iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6205

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Data Safety and Integrity Issue in IoT

Rahul Reddy Nadikattu
Department of Information Technology, University of the Cumberlands

Abstract: ***The IoT, also commonly referred to as (Internet of Things) may also be viewed as the new or modern paradigm that effectively combines all of the technological components towards coming up with effective services that best fit different approaches in the lives of all human beings. Ideally, the ubiquitous embedded technological gadgets, communication devices, sensor technologies, internet protocols, and pervasive computing is all combined and embedded together using IoT to come up with tools that work simultaneously together towards forming real-time digital systems that seamlessly perform in a symbiotic relationship. In the internet of things, the smart technological object is the structure or building block of the entire IoT architecture. This is mainly because, IoT is designed through merging various pieces of intelligence into daily smart objects that communicate through passing real-time information in the entire environment and through control or interactions with the physical world (Ashok, 2015). Moreover, IoT also requires that the objects should be in constant connectivity via the internet to enable the real-time exchange of information and data. Finally, in the IoT the numerous amount or number of the interconnected technological gadgets or devices alongside the vast amount of current data that brings about new unique opportunities for developers to create useful services that help create increased tangible benefits to the local citizens, the economy, environment and society in general. This research paper will focus on providing a comprehensive and candid evaluation of the Internet of Things. Moreover, this study will also review the data safety and integrity issues that are in IoT. Finally, for this study to achieve all of this, this paper will pay special attention to the case study on Dell, Inc's presence in IoT data and technological information solutions (Ashok, 2015). .***

Keywords: IoT, Dell, Data Safety and Integrity, America, Security Threats, Cybersecurity

I. INTERNET OF THINGS (IOT)

IoT may also be viewed as a comprehensive network of different interconnected technological systems that are always in both wireless and wired connectivity that mainly comprise of numerous hardware and software solutions for instance: transportation, large scale deployments, management of infrastructure, automation and building automation, conducting aerospace surveys, healthcare, and medical systems, logistics management, electronic commerce, agricultural irrigation, smart energy solutions, and intelligent manufacturing management solutions (Amnar et al., 2013). The main goal and objective of the internet of things (IoT) are entirely turning the previous traditional or manual products into digital and automated products that communicate together on a real-time basis via the internet infrastructure which allows them to exchange data, achieving remote control and monitoring objectives (Saniya & Rohit, 2015). Moreover, IoT comes with numerous advantages that range from efficiency in the data exchange and data collection (Saniya & Rohit, 2015). Furthermore, the internet of things (IoT) is responsible for protecting the entire environment through increased cost savings on energy solutions. Ideally, IoT is also useful in enabling advanced security options through interconnecting the virtual and physical technological devices based on the current interoperable communication and information technologies. It, therefore, follows that IoT generally involves various technical applications, domains, and protocols m (Audrey & Michael, 2016).

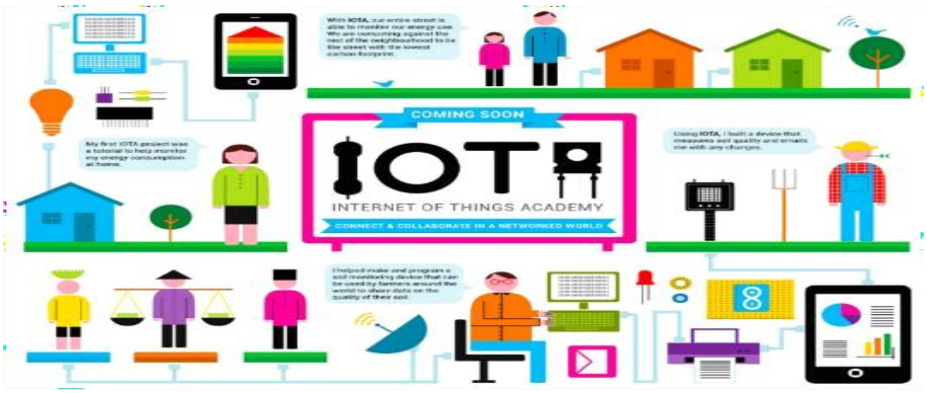


Figure 2: Showing the Conception of Internet of Things Sourced from (Audrey & Michael, 2016)

