	✓	✗	≈
…Resilience	✓	✓	✓	≈

During EU FP7 research projects, Internet of Things Architecture (IoT-A), Building the environment for the Things as a Service (BeTaaS), Open source cloud solution for the Internet of Things and (OpenIoT) and Internet of Things at Work (IoT@Work), were the IoT architectures that was presented. These selected IoT architectures are commonly followed by huge number of academic researchers and industrial partners.

IoT-A [28] is business driven architecture which generates different reference architectures depending on domain specific requirements. IoT-A domain includes Users, Services, Physical/virtual objects, resources and devices (sensors and tags). IoT-A outlines the rules for design of protocols and algorithms for IoT. There are about five security components in IoT-A [29].

When there is a requirement for the communication in between machine to machine (M2M), IoT architecture named as BeTaaS is proposed. BeTaaS is founded on the reference model named as Things of Service (TaaS) [31]. In this architecture, four layers are presented namely physical layer, adaptation layer, TaaS layer and Service layer. BeTaas provides identity management [32] and privacy.

The EU FP7 OpenIoT is a research project from the year 2012-2014 which has introduced IoT architecture [33], [34]. This architecture model is constructed from the reference model defined in IoT-A. Main focus of OpenIoT is on providing the infrastructure that is cloud-based middleware. There are two security modules presented in OpenIoT architecture specification [35], namely security & privacy module and trust module.

IoT@work is a project by European Commission which was completed in the year 2013. The main purpose of this architecture model is to create the industrial automation domain [36]. Most shining features of this architecture model is to provide reliable network communication, security via protocol discussed in [37], auto-configuration etc. The layers in architecture of IoT depend upon its area of deployment. The first layer is a complex hardware layer comprises of medical sensors, sensor networks, RFID tags and readers.

This layer controls identification, data storage, data collection, communication and control services .Middle layer acts as a bridge that connects hardware layer with application layer. Middle layer handles object management, data filtering, data aggregation, access control. Application layer handles delivery of different applications to different users [38].

Referred to Table 4, it is important for all the architectures of IoT to provide network security, trust, reliance, privacy and identity management as different devices and networks are connected with each other and data integrity is on risk. Data authentication is also the key parameter that should be addressed by selected architecture

Applications of IoT can be categorized by various factors such as network coverage, Impact on users, network availability, user involvement etc. There are four major types of IoT applications namely Short Area, Enterprise, Data Collection and Mobile. The biggest difference which sets the major applications types apart is the scale on which they operate. The main differences are shown in table 5.

Data in Short Area is mostly private information about the user usually health care related information which must not be disclosed to anyone or some multimedia device Information. Data collection application is also very critical because it holds the details about the nation's major installations such as nuclear power plants, power grid and

Table 5. Major Applications and their scope

Standards	**Sprawl**			**Possible Fields**			
	Personal	**Community**	**Large Area**	**Medical**	**Sensor Network**	**Sports**	**Multimedia**
Short Area	Yes	No	No	Yes	No	No	Yes
Enterprise	No	Yes	Yes	Yes	Yes	No	No
Data Collection	Yes	Yes	Yes	Yes	Yes	Yes	No
Mobile	No	Yes	Yes	Yes	Yes	Yes	No
Short Area	Yes	No	No	Yes	No	No	Yes

water supply network. Supply blockage or damage to these installations can disrupt life of that country because country's population depends on these supplies to fulfil their daily needs [39].

Mobile application is vulnerable due to its open and mobile nature and is more open to attacks compared to other areas of deployment. On the other hand, any security loophole in enterprise application domain can completely destroy the business. Factories use different sensors for security purpose. Any security mishap can lead to a big disaster like if the information get into wrong hands, it will damage the factory.

5. IoT Protocols related to Security

As now we have a clear understanding that IoT cover the vast range of application products, the number of protocols that are adding in IoT are keep on increasing. Protocols used for high level are assigned to the certain vendors which provide the room for the selection of different capabilities and features. In this section, focus will be on some certain IoT protocols that are used for the feature of security. Table 6 represent the comparison on IoT Protocols

QUIC (Quick UDP Internet Connections, pronounced quick). This protocol uses the User Datagram Protocol (UDP) and support a group of composite connections that are present in between two endpoints. QUIC have the ability to give the security protection just like Transport Layer Security or like Secured Sockets Layer with the feature of minimizing transport latency and no of connections. QUIC is also designed to estimate the bandwidth in either direction so that congestion problem should be avoided.

