RESEARCH ARTICLE OPEN ACCESS

Security Issues and Challenges in Internet of Things – A Review

Lilima Jain, Kishore Kumar. U, Vishanth Fastino. A, Prof. R. Manjula
SCOPE, VIT UNIVERSITY Vellore-632014, Tamil Nadu

ABSTRACT
The Internet of Things (IoT) alludes to the continually developing system of physical articles that component an IP address for web availability, and the correspondence that happens between these items and other Web empowered gadgets and frameworks. The security issues of the Internet of Things (IoT) are straight forwardly identified with the wide utilization of its framework. IoT securities and enhancing the design and several elements of this work showcases various security issues with respect to IoT and thinks of solutions for the issues under the advancements included. Here we are going to do a study of all the security issues existing in the Internet of Things (IoT) alongside an examination of the protection issues that an end-client might confront as an outcome of the spread of IoT. Most of the overview is centred around the security emerging out of the data trade innovations utilized as a part of Internet of Things. As a piece of IoTs, genuine concerns are raised over access of individual data relating to gadget and individual protection. This review tells about the security and protection issues of IoT.
***Keywords*:** Internet of Things, Security, Communication, Issues and Challenges in Maintenance Phase.

I. INTRODUCTION

The Internet of Things (IoT) is a combination of internet and the web in the physical world paradigm. It has a widespread development in distributed devices with embedded identification and sensing technologies. These devices have the unique addressing systems through which they can be identified in a complicated network environment. Internet of Things provides the means to communicate and interact with the devices and the physical entities. That it can cooperate with their neighbouring devices to reach the common goal. Nowadays people are using Internet of Things for sending and receiving emails, accessing internet and other distributed devices. Internet of Things is a backbone for internet connectivity of physical objects which have computation and communication capabilities around the sensing devices.

This invention helps to make the embedded devices smart and letting them to interconnect with the other devices in the physical world that it can work faster and easier. This will make the new change in the field of Information and Technologies. Its well known demand in this era made it to connect with the various technologies with the base as internet. And for making this communication and coordination secure. It provides a new way to service and communication.

Within certain perspective "Internet of Things" is briefly use to refer:

1. The distributed global networks connect all the devices through the internet connectivity so that they can sense and respond according to the communication and information.
2. Some technologies are necessary to sense the IoT like embedded devices, RFID, sensors, actuator networks, peer to peer communication devices.
3. Together working of all applications and services for investing on the techniques to start the new business and marketing opportunities.

In this review paper, The aim is to give a proper view of the security issues in the Internet of Things and also provide a review on the Internet of Things applications and research challenges. The protection and security concerns encompassing IoT frequently shows themselves as a treat to end-client appropriation and adversely sways trust among end-clients in these arrangements. In this paper, it presents a reference programming design for building cloud enabled IoT applications in backing of community oriented pervasive frameworks went for accomplishing dependability among end-clients in IoT situations. We introduce a contextual investigation that influences this reference design to secure touchy client information in an IoT application execution and assess the reaction of an end-client study finished through a study. Past the protection and security concerns enclosing IoT frameworks, it is turning out to be more unavoidable for pervasive synergistic gadgets to influence web administrations for information sharing and correspondence to backend stockpiling frameworks.

With the coming of distributed computing, it is not phenomenal for the versatile administrations that these pervasive gadgets convey with, to be facilitated in the cloud. Therefore, with the inescapable area particular protection and security attentiveness toward distributed computing, IoT, pervasive frameworks and web

administrations, it is vital to set up a reference engineering that gives a comprehensive answer for executing cloud-empowered applications and administration associations in IoT situations in a design that enhances the general objective of accomplishing end-user trust and, thusly, enhance client reception of IoT applications (Apps).

II. RELATED WORK

Internet of Things is related with the embedded devices and the sensors. we studied about how to make the IoT secure. Here there are some issues which we need to secure and how to test that it is insecure and the prevention mechanism.