A. Brief Historical Overview of Internet

According to (Audrey & Michael, 2016), the modified automated Coke digital machine was manufactured at Carnegie Mellon University in the year 1982. It had the unique ability to report the current inventory and temperature. The authors (Aikaterini, Melanie & Andre, 2010), strongly believe that this was the first instance of an internet-connected device. Moreover, the phrase Internet of Things (IoT) is an ingenious terminology that was perfectly coined by Peter T. Lewis during his speech in the year 1985 at the FCC, also Federal Communication Commission. Additionally, Mark Weiser, in the year 1991who was the United States' chief scientist, and the principal founder of the "ubiquitous computing," managed to write a research paper that conceptualized the concept of the internet of things through the ubiquitous computing (David et al., 2012).

Moreover, Echelon company's engineer known as Reza Raji managed to successfully define the term internet of things also IoT in Palo Alto in the year 1994 as simultaneously moving real-time packets of data to other large or numerous nodes that aim at automating and integrating all of the local home technological appliances to the factories. This successfully marked the incorporation of IoT from the year 1994 to 1996 that saw other multinational corporations, for instance: NEST, Novell, Microsoft, among others, provides comprehensive digital network products for the incorporation of the internet of things. Consequently, Kevin Ashton, who was a technological pioneer from the U.K., co-founded MIT's Auto-ID Center in 1999. According to (Aikaterini, Melanie & Andre, 2010), his deliberate strategic option of utilizing RFID and radio-frequency identification successfully increased the popularity of the internet of things. Moreover, the popularity of the internet of things. Moreover, the internet of things technology eventually transformed into other different technologies, for instance, the embedded technological systems, the micro-electromechanical systems also MEMS, and finally, wireless communication devices. Therefore, these technical realms regularly work together simultaneously to contribute to the internet of things IoT.

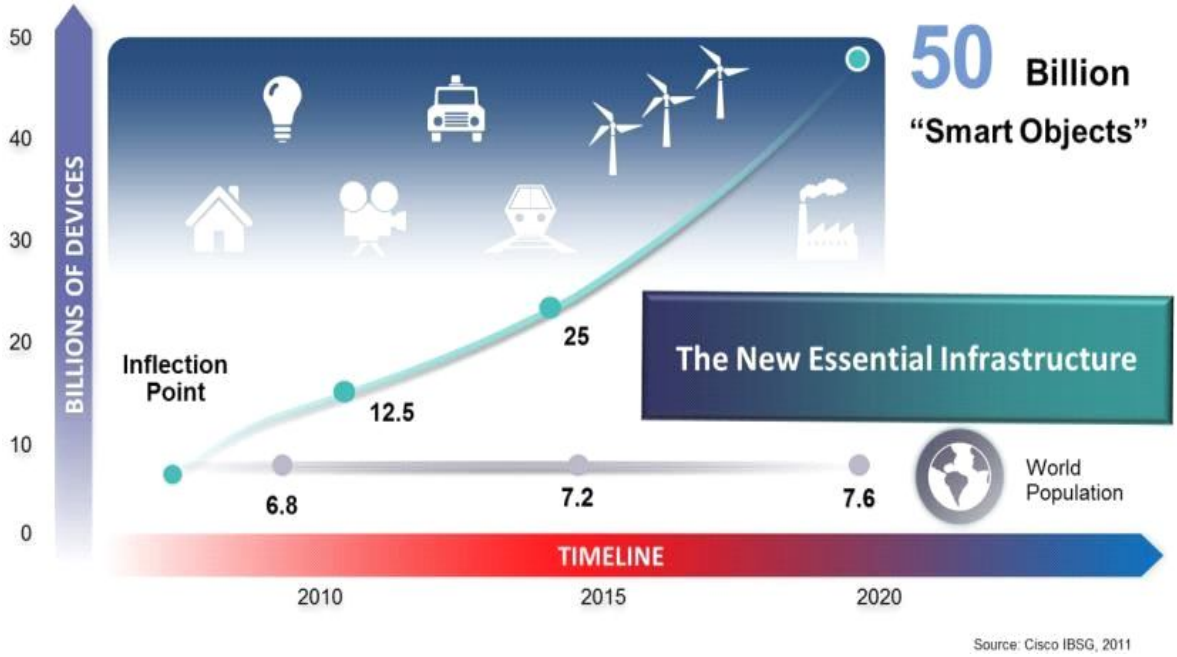


Figure Showing the total increase in the number of technological devices connected to the IoT (David et al., 2012)

