An Application of Internet of Things for Cyber Security and Control: Emerging Needs and Challenges

Monalisa Pattanayak[1]
[1]Ph.D. Research Scholar, Department of Business Management,
, Affiliated to Koneru Lakshmaih Education Foundation, Vaddeswaram, Vijayawada, Guntur, Andhra Pradesh, India
Email: monalisapattanayak36@gmail.com, Mob: 9666332722
Dr. A. Udaya Shankar[2]
[2]Associate Professor, Department of Business Management,
KLU Business School, KL University, Vaddeswaram, Vijayawada, Guntur, Andhra Pradesh, India
Email: dr.a.udayashankar@gmail.com, Mob: 9949540100
Prof. (Dr). S. V. Sukthankar[3]
[3]Associate Professor in Commerce, Govt. College of Arts, Science and Commerce Khandola, Marcela- Goa, Email: svsukh@yahoo.co.in
Prof. (Dr.) Ramesh Chandra Rath[4]
[4] Dean (R&D) and Head of Department of Master of Business Administration (MBA) at Guru Gobind Singh Educational Society's Technical campus, Chas, Bokaro, Steel city, India
Email: drramesh.rrc@gmail.com, ramesh.ch.rath@gmail.com ***Mob: 7008105343***

Abstract

At present, we are living in the Post-PC era in world where smartphones and other wireless handheld devices are changing our environment, making it more interactive, adaptive and informative. Termed as Internet of Things (IoT) evolving into Internet of Everything, the new ecosystem combines wireless sensor networks, cloud computing, analytical data, interactive technologies, as well as smart devices, to provision solutions in which the objects are embedded with network connectivity and an identifier to enhance object-to-object interactions. IoT innovation is advancing and provides diverse smart solutions or applications. From e-transport to e-health; smart living to e-manufacturing and many other e-solutions. In this environment, the rising trend of cyber-attacks on systems infrastructure coupled with the system inherent vulnerabilities presents a source of concern not only to the vendors, but also to the consumer. These security concerns need to be addressed in order to ensure user confidence so as to promote wide acceptance and reap the potentials of IoT. From the perspectives of firmware, hardware and software infrastructure setups, this paper looks at some of the major IoT application and service domains, and analyze the cyber security challenges which are likely to drive IoT research in the near future.

Keywords:

Internet of Things (IOT) Internet of Everything (IOE) Cyber threats System svulner abilities. (CTSSA) Internet of Things and Infrastructure (IoTI) IOT Applications (IOTA)

1. Introduction:

According to IBM, devices connected to the Internet are expected to exceed the number of human beings and the evolution of connectivity is expected to continue such that by 2020the number of connected devices will be around 50 billion [1]. This proliferation of connected devices in an actuating network has created what has become known as the Internet of Things (IoT). A platform in which sensors and actuators blend seamlessly with the environment to share information in order to develop a common operating picture [2].An IoT system starts from the level where a single object is identified using a unique global identifier which is globally addressable. The level of information obtained by accessing the object, in this case, can be as low as static data that is stored on the radio frequency identification (RFID) tags. IoT is therefore described as objects with a unique identifier, having Internet connectivity; is (interactively) accessible by other objects herein referred to as the ‘‘things’’. IoT has stepped out of its infancy and is the next revolutionary technology in the transformation of Internet into a fully integrated future Internet (of things). This development is fuelled by the recent increase in adoption and integration of wireless network technologies, Wireless Sensor Networks (WSN), RFID tags, as well as actuating nodes. On this concept, Karimi and Atkinson claimed, expanding communication networks to include physical objects will further accelerate the number of connected devices, as well as the amount of information that can be shared through the Internet [3].IoT presents ubiquitous connectivity for a wide range of devices, services, and applications. These include intelligent computers, smartphones, office equipment, wireless-enabled cars, lighting systems, heating, and ventilation and air-condition (HVAC), household appliances, and many others. To be IoT-enabled, a device (‘thing’) ought to be on a network and connected to a communicating node. Various communication network technologies (infrastructures) such as 3G, LTE, Wi-Fi, Bluetooth, ZigBee , Z-wave, Sigfox, etc. provide connectivity services for IoT deployment on many services platforms .As IoT advances, cloud computing is expected to provide the backbone for the worldwide information diffusion, data analytics (or computation) and storage. Cloud solutions such as Microsoft Azure, Amazon Web Services (AWS), Google Docs, etc., are expected to provide standard gateways for interconnecting physical objects with computation and communication capabilities across a wide range of applications, services, and technologies. Caceres and Friday [4] discuss the progress, opportunities and challenges of an environment of ubiquitous computing ‘ubicomp’ and identify the two critical technologies for growing the future ubicomp infrastructure as cloud computing and the Internet of Things. It is thus generally perceived, that as IoT matures, cloud computing will act as a receiver of data from the various ubiquitous sensors, as well as being the platform for big data analytics, analyzing and interpreting IoT generated data [4]. Additionally, various cloud-based solutions increasingly are provisioned to provide users with compatible web-enabled interface applications for user interactivity and connectivity