The following needs to be test for the Internet of Things:

1. Insecure web interface
2. Insufficient Authorization or login
3. Insecurity in Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insecurity in cloud interface
7. Insecure remote interface
8. Insufficient security configurability
9. Insecure software/Firmware
10. Poor Physical Security

1. Insecure web interface

Insecurity in web interfaces might bring about the loss of information or information corruption, lack of responsibility denial of access and it might prompt complete gadget takeover. An unstable interface in web can be available [2]when issues, for example, account enumeration, lack of record lockout or because of the vicinity of feeble credentials. Issues with the web interface are anything but difficult to find when analyze the interface physically with the testing devices

Checking for an insecure web interface includes:

- Determining if the default user name and password can be changed during initial product setup[9].
- Determining if a specific user account is locked out after 3 failed login attempts
- Identifying an authentic account in case of account recovery and password recovery.
- Reviewing the interface for certain issues such as cross site scripting, request forgery and sql injection.

2. Insufficient Authorization or Login:

Authentication is required for secure login. Insufficient authorization\authentication is prevalent as it assumed that the users will be provided with the interfaces only on the secure networks and not to external users on other networks insufficient authorization\authentication results in data loss.

- Lack of secret key unpredictability
- Poorly ensured certifications
- Lack of two element verification
- Privilege Escalation
- Lack of Role Based Access control

3. Insecurity in Network Services

Unstable System Administrations might be vulnerable to cushion flood assaults or assaults that make a disavowal of administration condition leaving the gadget difficult to reach to the client. Foreswearing of administration assaults against different clients might likewise be encouraged when shaky system administrations are available. Insecure system administrations can frequently be recognized via mechanized apparatuses, for example, port scanners and fuzzers.

Checking for insecure network services includes:

- Reviewing so as to figure out whether unstable system administrations exist your gadget for open ports utilizing a port scanner.
- As open ports are recognized, each can be tried utilizing any number of computerized apparatuses that search for DOS vulnerabilities, vulnerabilities identified with UDP administrations and vulnerabilities identified with cushion flood and fluffing assaults.
- Investigating system ports to guarantee they are completely fundamental and if there are any ports being presented to the web utilizing UPnP.

4. Lack of Transport Encryption:

Absence of transport encryption permits information to be seen as it goes over nearby systems or the web, Absence of transport encryption is pervasive on neighbourhood systems as it is anything but difficult to expect that nearby system movement won't be broadly noticeable, however on account of a neighbourhood remote system, mis-configuration of that remote system can make activity unmistakable to anybody inside of scope of that remote system. Numerous issues with transport encryption are viewing so as to anything but difficult to find basically arrange movement and hunting down decipherable information.[9] Mechanized devices can likewise search for appropriate execution of regular transport encryption, for example, SSL and TLS.

Checking for lack of transport encryption includes:

- Checking on system movement of the gadget, its versatile application and any cloud associations with figure out whether any data is gone in clear content.
- Inspecting the utilization of SSL or TLS to guarantee it is a la mode and appropriately executed.
- Assessing the utilization of any encryption conventions to guarantee they are suggested and acknowledged.

5. Privacy Concerns:

Concerns produced by the gathering of individual information not withstanding absence of appropriate insurance of that information is common. Security concerns are anything but difficult to find by basically assessing the information that is being gathered as the client sets up and enacts the gadget. Robotized apparatuses can likewise search for particular examples of information that might demonstrate accumulation of individual information or other delicate information.

Checking for Privacy Concerns includes:

- Recognizing all information sorts that are being gathered by the gadget , its versatile application and any cloud interfaces.
- The gadget and it's different segments ought to just gather what is important to perform its capacity.
- By and by identifiable data can be uncovered when not appropriately encoded while very still on capacity mediums and amid travel over systems.
- Assessing who has admittance to individual data that is gathered.