B. Applications of IoT: How IoT helps all Americans

The authors (Audrey & Michael, 2016), predicted that the successful introduction of the internet of things IoT is bound to result into the following benefits for all Americans and other locals across the entire globe:

1) Expected improvements in the intelligence and information obtained from the interconnected virtual and physical objects
2) Promotion of the increased interactions between the general environment and the individuals living in the society
3) Enhancing the security, operational efficiency and reliability
4) Reducing the consumption and costs of energy

This section of the research study will mainly focus on demonstrating some of the potential and viable areas of Internet of Things (IoT). Ideally, some of the few areas of IoT applications that will signify how Americans will utilize IoT include the following: (1) Smart Mobility, (2) Smart Homes and finally (3) Smart Health (David et al., 2012).

C. Smart Mobility

Introducing the modern concept of digital internet vehicles is critical in giving rise to safer and more comfortable transportation strategies for communicators and residents. Smart mobility is a concept that is enhanced through IoT that mainly aims at creating convenience, intensifying mobility, security, and safe transport systems through the use of three critical elements in the internet vehicles, for instance, vehicle-to-infrastructure communication, vehicle-to-vehicle communication security and network security (David et al., 2012). Finally, Smart Motors is key in ensuring fuel economy since they guarantee green or eco-friendly transportation,

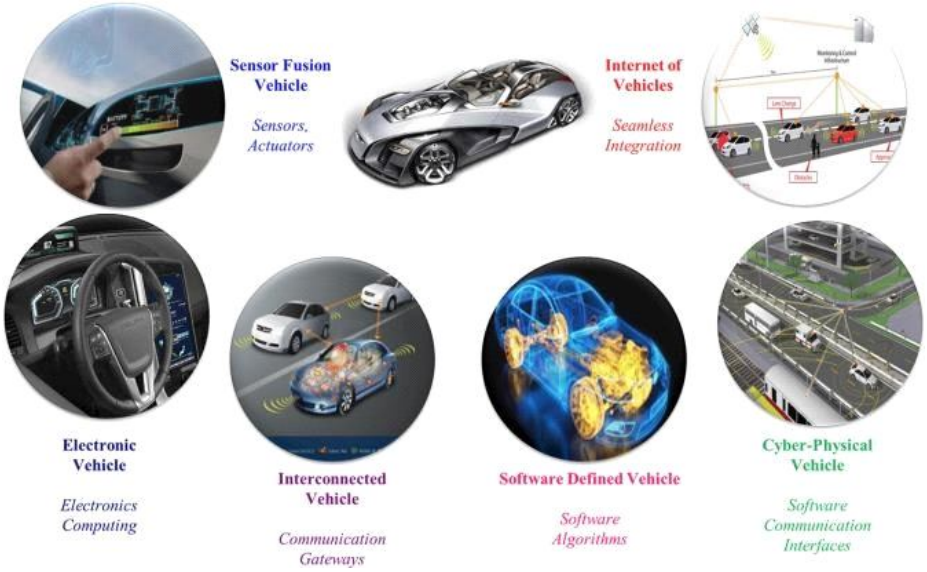


Figure 4: Showing the concept of the internet or digital vehicles Sourced from: (Aikaterini, Melanie & Andre, 2010)

D. Smart Homes

Most families and homesteads in this modern period in time have homes that are built with WiFi technological devices that allow the owners to access the premise using their iPhone and other technical devices like their smart T.V. (M.U., Muhammad & Anjum, 2015). Ideally, the home internet protocol network plays a critical function in the conception of the Smart Home. This is mainly because it contributes to the comprehensive environmental monitoring, assisted living, convenience, and finally, comfort. With the help of IoT, numerous technological sensors are carefully employed with the sole purpose of collecting data on natural environmental conditions like atmospheric pressure, noises, humidity, lighting, and temperature. The smart-home IoT technological application is critical in utilizing the intelligence and data to control the security, ventilation, heating, light, and air conditioning of the entire homestead (Aikaterini, Melanie & Andre, 2010).