.For instance, Gubbi et al. [2], have argued that for IoT to emerge successfully, the traditional computing and Internet connectivity platforms will have to be extended beyond the traditional mobile communication connecting human beings, and evolve into connecting objects and embedding intelligence into our environment. With this fundamental ground in

place, smart connectivity and context-aware computation can be accomplished .Certainly, with billions of devices expected to be connected to the IoT ecosystem, it is expected to generate enormous amounts of data which will have to be stored, processed and presented in a seamless, efficient, and easily interpretable form. Cloud centric computing would be required as the platform to provide virtual infrastructure support for IoT services [2]. The services will integrate monitoring, storage, computation (and/or analytics), visualization and client service delivery [2].

According to Gubbi etal. the vision of IoT can be seen from the 'Internet' and 'Thing' centric. The Internet-centric architecture embroils Internet-as-a-services being the core focus of IoT while data is contributed by the objects [2]. In the thing-centric architecture, smart objects take the center stage of IoT services and applications [5].The major concerns raised with IoT-Cloud integration is the fact that from infrastructural to service domains, cloud models are beset with various security challenges such as application services attack, data integrity attack, privacy, trust, identity, standardization ,etc. These challenges are likely to unveil when the two platforms merge raising some fundamental research questions which need to be explored.

2. Literature Survey:

In this section, we the researchers has done an extensive survey in both off line and online by asking a setoff questionnaire to the respondent's of various companies and fields as related with the aforesaid research problem "An Application of Internet of Things for Cyber Security and Control: Emerging Needs and Challenges".

In this regard, we have followed both the method of data collection and collected around 250 number of respondent's database from various sources like:

Accordingly, a study by International Data Corporation (IDC) claims, that while business leaders recognize the business potentials of IoT, they are deeply skeptical about the system's inherent security challenges [6]. Additionally, the study asserts, most business leaders admitted having little understanding or underestimate the security threats IoT brings. In a related study, KPMG stated, that the security breaches in consumer data as well as recent attacks on cyber infrastructure systems worldwide, make IoT users lose confidence and avoid solution providers who fail to take the appropriate measures to protect their systems [7]. The issue of cyber security challenges on IoT platforms is a major global concern which requires a holistic assessment from both research and industrial communities.

This paper assesses security related threats which are likely to impede the success of IoT adoption and consumer confidence .The paper is structured as follows: Sect. 2 provides an overview of the IoT concept and structures. In Sect. 3, the potential threat challenges in relation to IoT applications and service are assessed. In Sect. 4domain scenarios are outlined and the Smart Metering case presented. In Sect. 5 Cyber Threat in Smart Metering is analyzed as a case. Section 6summarizes the conclusions.

3. Research Objectives:

The following research objectives have been taken by the researchers in order to justify the aforesaid research work that:

- To know the process of application and impact of Internet of things (IoT) on cyber security and it's Control.
- To study the application and service domain of IoT in various social media ,
- To study the advance models of IoT on supply chain and logistic systems for product design, Production and it's control

4. Hypothesis:

In this section, we have taken two types of hypothesis such as Null hypothesis (H_o) and alternative Hypothesis (H_e) in order to justify the aforesaid research objectives.

4.1. Null Hypothesis: (H_o)

This hypothesis refers about the application of IoT has no impact on cyber security and control when Network and smart grid is weak or failure.

4.2 Alternative Hypotheses (H_e):

This hypotheses refers about the application of IoT on Cyber Security, it has a great impact and influence the function monitor and control all the security control and threats successfully.