6. Insecurity in Cloud Interface:

An unreliable cloud interface is available when simple to figure qualifications are utilized or account count is conceivable.[8] Unreliable cloud interfaces are anything but difficult to find by basically evaluating the association with the cloud interface and using so as to distinguish if SSL is being used or the watchword reset instrument to recognize substantial records which can prompt record identification.

Checking for insecurity in cloud interface includes:

- Figuring out whether the default username and watchword can be changed amid beginning item setup.
- Figuring out whether a particular client record is bolted out after 3 – 5 fizzled login endeavours.
- Figuring out whether substantial records can be distinguished utilizing watchword recuperation systems or new client pages.
- Auditing the interface for issues, for example, cross - site scripting , cross – site demand fabrication and sql infusion.
- Evaluating all cloud interfaces for any security breaches (API interfaces and cloud – based web interfaces).

7. Insecure Remote Interface:

An unreliable portable interface is available when simple to figure qualifications are utilized or account identification is conceivable. Unreliable versatile interfaces are anything but difficult to find by just inspecting the association with the remote systems and using so as to distinguish if SSL is being used or the secret word reset instrument to recognize substantial records which can prompt record count.

Checking for insecure Remote interface includes:

- Figuring out whether the default username and secret key can be changed amid starting item setup.
- Figuring out whether a particular client records is bolted out after 3 – 5 fizzled login endeavours.
- Figuring out whether substantial records can be recognized utilizing secret word recuperation systems or new client pages.
- Looking into whether qualifications are presented while associated with remote systems.
- Looking into whether two component verification alternatives are accessible.

8. Insufficient Security Configurability:

Lacking security configurability is available when clients of the gadget have restricted or no capacity to modify its security controls. Deficient security configurability is obvious when the web interface of the gadget has no choices for making granular client authorizations or for instance, constraining the utilization of solid passwords. Manual audit of the web interface and its accessible alternatives will uncover these lacks.

Checking for insufficient security configurability includes:

- Looking into the managerial interface of the gadget for choices to fortify security, for example, constraining the making of solid passwords.

- Evaluating the regulatory interface for the capacity to isolated administrator clients from typical clients.
- Evaluating the regulatory interface for encryption alternatives.
- Evaluating the regulatory interface for alternatives to empower secure logging of different security occasions.
- Evaluating the regulatory interface for alternatives to empower alarms and notices to the end client for security occasions.

9. Insecure Software/ Firmware:

The absence of capacity for a gadget to be overhauled presents a security shortcoming all alone. Gadgets ought to be able to be redesigned when vulnerabilities are found and programming/firmware upgrades can be frail when the overhauled documents themselves and the system association they are conveyed on are not secured. Programming/firmware can likewise be shaky on the off chance that they contain hardcoded touchy information, for example, accreditations. Security issues with programming/firmware are moderately simple to find by just reviewing the system activity amid the overhaul to check for encryption or utilizing a hex editorial manager to examine the upgrade record itself for fascinating data.

Checking for insecure software/firmware updates includes:

- Looking into the upgrade record itself for introduction of delicate data in intelligible configuration by somebody utilizing a hex alter apparatus.
- Looking into the creation record overhaul for legitimate encryption utilizing acknowledged calculations.
- Looking into the creation record overhauling to guarantee it is legitimately marked.
- Looking into the specialized technique used to transmit the upgrade.
- Checking on the gadget for legitimate approval of marked upgrade documents.

10. Poor Physical Security:

Physical security shortcoming are available when an assailant can dismantle a gadget to effectively get to the capacity medium and any information put away on that medium. Shortcomings are additionally present when USB ports or other outer ports can be utilized to get to the gadget utilizing highlights proposed for arrangement or upkeep.

Checking for poor security includes:

- Inspecting how effortlessly a gadget can be dismantled and information stockpiling mediums got to or evacuated.
- Auditing the utilization of outer ports, for example, USB to figure out whether information can be gotten to on the gadget without dismantling the gadget.
- Looking into the quantity of physical outside ports to figure out whether all are required for appropriate gadget capacity.
- Looking into the managerial interface to figure out whether outside ports, for example, USB can be deactivated.
- Looking into the managerial interface to figure out whether regulatory capacities can be restricted to neighbourhood get to as it were.