Table 7: Comparison between IoT Protocols related to Security

Features	QUIC	DTLS	AMQP
Layer	Transport	Transport	Application
Security	Yes	Yes	Yes
Interoperability	Yes	Partial	Yes
Manageability	Yes	No	Yes
Objective	Composite connections	Communication privacy for UDP	Message Orientation
Delivery	Not guaranteed	Not guaranteed	Guaranteed
UDP/TCP	UDP	UDP	TCP

DTLS (Datagram Transport Layer) – this protocol is responsible for providing the communication privacy for UDP. With the use of DTLS, client/server applications are eligible to prevent issues like message tampering, message forgery or eavesdropping. The base of DTLS protocol is TLS which is used for the purpose of providing security. Table 7 presents the comparison between IoT Protocols related to Security

Table 6. Comparison on IoT Protocols [40]

Protocol	*Transport*	*Messaging*	*2G,3G,4G (1000's)*	*LowPower and Lossy (1000's)*	*Compute Resources*	*Security*	*Success Stories*	*Arch*
Azure-IoT	AMPQ or Https/TCP	Rqst/Rspnse	Excellent	Good	10K-100Ks RAM Flash	High-Manditory	Weraables	Client-Server
CoAP	UDP	Rqst/Rspnse	Excellent	Excellent	10Ks/RAM Flash	Medium - Optional	Utility field area ntwks	Tree
Continua HDP	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	None	Medical	Star
DDS	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Poor	100Ks/RAM Flash +++	High-Optional	Military, Industrial	Bus
DPWS	TCP		Good	Fair	100Ks/RAM Flash ++	High-Optional	Web Servers	Client Server
HTTP/ REST	TCP	Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	Low-Optional	Smart Energy Phase 2	Client Server
MQTT & MQTT-SN/S	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	Medium - Optional	IoT Msging	Tree
SNMP	UDP	Rqst/Response	Excellent	Fair	10Ks/RAM Flash	High-Optional	Network Monitoring	Client-Server
Thread	UDP	Rqst/Rspnse	Excellent	Excellent	10Ks/RAM Flash	High-Manditory	Nest?	Mesh
UPnP	UDP	Pub/Subscrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	None	Consumer	P2P Client Server
XMPP	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	High-Manditory	Rmt Mgmt White Gds	Client Server
ZeroMQ	UDP	Pub/Subscrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	High-Optional	CERN	P2P

6. Security and Privacy Needs

IoT devices have scarce resources so we cannot use complete security suites. We have to design special security framework or choose from existing solutions. We have to look towards lightweight security solution to make IoT secure because this will put burden on device resources. Core Security threats in IoT Technologies taken from reference [14] are shown in Table number 8.

6.1 Requirements

IoT architecture will always impact privacy and security of users. Privacy is to make sure that the user information is hidden from prying eyes. Privacy of the user is his/her personal right. The attribution of tags to objects is not known to users, and there is no audio-visual signal to indicate object's user. Thereby, users can be followed without their knowledge about it and traces of their activities on the internet. The state and marketing enterprises makes matters even worse by collecting these types of private user data and using it for their own purposes without the knowledge of the user. Table 8 gives the summary of core Security threats in IoT Technologies that has been referred from [14]. Following are the major security and privacy requirements of IoT to be fulfilled:

6.1.1 User privacy

Steps must be followed so that the information provider is able to abstain from observing the use of the lookup system related to a user. Enhancing user privacy and security on every layer is now becoming the major requirement.
For the purpose of privacy management in Internet of Things, a data tagging is proposed in [42] and for the reason to preserve important data, [43] illustrate the privacy model named as k-anonymity model. In [44], there is an analysis on the privacy risk in the situation when fixed domain name is given to a certain node of IoT.

6.1.2 Access control

Information service provider must apply any access control mechanism to protect data from misuse and damage of private information of a user by others. Data must be only accessible to those who it belongs to [45].
There are two terms which are in [46], defines Access Control. These terminologies are namely Data holder and Data collector. Problems related to the authentication for outsourced data stream can be seen in [47]. For the case of streaming data, access control is specified in [48].

6.1.3 Identity management

It is a vast administrative area that deals with identifying object by using different techniques in a system and controlling their access by associating user rights and restrictions with the recognized identity [45].

6.1.4 Secure data communications

Securing data communication is a major part of IoT security. It includes authenticating communicating objects, ensuring confidentiality and integrity of communicated data and protecting the identity of communicating objects [45].