5 The IoT Concept

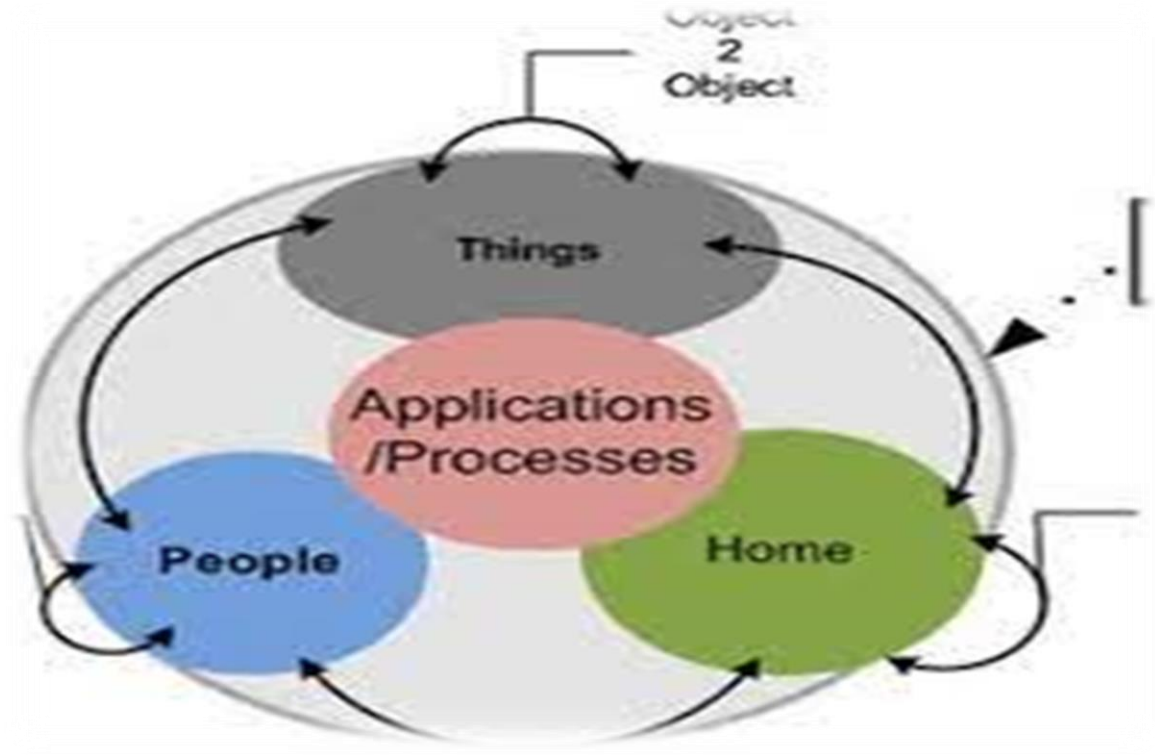
Over the past decade, Internet technologies have revolutionized the interconnection among people at an unprecedented scale and pace. The next revolution is expected to craft the interconnection among diverse objects leading to what experts termed as the smart environment. As we move from www (static pages web) to web2 (social networking web) toweb3 (ubiquitous computing—or web of things), the need for data-on-demand using sophisticated intuitive queries continues to increase significantly [2]. This era could be termed as the post-PC era where smartphones and related devices are changing our environment and the way ‘‘things’’ (including humans) interact. Things in the new environment are becoming more interactive as well as informative. Mark Weiser (father of Ubiquitous Computing), defined the new ecosystem as the ‘‘smart environment in the physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects, and connected through a continuous network’’ [8]. As mentioned, Gubbi et al. [2] argued that the growth of ubiquitous computing are shaped by cloud computing and the IoT. IoT as a concept is presumed to have been coined by Kevin Ashton in a submission, where he argued ‘‘adding RFID and other sensors to everyday objects will create an Internet of Things, and lay the foundations of a new age of machine perception’’ [9]. Since then, the idea has advanced in its acceptance both in the research and industrial eco spheres .Roman et al. [10] argue that

basically, an IoT device as a heterogeneous object will have a locatable, addressable, and readable counterpart on the Internet whereby IoT opens up a communication channel with any other entity, providing and receiving services at any time, any place, and in any way. In that perspective, most 'things' (e.g. Human beings, pets, farm animals, and computers, books, cars, household appliances and food) will be on the Internet in one form or the another leading to the evolution of Internet of Everything (IoE)