III. MOTIVATION

The reference architecture displayed in this paper gives a structure to guaranteeing that protection and security become the dominant focal point all through the application improvement lifecycle in the quest for augmenting the guarantee of IoT, Ubiquitous processing and Distributed computing originals. In inferring our reference design, we layout the significant segments of cutting edge IoT frameworks that can profit by safeguarding security and information protection by considering a portion of the key parts of IoT frameworks in the accompanying relevant situations:

Scenario 1:

A home mechanization checking administration that is fit for watching the use of power in a given family unit and flawlessly manages the home's utilization of power by taking in the inclinations of the family unit in correlation with ideal force utilization best practices of other neighbouring family units of comparative size .

Scenario 2:

An Online Social Networking (OSN) administration that is coordinated with a pervasive eyewear gadget, similar to Google Glass, for catching pictures and recording recordings of fascinating minutes. The administration is thought to be valuable for putting away the recorded photographs and recordings in cloud capacity while empowering the end-client to share the put away media with different companions in the OSN too as free.

Scenario 3:

A motion picture suggestion administration that influences past media content review designs and the inclinations of persuasive

individuals in a specific family client's circle of OSN companions to suggest future motion pictures that will be of hobby to the client. This situation is utilized for our situation study execution.

In accordance with the situation introduced over, a percentage of the major parts that have their own particular aspects for protection and security concerns include:

- End-User Preferences for Security, Privacy and Trust Cloud Computing: as a cloud-facilitated web alternately versatile administration and cloud-based information stockpiling
- Ubiquitous Computing: spoke to by the Kinect Sensor, Tablet gadget and a Smart TV
- Service Oriented Architecture (SOA): as the Facebook Graph API (web administration) utilized for surmising the inclinations of compelling companions in a given family part's OSN circle and in addition the YouTube API (web administration) for spilling a film.
- Network correspondence crosswise over remote systems for transmitting and accepting information.

Reference Architecture:

A portion of the key concerns inborn in every layer of the IoT reference design.

A. Security and Privacy in the Ubiquitous Sensors and Gadgets in the Smart Environment:

In considering the security and protection worries of IoT applications, it is critical to focus on a percentage of the security also, protection challenges relating to pervasive gadgets and sensors that are regularly working universally to gather and trade information in nature. From a security and security point of view, a portion of the key prerequisites that can be tended to at this layer of the IoT application incorporate. User recognizable proof and approval to control get to and implement consents and approval levels for different segments of the framework.[4]

• Tamper resistance of the physical and sensible gadget. Since IoT gadgets are regularly unattended, physical assault vulnerabilities are basic.

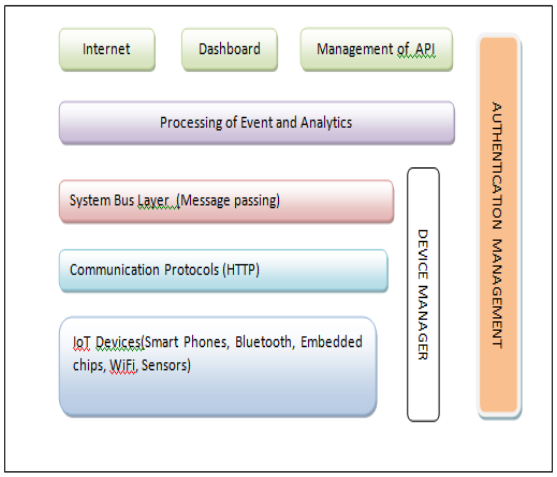
• Content security - through computerized rights administration (DRM) of substance utilized as a part of the framework.

• Data security to ensure touchy client information.

• Data interchanges and capacity security through defensive measures for both information in-travel and information at rest.