6.1.5 Resilience to attacks

In the open and connected world of IoT, attackers can easily find and exploit any vulnerability in the system. System must have any mechanism to protect against such attacks. It should have to protect against single point of failure and must adjusts in case of node failure. It should have the capability to fight against different types of attacks.

6.1.6 Trust

This is also one of the essential requirements for IoT as trust is highly dependable on the quality of data. Trust can be decomposed into device trust, entity trust, and data trust [49].

Table 8: Core Security threats in IoT Technologies [14]

	Threats	Key Components	Security Need
RFID	DoS Attacks	RFID Tags and Reader Communications	Encryption
	Eavesdropping	User Private Data	Encryption
	Skimming	User Private Data	Blocking Tags
	Relay Attack	Authentication Result	Synchronization
	Side Channel Attack	User Private Data	Authentication
	Hardware Destruction	Tags	Protective Electronic Component
NFC	Phishing Attack Interfaces	Application Processor	Authentication
	User Tracking	User Privacy	Random UIDs
	Relay Attacks	Tag / Reader	Synchronization
	Data Forging Attack	User Data	SSL Communication
WSN	Wormhole	Multi-hop Wireless Network	Time limit on Packets Delivery
	Neighbor Discovery	Network Discovery Protocol	Authentication Supported Protocol
	Spoofing	Wireless Network Packet	Authentication
	Ping Flood, ICMP Flood, Syn Flood	Network Nodes	Use of IDS

6.1.7 Mobile security

There is a continuous movement of mobile nodes from one cluster to the other cluster in IoT. For this purpose a cryptography based protocol is frequently used to permit protection for authentication, privacy and identification. In the scenario when the mobile node connects with the new cluster an ad-hoc protocol in [50] has been discussed. This protocol has the ability to rapidly provide the above mentioned protections and guard against attacks like replay attack, eavesdropping, and tracking or location privacy attacks [51].

6.1.8 Secure middleware

In IoT, as there are different types of devices interacting with each other which in results involves several types of middleware layers that will affect the security and integrity of data and device used within the same network.
In IoT, data is provided by establishing the interaction among machine-to-machine, consumers and machines and users. Due to this reason designing and creation of middleware is of essential importance with respect to security concerns.

6.2 Privacy Enhancing Technologies

Privacy of the user data is a major concern in open world of IoT and it should be protected on every cost. To enhances the privacy of user personal data there are few technologies that can be used and mentioned in [52]. Some of them are as follows:

6.2.1 Transport layer security

Transport Layer Security (TLS) can increase confidentiality and integrity of data in IoT. The major issue in Transport layer security is that each object needs a new TLS connection searching for information, can be halted by many additional layers and also create a big system overhead.

6.2.2 Encryption

As major IoT enable devices will be battery operated, keeping this constrains along the use of low processing power algorithms, encryption can be done for data integrity throughout transporting of data.

6.2.3 Virtual private network

Virtual Private Network (VPN) is networks that can be accessed from outside formed by close group of partners. Only partners can access the system and they promise to make personal data confidential and data integrity is maintained. Virtual private network does not provide facility of dynamic global information exchange and you are bound to a limited area which makes this privacy enhancing technique ineffective.

6.2.4 Onion routing

Onion routing is another privacy enhancing technique which encrypts and merges internet traffic from various sources. In Fig. 4, it can be seen that working is done by warping data into the numerous layers of encryption. Public key of onion routers on the transmission path had to be used. This process can hamper matching of internet packets to a particular source.

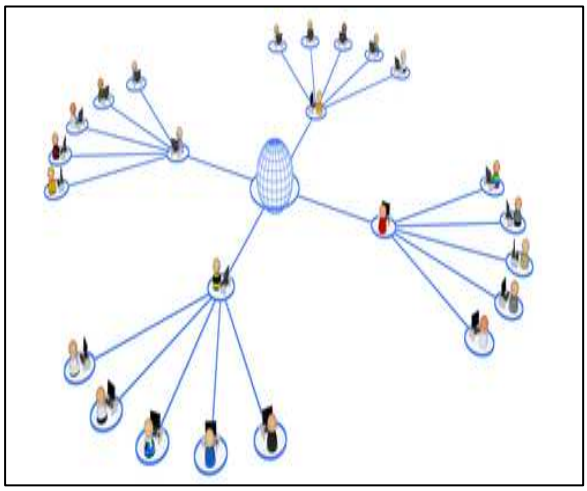

Figure 4. Onion Routing

7. Major Security Issues

Internet has evolved from Internet for computers to IoT with machine to machine communication feature. For the reason of making IoT feasible for wider adoption, it is important to make it low cost and increase the number of supported devices. There are some technical as well as security issues that need to be solved before achieving the goal of wider IoT adoption.