6. IoT Infrastructure:

It is established, that generally the IoT infrastructure (Fig. 4) consists of diverse hardware resources such as WSNs, RFID tags, actuators, readers, cameras, controllers, GPS, sensors(magnetometers, waspmote, ultrasound and infrared), device processors, terminals and other sensor gateways). Moreover, at the firmware level, most IoT objects are embedded with silicon integrated circuits (IC) and nano-electronics focusing on miniaturization, low cost and increased functionality in design of wireless identifiable systems or communication-enabled nodes. RFID tags and WSN hardware remain two most prominent IoT hardware infrastructure resources. RFID technology enables data transmission over a short distance. It consists of either active or passive radio frequency (RF) tag attached to an item

6.1 Futuristic Ecosystem Model



7. Characteristics of IOT devices:

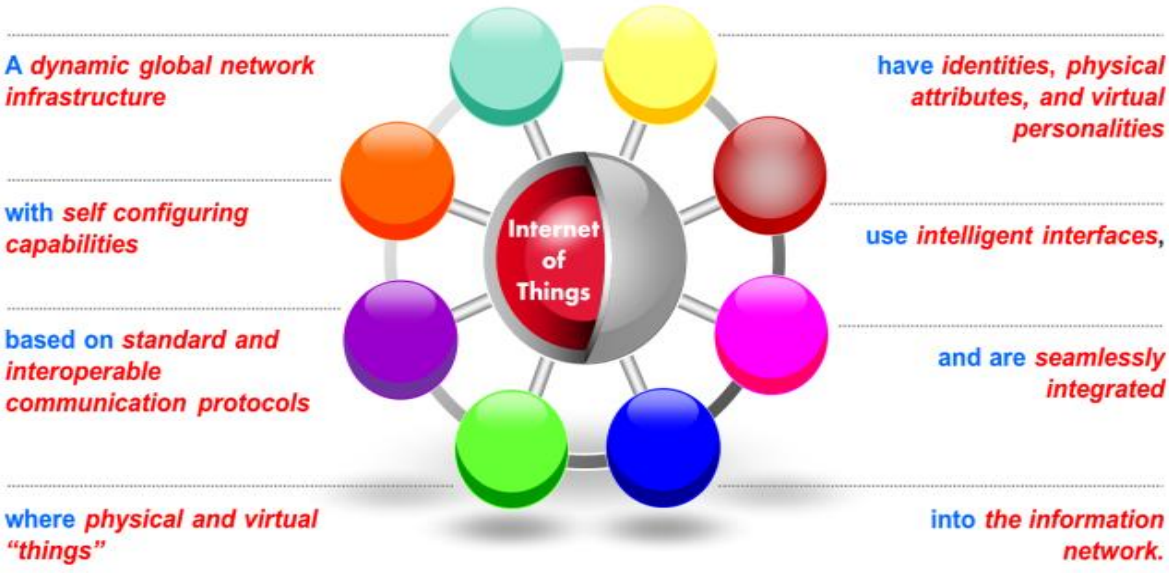
Some of the general and key characteristics identified during the research study such as: Intelligence IoT comes with the combination of algorithms and computation, software & hardware that makes it smart like:

- Connectivity
- Dynamic Nature.
- Enormous scale.
- Sensing.
- Heterogeneity
- Security.

8. Definitions of IERC:

The IERC definition states that IoT is "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.”. Being tracked and an RF reader/emitter

8.1 Figure –II refers about the IERC Model of IoT



. A passive tag draws energy from its reader, whereas an active RFID tag draws power from its embedded device. WSN hardware contains sensor interfaces, processing units, transceiver units and power supply. IoT supporting software, on the other hand, varies from firmware operating systems to application software with cloud-based software solutions (SaaS) and Mobile OS (iOS , android, Blackberry) as the backbone. Other software solutions include network and device

OS which are mostly microkernel based (e.g. Tiny OS, Tiny DB, Nano-RK, Lite OS, VMs).Others include application development software such as HTML, JavaScript, Ajax, PHP, and Ruby. IoT software integration in addition to general software services also supports data visualization, system integration, remote access control and application programme interface (API