• Secure system interchanges to guarantee that system interchanges between pervasive gadgets and outer administrations are just approved through secure association channels (for instance, the remote correspondence in the shrewd home environment of our contextual investigation must be transmitted through the client's assigned "home" remote switch, as a matter of course.

• Privacy in pervasive registering comes to play on the grounds that the route in which the gadget or sensor gathers information about the end-clients may strife with the client's security inclinations for a specific situation. These security obstructions and inclinations must be protected keeping in mind the end goal to ingrain end-client trust in the framework.



Fig, IoT Reference Architecture

B. Security and Privacy in the Cloud Computing Layer: Distributed processing can be portrayed as "a model for engaging general, supportive, on-interest framework access to a typical pool of configurable figuring resources (e.g., frameworks, servers, stockpiling, applications, and institutions) that can be easily recognized and made for the public with very less effort from the management or the organization ".

We consider the related layers in an IoT arrangement that makes utilization of an open cloud arrangement:

• Services Layer - which incorporates:
- Security Applications.
- Data administration frameworks.
- Operating Systems.

• Server Virtualization layer

• Physical Hardware layer - which incorporates:
- Physical equipment
- Network correspondence framework.

C. Security and Privacy in the IoT Application and Service Layer:

Security issues in integrating mobile agents and devices with services can be categorized as: Confidentiality, Authentication, Authorization, Integrity, Non repudiation, Privacy and Availability.

The IoT application client interface itself may have its own particular protection and security concerns[1]. Maybe what's more, the outsider outer administrations utilized in the arrangement ought to

be represented to guarantee that they ensure the end-client's protection and security inclinations.

IV. ISSUES AND CHALLENGES OF INTERNET AND THINGS

Issues of IOT:

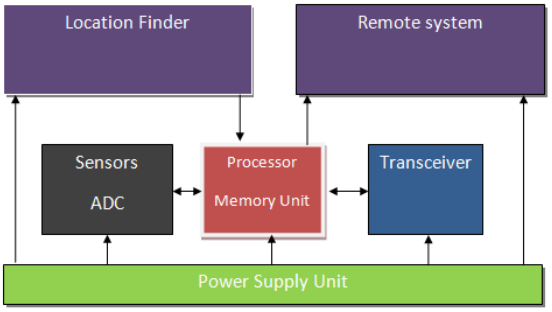
To the different functionalities and originated from different technology and application fields are belonging to the same communication environment. IoT devices have various variety in it ranges from:

Wireless: IoT devices are the mode for Wireless communication modules (e.g, Bluetooth, WiFi, ZigBee etc.) and it can also communicate with its neighbouring devices. These wireless networks have the sensors attached with it through which it can connect with the network nodes through the air channel.

Heterogeneous: The IoT have the high level of heterogeneity than the Internet. As these both objects belongs small RFID tags to the large connected servers.Thus, comparing security and protection measures ought to be interface-accommodating and perfect with different sorts of IoT equipment.[8]

Specificity: Vast dominant part of current IoT gadgets (e.g., SmartBand) are intended for a specific utilize and could gather delicate individual data (e.g., circulatory strain, heart rate, living propensity, and so on.), in which case how to viably secure client protection will be a major concern. In expansion to buyer hardware, IoT gadgets are more utilized in modern and rural computerization. For instance, IP observation cameras are generally used to screen resource status in the inventories. Bargained IoT gadgets could uncover huge competitive advantages.

Asset Constrained: Most IoT gadgets are minimal effort equipment with obliged assets as far as figuring, correspondence, and capacity capacities, which requires comparing security and protection measures to be lightweight and practical. For instance, latent RFID labels utilized to track and follow products in the store network are normally prepared with straightforward read/compose operations, XORing with irregular numbers, and cyclic redundancy check (CRC) capacities. Remote sensor system (WSN) sensors are normally outfitted with ease microcontrollers with little piece width.[10]



Fig, Sensors

Infectivity: Since more often than not IoT gadgets are associated with the system and more often than not have the same system key or gathering key inside of a apparently trusted range (e.g., amusement parks, music shows, sports diversions, and so forth.), if one gadget is traded off, the enemy could undoubtedly hack its neighbouring gadgets with the deciphered system/bunch key. For instance, IoT gadgets inside of the same ZigBee system will scramble parcels utilizing the common system key subsequent to confirming themselves to the trust focus with their connection keys .