Technical issues of IoT include Energy, Wireless communication, Scalability, Security etc. Here the discussion is about security related issues in IoT. Some of the major security related issues are;

7.1 Identification

Identification per device is required, whether it is original or some malicious node. Some reference of a manufacture is needed to be available.

7.2 Authentication

Authentication in IoT is one of the biggest issues due to the number of devices. Authenticating each and every device is not an easy job to accomplish. Due to the features of rapid computation and energy efficiency, based on private key cryptographic primitives, many security mechanisms have been proposed.

7.3 Data Management

Identification of billions of devices and their addressing can be considered a major problem in IoT. According to estimates, by the year 2020 more than 50 billion devices (refer to Fig. 5) will be smart devices and connected to the internet [53]. Managing the devices and their addressing will be difficult even for IPv6.There are methods that can be used for identification of the objects in IoT. Some of them are Bar code identification, Vision based object identification etc. RFID and NFC technologies are used for scanning purposes.

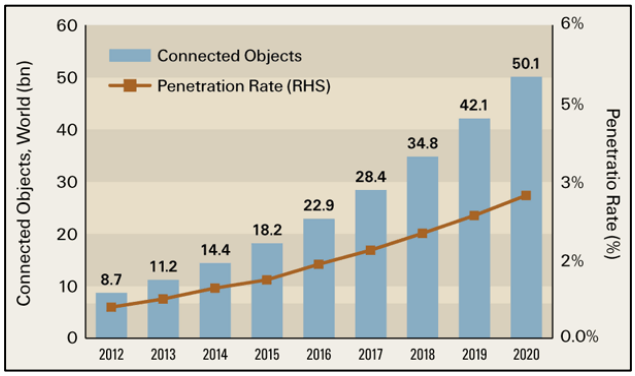

Figure 5. The No. of Connected Objects Is Expected to Reach 50 Billion by 2020 [53]

7.4 Heterogeneity

The biggest security and privacy issue is by far the issue of device heterogeneity. Problems need to be tackled properly to make IoT more secure and reliable. Managing hundreds different types of devices with each have their own security issues and requirements. Each object needs to be tackled differently which makes it difficult to apply a single solution to all. It will be a tough task to secure every types of device from different types of attacks. It makes it harder to manage the objects.

Each device needs is to be fulfilled to keep it functioning. Communication between different types of devices can also

be a major issue. Each device communicates and works differently as compared to other device. Device heterogeneity can affect many other aspects as well such as difficulty in integration, privacy, identification etc. In [54], authors have presented the method for a security incidents detection and investigation in IoTs. With the help of this method detection of attacks (known or unknown) in IoTs are possible.

8. Remedy of Problems

Solutions to different issues related to security and privacy of IoT are as follows:

8.1 Identification

Identification of devices can be done by considering their physical / hardware addresses of by deploying via IPv6 as identification is necessary for further proceeding towards Authentication and Data Management. Some pre-loaded scales of identification provided by manufacturer can be saved in data base of Identification and authentication server.

8.2 Authentication

Authenticating large number of devices in real time is an issue, to overcome this various schemes and algorithms of handshaking and pre-shared keys for low power are available. RFID plays main part in the identification of objects. It uses electromagnetic induction and propagation of electromagnetic waves to identify objects. From security point of view, RFID can also be used against reproduction, combined encryption, and securer data on document, certificate, and other elements for the purpose of anti-counterfeiting and their control and management [55].

A scheme used for authentication of devices in IoT is one where user nodes are authenticated but it is not lightweight and can put a dent on battery life and performance. Another method used is the handshake process. This process utilizes a bit amount of time and concept of symmetric key cryptography. A public key cryptography based solution overcomes these challenges because of its high scalability, low memory requirements and no requirement of key pre-distribution infrastructure [56].

8.3 Data Management

Most common and low power is Bar code identification technique is fast and accurate. It has low error rate and gives output quickly. Bar code scanner scans the bar code and the information contained in the bar code will transfer the data, which can be recognized by computers.

Another useful solution is vision based identification.