According to Roman et al. [10], one key challenge which must be overcome in order to push IoT into the real world is security. Security challenges relating to IoT line up with the traditional Information Systems (IS) security objectives (SO) which are confidentiality, integrity, and data availability [12]. Moreover, there are other security challenges which

appear to be IoT-specific. For example, the merging of cloud computing and IoT, exposes IoT platforms to cloud induced vulnerabilities such as those contained in OWASP top 10[13]. Figure 5below presents cloud induced vulnerabilities identified in 2015 from the common vulnerability database [13]. These vulnerabilities which are inherent in cloud applications are likely to impact on IoT solutions and services as the two emerge. Another significant risk vector may be found in substandard IoT products and services .These have the potential to threaten the survivability of IoT services. For instance, poorly designed, crafted and out-dated or counterfeit products present very significant risks to IoT enabled applications. On this subject, Touhill and Touhill [14] argue, businesses around the world suffer countless hours of monetary and mission lose due to unexpected equipment and system failures, caused by poor or improper maintenance, poor and inaccurate advice from an unqualified service personnel. Additionally, the authors claim poor performance by contracted personnel, and even inaccurate data from a business partner and perhaps IoT devices may be accepted for information processes and critical business decisions [14].Furthermore, most IoT cyber security challenges lay in the system's own inherent vulnerabilities which expose the infrastructure setup to various attacks. The sources may include firmware, hardware (device), system applications, data, as well as the network interfaces or ports. Also, the bi-directional communication links between objects-to-objects leave the system open for network-related attacks and protocol failure. Other related

9. IoT Application and Service Domains:

Considering the recent advances made in IoT platforms, it is nearly impossible to envisage the numerous IoT applications, having in mind the continuous innovation in the technology, services and continuous needs in the industry. The current application domains include (but are not limited to) independent living (smart homes), smart cities, smart energy (smart grid and metering), smart mobility and transport, healthcare, retail and logistics, environmental monitoring, smart manufacturing There are security challenges associated with all of these areas where the domain specifics raise different concerns. Some are very obvious and generally discussed as security breaches related to healthcare opening for misuse of very personal information the etrade/retailing may open for monetary/financial misuse, but also the fast evolving.

9.1 Smart Grid:

There are huge possibilities to make a city 'smart' in the perspective of IoT. The domain covers activity sensing and events tracking, involving interactive objects in a smart environment. IoT application in a Smart City involves a huge variety of both infrastructure and technology requirements. One of the areas emerging with huge IoT potentials is the energy domain/smart energy. Smart energy (grid) is a kind of ''Internet'' in which the energy packet is managed similarly to the data packet—across routers and gateways which can autonomously decide the best pathway for the packet to reach its destination with the best integrity levels [18].The ''Internet of Energy (IoEn)'' concept is defined as a network infrastructure based on standard and interoperable communication transceivers, gateways and protocols allowing a real-time balance between a local and a global energy generation,

storage, distribution and demand optimization. The IEEE 2030 standard on smart energy identifies Wide Area Network (WAN), Field/Neighbour hood Area Network (FAN/NAN) and Home Area Network (HAN) as the major components of a smart grid.

9.2. Smart Metering:

According to Vermesan and Friess, IoEn is expected to provide an innovative concept for power distribution, energy storage, grid monitoring and communication as presented in[19]. IoT as a supporting platform supports energy distribution as when and where energy is needed. Thus, power consumption monitoring is performed at all levels; from local (home) devices to national and international distribution point [20].