Portability: Many IoT gadgets (e.g., advanced mobile phones) are versatile and would move together with their clients. Therefore, their correspondence neighbourhood will be changed a periodically.Dynamic correspondence neighbourhood will be a test to verification techniques in view of altered IP locations or communication with neighbouring gadgets.

Versatility: The quantity of IoT gadgets on the earth have been developing exponentially. The administration of such countless gadgets will be a major test. Besides, the quantity of IoT gadget sorts is likewise on the ascent, which raises another test to gadget confirmation.

Security Challenges

The aforementioned properties raise new difficulties to security and protection support for IoTs. General ways to deal with equipment, programming and system security can't be basically received to determine the security and privacy issues related with IoTs. New less weight and financially savvy arrangements particular to worldwide supply chains of IoT gadgets should be proposed to make room for expansive scale arrangement of IoT gadgets in different territories. The security and protection challenges related with IoTs are recorded as takes after:

Component Trust: Against the scenery of worldwide supply chains, more also, more IoT gadgets are amassed at abroad assembling plants.

components on IoT gadgets are given by various sellers and pass through numerous elements on various landmasses before they are introduced in their last applications. In this connection, fake ICs or ICs containing equipment Trojans might have been mounted on the PCBs of IoT gadgets deliberately or unexpectedly by constructing agents before they enter the inventory network. Instruments guaranteeing trust towards segments given by untrusted merchants ought to be incorporated into security conventions. As an illustration, DARPA propelled the SHIELD project to build up a dielet that empowers IC confirmation by incorporating solid encryption, sensors, close field force and interchanges into an infinitesimal scale chip equipped for being embedded into the bundle of an IC.

Gadget Authentication: Before touching base at end-clients, IoT gadgets generally need to go through numerous substances over the worldwide inventory network. Cloned or fake IoT gadgets might likewise enter the store network and be blended with the credible ones. A few clients might buy cloned or fake IoT gadgets from dark market intentionally or unwittingly to spare cash. More than 700 seizures of fake Cisco system equipment and marks with an expected retail estimation of more than $143 million were accounted for by Division of Justice in 2010 . the remote server ought to validate one another before getting system administrations (e.g., downloading important firmware upgrades).

Equipment Theft: IoT gadgets and now and then costly segments on them (e.g., focal preparing units) might be lost or stolen in inventories, amid conveyance or even after sending. In 2012, 117 electronic robberies were accounted for in the US with the normal loss of $382,500 per burglary occurrence . In 2014, 1 million dollars worth of costly focal handling units were supplanted with less expensive parts before they were stolen from Hewlett-Packard distribution center in And over .

Access Control: We allude to the specific limitation of access to certain equipment or programming assets as access control. Whenever stopped into the system, IoT gadgets might be gotten to by malignant system hubs. True blue imparting gatherings might likewise attempt to get to substance surpassing their entrance benefits. Access control counteracts exercises that could endanger framework security by obliging what a client can do straightforwardly, and also what programs running in the interest of the clients are permitted to do . Part based access control models dole out least benefits to framework parts to complete their professional details. In this instance, if any of the part is swapped or its qualification is stolen, the interloper will have negligible access to different parts of the framework and the effect of security rupture will be minimized.

Information Confidentiality: Communications between IoT gadgets and between IoT gadget and trust focus might experience the ill effects of listening stealthily since they more often than not work reporting in real time channel and are secured by powerless conventions (e.g., ZigBee , EPC C1G2 , and so forth.). Correspondence in the middle of door and remote server is more secure since it is more often than not ensured by solid conventions (e.g., TLS , IPsec , and so forth.).