It performs matching of the features which are select to recognize the objects. There are two approaches local and global. Local approaches search for salient regions such as corners or entropy. Global approach considers the complete details of an Image [57]. To manage all the data as for authentication and identification as well as device's transmission in case of any sensor network or may be medical need, is hectic and use of SQL Lite on some multi-core hand held device can be possible.

8.4 Heterogeneity

To remove the issue of heterogeneity, IDRA architecture must be used which is specially designed to integrate all the devices. IDRA can connect objects directly without any gateway. It supports backward compatibility and needs fewer resources. IDRA can interpret an incoming packet type and drop unrecognized packets. IDRA supports communication between devices that uses different MAC protocols. The best thing about IDRA is that memory and processing overheads are negligible. IDRA reduces cost significantly. IDRA transparently supports 'best connected' strategy between different technologies at all network levels.

Since in IoT we can aspect the heterogeneous network, for such a case different devices needs to communicate with each other and also need to communicate with humans. A method has been proposed in [58] by Aggarwal which is used to provide security for devices using RFID technology for communication. Such a method has a drawback that it is unable to provide security for data. Another security method named as risk analysis is used in Intelligent Transport System (ITS). In this method, a key (public key) infrastructure is used to provide certificates for the authorities so that the prevention of data for being interrupted can be ensured.

As encryption is an important factor in the field of data security. For IoT, a KPI-like protocol [59] was presented by Zhihua Li. This protocol is used to encrypt the routers (for source and destination data flow). Decryption is performed by using the key.

Summary is provided in Table 10 which is the partial table taken from [60] which covers most of the existing methods under the heading of security and reliability for IoT along with their possible limitations. IoT Major Problems and their Solutions are in Table 9.

Table 9. IoT Major Problems and their Solutions

Areas	Observed Problems	Available Solutions
Identification	Per device Identification	Hardware address Use of Ipv6
Authentication	Authentication of Larger Number of devices in real time	Handshake process Public key cryptography
Data Management	Management of preloaded data Validating changes time to time	SQL Lite
Heterogeneity	Communication Between different types of device Latency and processing speed	IDRA architecture

Table 10: Existing Methods And Their Limitation Form Providing Security and Reliability for IoT [60]

Method	Issues it addresses	Solution	Limitations
RFID Tags (Radio Frequency ID)	Not being able to connect devices	RFID tags can be installed/embedded into smart objects to allow fast communication between devices	While RFID tags are useful for providing security, they are also very prone to hacking as more and more RFID banking applications are becoming susceptible to" RFID hacking"
Identity Management Framework Method	Authenticating data that travels between the device and the cloud	Place an Identity Manager and Service Manager on the devices	The protocols to develop the method have not yet been implemented
ITS Security Methods and Standards for Efficiency – Risk Analysis	Address threats to the ITS or Intelligent Transportation System (i.e. smart transportation)	A public key infrastructure is used in that certificate authenticating (CA's) are used for managing and monitoring security credentials for the network nodes on ITS to devices to prevent data from being interrupted	Technology is still being developed
Authentication and Control	Fixes loopholes in device security and data integrity	A user requests authentication to access a device, things ask for permission to do so from a "Registration Authority", RA approves device to send user a question, if response is OK, user is authenticated access to the device	Systems are still very vulnerable to Man in the Middle attacks and Eavesdropping attacks
PKI – Product Key Infrastructure	Threats involving node security	Nodes are authenticated by an "offspring node" that sends a decryption key when the node is safely transmitted. Offspring node still continues to be improved and developed.	Encryption is not fast
Preference Based Privacy Protection Method	Issues in data privacy	A third party entity evaluates the user's security and privacy preferences and reports it to the service provider that gives the user an appropriate security level based on its sensed preferences before it connects the device to the Internet of Things.	The security mechanism and levels at which to set privacy still require more development as the Internet of Things is fairly new
SMSC	Scalable security model for IoT infrastructure	Scalable security enhancement system of the SMC model for distributed resources	This generic model needs to validated for specific applications and security objectives
DSM	Security metrics Information systems	For the development of security metrics, they propose five elements that deal with security analysis and policies in general	Fail to address the methods for the identification, collection, computation or the application of the security metrics to address the security issues and objectives.

9. Future Research Directions

With the goal to achieve security and privacy in IoT, significant need of research is needed. Some of the key areas for research mentioned in [61] are namely Scaling, Architecture and Dependencies, Utilization of Big Data, Robustness, Openness and off-course Security and Privacy. Since in IoT large numbers of devices are connected together which in result affects the utilization of system, therefore, scaling of a system is required and research work need to be done in this domain for the successful working of IoT. Since there is no standard architecture for IoT and billions of objects are getting attached with the traditional internet day by day, it is very much important to have an architecture which is adequate in nature and allows easiness in connectivity, communication and control.