9.3 The advanced Product supply chains are complex & weak:

Figure 03 Stated about the Product supply chain Model of Complex and weak in attacks and service

Figure -4 refers about the Many players, multiple attack opportunities

10 Device Management:

- A remote server opens a secure channel in a mutual authenticated TLS session
- This secure channel can be now used to change the configuration of the device and update/modify parts of the firmware/RTOS/apps/services

11. Data Table:

After a careful survey, the following information's are recorded in the data table for the proper conduction of research work analysis of result. The following information are given below

11.1 Application of Internet of things (IoT) on Cyber Security and control:

Companies/ Offices	No of Respondent	Use of Models	Positive Response	Percentage %
GOOGLE CLOUD	30	FESM	21 (30)	70%
AMAZON	30	SMS	24(30)	80%
FLIP CARD	30	FESM	26 (30)	**86.66**
SECURE THING Z	30	FESM	24(30)	80%
AVINET	30	FESM	21 (30)	70%
MACRO CHIEF	30	FESM	24(30)	80%
IAR ARM	30	FESM	28 (30)	93.33%
NP REMESAS	30	FESM	24(30)	80%
SILICON	30	PSMC	23 (30)	76,66%
/WOW AVNET	30	FESM	25(30)	83.33
Total	300		240(300)	80.00%

Mean = 30

11.2 Mean (PR)-24.0 Mean (NR) =60/10 =6.00

From the above table, we may understand Mean Value= Sum total of Respondents/number of users 300/10=30 Respondent's from each company. Out of 300 Respondent's 240(300) is response positive and the mean value is 24.0 and the negative repodent is 80/10 =8.00.

12. Final Result Table:

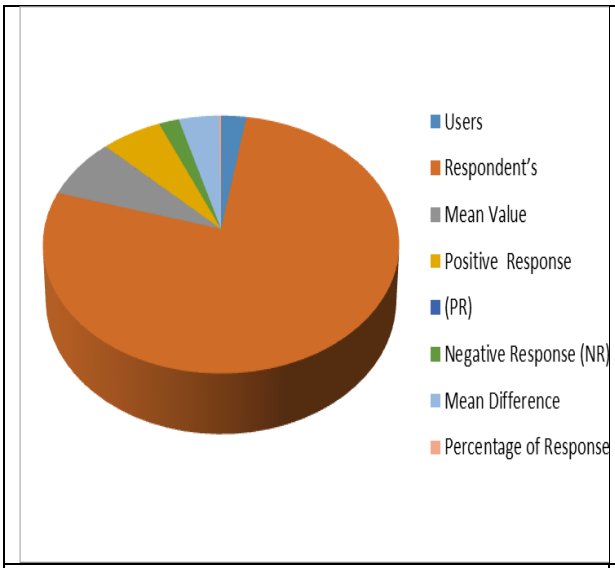
In this section, we have obtained a very good data from the respondents , out of 300 respondent's 240 people response positively and 60 number not the favour of use of IoT in cyber security and its control has a great impact and useful.

Users	10
Respondent's	300
Mean Value	30.00
Positive Response (PR)	24.00
Negative Response (NR)	8.00
Mean Difference	16.00
Percentage of Response	80.00%

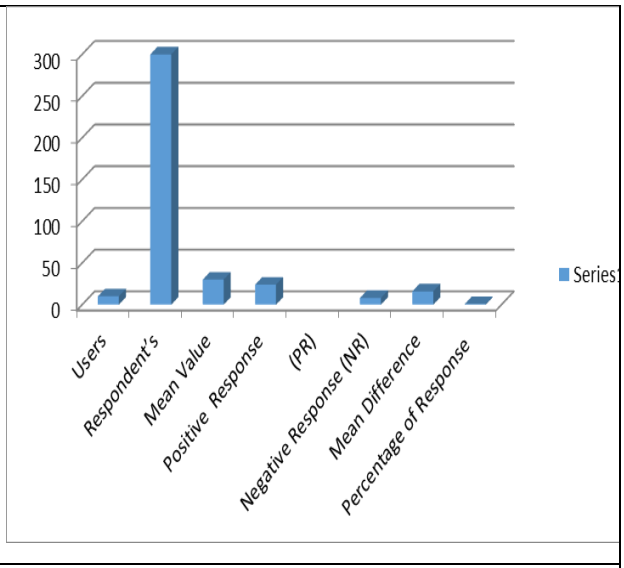
13, Hypothesis Testing:

In this section, from the final result table and the data table, we came to know that the null hypothesis is not true due to lack of support of response (against the Statement of Hypothesis) and most of respondent support the application of IoT for cyber security and its control when use of IoT in different constrains and Platforms. Thus, we have rejected the null hypotheses and accept the alternative hypothec due to its significance in both the levels of alpha 0.1 and 0.5 Points. Here the semantic models of response model also presented for your kind perusal and understanding.