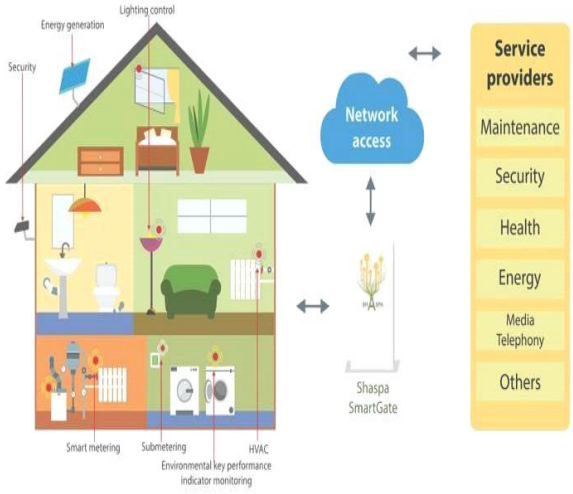


Figure Showing the IoT concept of Smart Home

E. Smart Health Applications

The internet of things also IoT technological devices may be effectively utilized in enhancing remote healthcare monitoring patients. In recent modern times, the smart health technological devices have increasingly become more popular in the economy with the intervention of the wearable data capture technological tools that use Bluetooth light energy technology, smartwatches, pet wearable devices, pregnancy wearable gadgets, baby wearable devices, tracking industrial products, fitness devices among other intelligent applications. The Smart Health application captures the patient's data using in-built sensors, which is transmitted through GPRS to remote physician or doctor monitoring locations (M.U., Muhammad & Anjum, 2015).

F. Problem Statement: IoT Data Safety and Integrity

The data safety and integrity issues in the IoT are one of the significant drawbacks affecting the successful implementation of IoT. The unethical and biased security and data attackers may reliably utilize different strategies in the different layers to attack the current data by tapping into the entire IoT digital network. Moreover, with an increase in the evolution of IoT and as more and more users increasingly appreciate the smart technological devices powered with IoT, the cyberattacks and crimes are also becoming the most viable threat affecting the existence of IoT. Therefore, one of the most critical considerations in the design of unique IoT system networks is the safety and the integrity of the data within these systems (Rabi, Manas & Suresh, 2011).

Figure 6: Showing the Smart Health application Sourced from:

The internet computer and internet controlled Smart devices in the vehicles, for instance: dashboards, locks, engines, and breakers, have increasingly been susceptible and more vulnerable to increased cyber attacks from unethical hackers. They use all means to access the IoT network illegally. Since the IoT network may be viewed as a vibrant and viable source of intelligence, it will always be prone to more advanced and sophisticated security attacks. There are several security concerns from the view of the IoT end users concerning the safety and security of IoT networks. The security concerns include the following:

1) Lack of sufficient data security for the interlinked or connected technology devices
2) Website interfaces that are insecure and prone to attacks
3) Firmware or software that is insecure
4) Mobile applications or interfaces that is insecure
5) Network services that is insecure
6) Inefficient authentication and authorization systems
7) Confidentiality and privacy concerns
8) Data safety and integrity issues
9) DdoS also Distributed Denial-of-service threats

The data security and integrity issues are an essential and critical concern for the end-users and the providers of the IoT systems network(Priyanka & Nikita, 2015). Therefore, this paper's main objective is to provide a candid and comprehensive analysis of the data safety and integrity issues in IoT. This paper will utilize the case study on Dell Inc's IoT strategy, to provide a practical understanding of the data safety and integrity issues in IoT. Moreover, this paper will utilize the theoretical framework on the layered structure of IoT to provide mechanisms on how Dell Inc could implement security measures to capture the safety needs of all the layers in the IoT architecture. Finally, this study will propose the IoTSM also Internet of Things Security Management System as the solution for providing seamless security measures during the installation of the IoT devices, design of the software, and sensors for remote monitoring. The IoTSMS should be empowered to simultaneously handle numerous interconnected devices and systems in the IoT network that will ensure maximum data safety and integrity. monitoring. The IoTSMS should be empowered with the capability of simultaneously handling numerous interconnected devices and systems in the IoT network that will ensure maximum data safety and integrity.