Information Integrity: Sensor information and validation data might be noxiously adjusted in travel for dissent of-administration assault. Advanced marks furthermore, message validation codes can be utilized to secure information respectability.

Data Confidentiality: Communications between IoT devices and between IoT device and trust center may encounter the evil impacts of listening stealthily since they as a general rule work reporting progressively channel and are secured by feeble traditions (e.g., ZigBee , EPC C1G2, et cetera.). Correspondence amidst entryway and remote server is more secure since it is as a rule guaranteed by strong traditions (e.g., TLS, IPsec , etc.).

Data Integrity: Sensor data and acceptance information may be poisonously balanced in go for difference of-organization ambush. Propelled marks besides, message acceptance codes can be used to secure data respectability.

V. CONCLUSION

The Internet of Things provides the vision of its security and privacy. The paper proposed a systematic and cognitive approach for IoT security. The development of embedded devices leads to the new directions for both research and business. In this review paper, given a overview for the security issues and challenges in the Internet of Things. By the use of IoT we can operate our machines or systems from remote places. Many industries are using IoT nowadays for their work purpose to keep their industries secure and to make the work easier. We do hope that this review will be useful for the practitioners and researchers in this field of IoT.

REFERENCES

[1]. Arbia Riahi, Enrico Natalizio, Yacine Challal, Nathalie Mitton, Antonio Iera "A systemic and cognitive approach for IoT security", 2014 International Conference on Computing, Networking and Communications.

[2]. Open Web Application Security Project-Internet of Things -2014-OWASP.

[3]. Kun Yang, Domenic Forte, and Mark M. Tehranipoor "Protecting Endpoint Devices in IoT Supply Chain"- 2015-IEEE.

[4]. Ivor D. Addo, Sheikh I. Ahmed, Stephen S Yau, Arun Buduru "A Reference Architecture for Improving Security and Privacy in Internet of Things Applications" - 2014 IEEE International Conference on Mobile Services.

[5]. Tuhin Borgohain, Uday Kumar, Sugata Sanyal "Survey of Security and Privacy Issues of Internet of Things".

[6]. [6] Daniele Miorandi , Sabrina Sicari , Francesco De Pellegrini , Imrich Chlamtac "Internet of things: Vision, applications and research challenges"- April 2012-Elsevier.

[7]. Luigi Atzori , Antonio Iera , Giacomo Morabito "The Internet of Things: A survey" - Computer Networks, Vol. 54, No. 15, 2010, pp. 2787-2805-Elsevier.

[8]. Huansheng Ning, Hong Liu " Cyber-Physical-Social Based Security Architecture for Future Internet of Things" Advances in Internet of Things ", 2012, 2, 1-7-Scientific Research Publishing.

[9]. R. Roman, C. Alcaraz, J. Lopez and N. Sklavos, "Key Management Systems for Sensor Networks in the Context of the Internet of Things," Computers & Electrical Engineering, Vol. 37, No. 2, 2011, pp. 147-159

[10].]Kun Yang, Domenic Forte, and Mark Tehranipoor. ReSC: RFID-enabled Supply Chain Management and Traceability for Network Devices. In The11th Workshop on RFID Security, 2015

[11]. A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, A. Bouabdallah, "A Systemic Approach for IoT Security," , 2013 IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), pp.351,355, doi: 10.1109/DCOSS.2013.78IoTIP,Boston, USA, May 2013.

[12]. M. Abomhara and G. Koien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on, May 2014, pp. 1–8.

[13]. L. Zhou and H. C. Chao, "Multimedia Traffic Security Architecture for the Internet of Things," IEEE Network, Vol. 25, No. 3, 2011, pp. 35-40.

[14]. R. Roman, P. Najera, J. Lopez, "Securing the Internet of Things", IEEE Computer, vol. 44, no. 9, pp. 51-58.

[15]. Sen, Jaydip. "Security and privacy challenges in cognitive wireless sensor networks." arXiv preprint arXiv: 1302.2253 (2013).