13,1 Semantic Response Models in Pie chart:



Semantic Response Models in Pie chart



Semantic Response Models in Graph chart

Figure -7 Refers Model for Alignment for a secure future

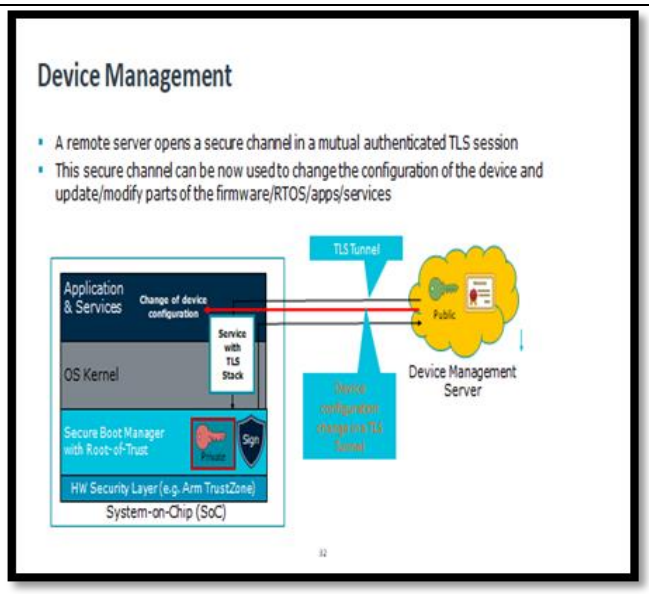


Figure -8 Refers Model for Device Management for a Secure future

Conclusion:

In this paper, an attempt has been made to evaluate the taxonomy of various system inherent vulnerabilities which expose IoT infrastructure and applications to various cyber threat vectors and make a case for research effort in this emerging technology. Our discussion involves the identification of different vulnerabilities inherent within IoT application and service domains. We executed two different attack scenarios (tests) on smart metering communication infrastructure setup. Our tests results show vulnerable IoT systems (being it application, hardware, software or firmware) could be abused by various threat actors via crafted vectors. Finally, it is critical to continue the discussion while at the same time challenging device manufacturers and components' vendors to design, and implement solutions so as to counteract threats from cyber adversaries so as to guarantee consumer utmost trust in IoT innovation and transformation

References:

[1.]Statista.https://www.statista.com/statistics/471264/iot-number-of-connected-devicesworldwide/

[.2.] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.

[3.] Karimi, K., & Atkinson, G. (2013). What the Internet of Things (IoT) needs to become a reality. White Paper, Free Scale and ARM

[.4.] Caceres, R., & Friday, A. (2012). Ubicomp systems at 20: Progress, opportunities, and challenges. IEEE Pervasive Computing, 11(1), 14–21.

[5.] Lo´pez, T. S., Ranasinghe, D. C., Harrison, M., & McFarlane, D. (2012). Adding sense to the Internet of Things. Personal and Ubiquitous Computing, 16(3), 291–308

[.6] Lund, D., Turner, V., MacGillivray, C., & Morales, M. (2014). Worldwide and regional Internet of Things (IoT) 2014–2020 forecast: A virtuous circle of proven value and demand. IDC.

[7] Matuszak, G., Bell, G., & Le, D. (2015). Security and the IoT ecosystem. KPMG, December 2015, 132631–G.

[8.] Darianian, M., & Michael, M. P. (2008) Smart home mobile RFID-based Internet-of-Things systems and services. In International conference on advanced computer theory and engineering, 2008.ICACTE'08 (pp. 116–120).

[9] Ashton, K. (2009). That 'Internet of Things' thing. RFID Journal, 22, 97–114.

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

[11.] ITU. (2005). ITU network reports, Internet of Things, Geneva.

[12.] Evans, D. L., Bond, P. J., & Bement, A. L., Jr. (2004). Standards for security categorization of federal information and information systems. Gaithersburg: U. S. Department of Commerce.

[13]. Pandya, D., & Patel, N. J. (2016). OWASP top 10 vulnerability analyses in government websites. International Journal of Enterprise Computing and Business Systems, 6(1).

[14.] Touhill, G. J., & Touhill, J. C. (2014). Cyber security for executives: A practical approach. Hoboken, NJ: Wiley.

****