As suggested by A. Sardana and S.Horrow [54] devices that are used in IoT needs to contain an Identity Manager, but there is still a need for fast encryption, research is suggested to have a better method as compared to the existing one. Identification of privacy requirement is a key in IoT, a research work need to be done in this domain also so that the IoT system can be kept away from privacy related threats

More work suggestion could be on the issue of heterogeneity as in IoT there are different interconnections and at the moment there are many issue in its implementation. There should be research on expected data transmission, storage and capacity issues as with the passage of time number of devices will get increased on IoT.

10. Conclusions

IoT will become the core component of Future Internet. Thanks to its sensing and actuating capabilities which makes it unique. It acts as a bridge to connect both real and virtual world. However, a large number of information security and privacy problems appear that needs to be considered before

applying IoT. As the objects become smarter, the pace of the development also become more prevalent to ensure that these objects can co-exist in seamless and non-hostile environments equally well. This paper puts major emphasis on Security and privacy issues of IoT but also discussed many other aspects of IoT such as applications, architecture and many more.

References

[1] Gartner‘s Hype Cycle Special Report for 2011, Gartner Inc. http://www.gartner.com/technology/research/hype-cycles/, 2012.

[2] Differences between the IoT and Traditional Internet by Dr. Opher https://www.rtinsights.com/differences-between-the-iot-and-traditional-internet/ [Accessed: 11-Oct-2016]

[3] Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M. and Borriello, G., “Building the internet of things using RFID: the RFID ecosystem experience,” IEEE Internet Computing, Vol. 13, No. 3, pp.48-55, 2009.

[4] Juels, Ari. "RFID security and privacy: A research survey," IEEE journal on selected areas in communications, Vol. 24, No. 2, pp. 381-394, 2006.

[5] Shen, Guicheng, and Bingwu Liu. "The visions, technologies, applications and security issues of Internet of Things," In 2011 International Conference on E-Business and E-Government (ICEE), 2011.

[6] Rolf Clauberg. “RFID and Sensor Networks: From Sensor/Actuator to Business Application,” RFID Workshop, University of St. Gallen, Switzerland, September 27, 2004.

[7] Umar Mujahid Khokhar, Muhammad Najam-ul-islam, "Pitfalls in Ultralightweight RFID Authentication Protocol,” International Journal of Communication Networks and Information Security (IJCNIS), Vol. 7, No. 3, p. 169, 2015

[8] J.Yiek, B.Mukherjee, “Wireless Sensor Network Survey,” Computer Networks, Vol. 52, pp. 2292–2330, 2008.

[9] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless Sensor Networks: A Survey,” Computer Networks, Vol. 38, pp. 393–422, 2002.

[10] Franco Frattolillo, "A Deterministic Algorithm for the Deployment of Wireless Sensor Networks,” International Journal of Communication Networks and Information Security (IJCNIS), Vol. 8, No. 1, 2016.

[11] Urien, P, “LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of things,” In Proceedings of the IEEE consumer communications and networking conference (CCNC 2013), pp. 845–846, Las Vegas, USA, 2013.

[12] Laeeq, Kashif, and Jawwad A. Shamsi, "A Study of Security Issues, Vulnerabilities and Challenges in Internet of Things," Securing Cyber-Physical Systems, p. 221, 2015.

[13] Sun, Weiping, Munhwan Choi, and Sunghyun Choi, "IEEE 802.11 ah: A long range 802.11 WLAN at sub 1 GHz," Journal of ICT Standardization, Vol. 1, No. 1, pp. 83-108, 2013.

[14] LoRa Alliance, "A technical overview of LoRa and LoRaWAN,” White Paper, November 2015.

[15] "What Exactly Is The "Internet of Things"?" Internet: http://postscapes.com/what-exactly-is-theinternet-of-things-infographic, [Accessed: 17-Oct-2016].

[16] Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S., "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," 10th International Conference of Frontiers of Information Technology (FIT), pp.257-260, 17-19 Dec. 2012.

[17] Miao Wu; Ting-Jie Lu; Fei-Yang Ling; Jing Sun; Hui-Ying Du, "Research on the architecture of Internet of Things," 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Vol.5, pp.V5-484-487, 20-22 Aug. 2010.