G. Case Study/Review: Dell, Inc.

Dell Inc is a technological multinational corporation that actively manufactures technological gadgets and devices. Recently, Dell Inc launched its new IoT technical products, and the company is also focusing on entering into other long-term partnerships with companies like Microsoft that will enable the consumers to be able to handle the deployment of the complexities arising from IoT (Dell.com, n.d.). This is a significant move that will initiate those transformations into the digital era. Moreover, the new product by Dell Inc, for instance, the "VMware Pulse IoT Center" is mainly tasked with the responsibility of securing the management solutions of IoT infrastructure by enabling the consumers to gain total control of their networked or connected technological products (Rabi, Manas & Suresh, 2011).

Ideally, VMware Pulse IoT is an ingenious product by Dell, Inc that increasingly enabling the consumers to protect, scale-up, and manage all of their IoT projects. This is mainly because it is the most preferred enterprise monitoring and management solution for all of Dell's gateways (Dell.com, n.d.). Moreover, Dell Inc has also ventured into the IoT consultancy and advisory services with the help of Dell EMC to assist developers in identifying the right IoT system architecture and safety capabilities that are required to protect and leverage on the intelligence and information in the IoT system network through the technological devices like connected devices, wearable, smart mobile phones, gateways, beacons and sensors (Priyanka & Nikita, 2015). The move to further intensify the security in the IoT network will go a long way in utilizing the data in optimizing significant operations, reducing security risks and compliance, and creating numerous opportunities for consumer engagement activities. Dell Inc has increasingly offered different products under the domain of IoT, for instance: IoT Labs, IoT Industries, IoT Services, IoT Security, and IoT Analytics (Dell.com, n.d.).

H. Theoretical Framework: Security Concerns in the IoT Layers

To effectively comprehend the data safety and integrity issues in IoT, this paper will adopt the conceptual framework on the security concerts in the various IoT layers. The primary function of the IoT architecture has been subdivided into four (4) main distinct layers, for instance, the application layer, service layer, network layer, and element. The four different IoT layers are susceptible to various security concerns; for example, the element layer that is mainly composed of smart technological applications further requires low power and computing sensors. Moreover, intelligent technological devices are increasingly susceptible to spoofing attacks, eavesdropping, and unauthorized access. Therefore, the various IoT layers require different security measures to enforce the data security measures for the IoT. Finally, the proposed IoTSMS will result in protection and security aspects in the IoT network, for instance: non-repudiation, integrity, and confidentiality. Moreover, the IoTSMS will also intensify the prevention of denial-of-service attacks, access control measures, authentication, and authorization (Dell.com, n.d.)

Dell Inc should comprehend the IoT layered structure in developing applications that best meet the security needs of the different layers. Ideally, the four main layers of the IoT architecture include the following: element layer, network layer, service layer, and finally, the application layers. Firstly, the most fundamental layer in the IoT structure is the element layer that incorporates the smart devices, actuators, and sensors responsible for collecting real-time data. Secondly, the network layer is the infrastructure supporting communication by providing security and bandwidth requirements.

The network layer also allows different organizations to use and share similar data through sourcing information, vast raw data (Mounib, Mouhcine & Hussein, 2013).

Finally, the application IoT layer is useful in providing the right user interface for the IoT network through supporting various technological applications like smart cities, supply chains, transportation, and healthcare (Lee, 2015). The primary data safety and integrity challenges emanate from the fact that IoT utilizes numerous data. A large number of physical components and devices are responsible for powering the increased efficiency and conducting security management operations (Mounib, Mouhcine & Hussein, 2013).