[18] Said, Omar, and Mehedi Masud, "Towards internet of things: Survey and future vision," International Journal of Computer Networks, Vol. 5, No. 1, pp. 1-17, 2013.

[19] Jinxin Z., Mangui L., “A New Architecture for Converged Internet of Things,” International Conference on Internet Technology and Applications, Beijing, China, pp.1-4, 2010.

[20] Zhang J, Liang M., “A New Architecture for Converged Internet of Things,” IEEE International Conference on Internet Technology and Applications, Wuhan, China, pp.1-4, 2010.

[21] Inge G., “Architecture for the Internet of Things (IoT): API and interconnect,” 2nd International Conference on Sensor Technologies and Applications, Cap Esterel, France, pp. 802-807, 2008.

[22] Liang Z., Han-Chieh Chao, “Multimedia Traffic Security Architecture for the Internet of Things,” IEEE Networks, Vol. 25, No. 3, pp. 35-40, 2011.

[23] Junwei Lv, 11, Xiaohu Yuan and Haiyan Li, “A New Clock Synchronization Architecture of Network for Internet of Things,” International Conference on Information Science and Technology, Nanjing, Jiangsu, China, pp. 685-688, March 26-28, 2011.

[24] Xiong Li, Zhou Xuan,Liu Wen, “Research on the Architecture of Trusted Security System Based on the Internet of Things,” Fourth International Conference on Intelligent Computation Technology and Automation, Shenzhen, China, pp. 1172-1175, 2011.

[25] Castellani, Angelo P., Nicola Bui, Paolo Casari, Michele Rossi, Zach Shelby, and Michele Zorzi, "Architecture and protocols for the internet of things: A case study," 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 678-683, 2010.

[26] Castro, Miguel, Agustín Guillén, Jose L. Fuster, Antonio J. Jara, Miguel A. Zamora, and Antonio F. Gomez Skarmeta, "Oxygen Cylinders Management Architecture Based on Internet of Things," International Conference on Computational Science and Its Applications (ICCSA), pp. 271-274, 2011.

[27] Neil Bergmann, and Peter J. Robinson, “Server-Based Internet of Things Architecture,” The 9th Annual IEEE Consumer Communications and Networking Conference, pp. 360 – 361, 2012.

[28] IoT-A Consortium. IoT-A – Internet of Things Architecture. http://www.iot-a.eu/. 27 Jan. 2014. [Accessed: 14-Oct-2016]

[29] Serbanati, A., A. S. Segura, A. Oliverau, Y. B. Saied, N. Gruschka, D. Gessner, and F. Gomez-Marmol, "Internet of Things Architecture, Concept and Solutions for Privacy and Security in the Resolution Infrastructure,” EU project IoT-A, Project report D4. 2, 2012.

[30] Vasilomanolakis, Emmanouil, Jörg Daubert, Manisha Luthra, Vangelis Gazis, Alex Wiesmaier, and Panayotis Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," In 2015 International Workshop on Secure Internet of Things (SIoT), pp. 49-57. 2015.

[31] BETaaS Consortium. D1.4.2 – TaaS Reference Model. http://www.betaas.eu/docs/deliverables/BETaaS%20-%20D1.4.2%20-%20TaaS%20Reference%20Model%20v1.0.pdf, [Accessed: 25-Oct-2016]

[32] BETaaS Consortium. Building the environment for the things as a service. http://www.betaas.eu/, 2012. [Accessed: 12-Oct-2016]

[33] OpenIoT Consortium. OPENIoT D2.3 Detailed Architecture and Proofof- Concept Specifications. http://openiot.eu/?q=node/49, 2013. [Accessed: 25-Sept-2016]

[34] OpenIoT Consortium. OPENIoT project description. http://www.openiot.eu/, 2013. [Accessed: 30-Sept-2016]
[35] Robert Gwadera. D5.2.1 Privacy and Security Framework. 2013. [Accessed: 15-Oct-2016]
[36] IoT@Work Consortium. D1.2 – Final framework architecture specification. https://www.iot-at-work.eu/data/D1.3 IoT@Work Architecture final v1.0-submitted.pdf, July 2013. [Accessed: 18-Oct-2016]
[37] P. Congdon, B. Aboba, A. Smith, G. Zorn, and J. Roese. IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines. RFC 3580 (Informational), September 2003. Updated by RFC 7268.
[38] Bandyopadhyay, Debasis, and Jaydip Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless Personal Communications Vol. 58, No. 1, pp. 49-69, 2011.
[39] Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, Vol. 10, No. 7 pp. 1497-1516, 2012.
[40] Kim Rowe, "Internet of Things requirements and Protocols", http://www.standardsuniversity.org/e-magazine/march-2016/internet-of-things-requirements-and-protocols/ [Accessed: 15-Oct-2016]
[41] IoT Standards and Protocols, http://www.postscapes.com/internet-of-things-protocols/ [Accessed: 25-Oct-2016]
[42] Evans, David, and David M. Eyers. "Efficient data tagging for managing privacy in the internet of things." In 2012 IEEE International Conference on Green Computing and Communications (GreenCom), pp. 244-248. 2012.
[43] J. Cao, B. Carminati, E. Ferrari and K.L. Tan, "CASTLE: continuously anonymizing data streams," IEEE Transactions on Dependable Secure Computing, Vol. 8, No. 3, pp.337–352, 2011.
[44] Y. Wang andQ. Wen, "A privacy enhanced dns scheme for the internet of things," IET International Conference on Communication Technology and Application (ICCTA 2011), Beijing, China, pp.699–702, 2011.
[45] Babar, Sachin, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)," In Recent Trends in Network Security and Applications, pp. 420-429. Springer Berlin Heidelberg, 2010.
[46] A. Alcaide, E. Palomar, J. Montero-Castillo and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target driven applications," Computer Security, Vol. 37, pp.111–123, 2013.
[47] S. Papadopoulos, Y. Yang and D. Papadias, "Cads: continuous authentication on data streams," Proceedings of the 33rd International Conference on Very Large Data Bases (VLDB'07), Vienna, Austria, pp. 135–146, 2007.
[48] B. Carminati, E. Ferrari and K.L. Tan, "Specifying access control policies on data streams," Proceedings of the Database System for Advanced Applications Conference (DASFAA 2007), Bangkok, Thailand, pp. 410–421, 2007.
[49] Joerg Daubert, Alexander Wiesmaier, and Panayotis Kikiras, "A view on privacy & trust in IoT," In IoT/CPS-Security Workshop, IEEE International Conference on Communications (ICC 2015), London, GB, June 08-12, 2015.
[50] J. Mao and L. Wang, "Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection," Journal of Networks Vol. 7, No. 7, pp.1099–1105, 2012.
[51] Balte, Ashvini, Asmita Kashid, and Balaji Patil, "Security Issues in Internet of Things (IoT): A Survey," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5, No. 4, 2015.
[52] Weber, Rolf H, "Internet of Things–New security and privacy challenges," Computer Law & Security Review Vol. 26, No. 1 pp. 23-30, 2010.
[53] Arthur K. Weise, F. Thomas O'Halloran, J.D., and Anthony Hipple, "Finding Growth in an Increasingly Digital World," http://www.slideshare.net/jrisley/internet-of-things-in-logistics-59997781 [Accessed: 12-Oct-2016]
[54] A. Sardana and S. Horrow, "Identity management framework for cloud based internet of things", Proceedings of the First International Conference on Security of Internet of Things, pp. 200-203, 2012.
[55] Yun, Miao, and Bu Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," In 2010 IEEE International Conference on Advances in Energy Engineering (ICAEE), pp. 69-72, 2010.
[56] Medaglia, Carlo Maria, and Alexandru Serbanati, "An overview of privacy and security issues in the internet of things," In The Internet of Things, pp. 389-395. Springer New York, 2010.
[57] Wang, C., "Object Identification Techniques and the Application in IoT," Advances in Media Technology, p.9, 2013.
[58] Renu Aggarwal, "RFID Security in the Context of "Internet of Things," Proceedings of the First International Conference on Security of Internet of Things, pp. 51-56, 2012.
[59] Li, Zhihua, Xi Yin, Zhenmin Geng, Haitao Zhang, Pengfei Li, Ya Sun, Huawei Zhang, and Lin Li, "Research on PKI-like Protocol for the Internet of Things," In 2013 IEEE Fifth International Conference on Measuring Technology and Mechatronics Automation, pp. 915-918, 2013.
[60] Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," In 2016 IEEE 49th Hawaii International Conference on System Sciences (HICSS), pp. 5772-5781, 2016.
[61] John A. Stankovic, Life Fellow, "Research Directions for the Internet of Things," IEEE Internet of Things Journal, Vol. 1, Feb. 2014.