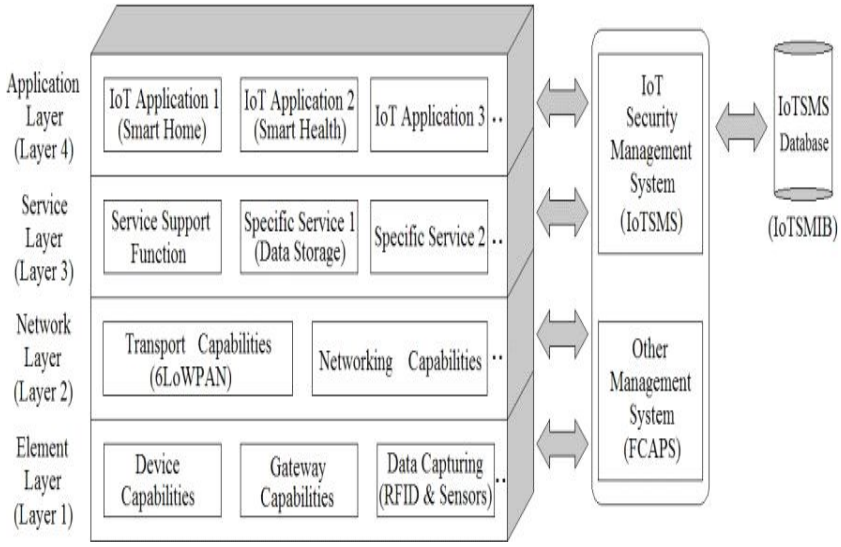


Figure 7: The IoT Layered Structure Sourced from

I. Data Flow between the IoT Layers

The data seamless data flow in the IoT layers may further be subdivided into the following four (4) major stages (please see figure 7 below):

1) Data collection
2) Data transmission
3) Data storage
4) Data analysis

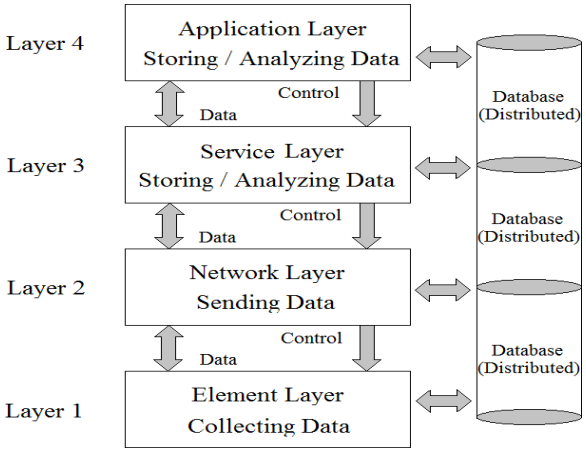


Figure 8 Data flow between the different layers in the IoT network

The data storage and collection in the IoT structure are critical in enabling the system to conduct the five major network management activities for instance: FCAPS also commonly known as: (1) fault, (2) configurations, (3) accounting and (4) performance and security. All of the IoT layers have their in-built security components, protocols and standards for communication. Therefore, the main advantage of the layered IoT structure includes the following:

a) Provision of effective IoT modular management by implementing various data safety and integrity protocols at all of the layers in enhancing the overall security of the entire system
b) Providing a layered IoT structure that is expandable since the lower layers are input services to the upper layers
c) Allowing new technology for the software and hardware to be included into the new IoT system.
d) Finally, the layered IoT system structure is very easy system structure to manage and configure in protecting the data safety and integrity.

J. Data Safety and Integrity Issues in IoT

According to (M. Fahandezh, M.Bondy & Erfani, 2009), the primary security challenge and the issue of IoT is the need for the right mechanisms for identity protection and authentication to ensure confidentiality of the users. Moreover, the three primary data security areas in the IoT network include data availability data integrity and data confidentiality (Lee, 2015). Furthermore, a breach of all of the three security and data integrity areas may eventually affect the integrity of these systems by damaging the entire IoT network. Furthermore, data confidentiality is another essential element of enforcing data integrity (Priyanka & Nikita, 2015).

This is mainly because it is responsible for protecting the privacy of details or information through preventing unauthorized or illegal access. Ideally, for the IoT technological devices, the technological tools like nodes and sensors, data confidentiality include instituting systems aimed at preventing unauthorized transmission of the data to unauthorized persons. These devices actively encrypt the data by converting it into ciphertext, which will prevent unauthorized persons from accessing it. Moreover, the two-step data verification process is another essential method of ensuring that data confidentiality is enforced in the IoT network (M. Fahandezh, M.Bondy & Erfani, 2009).

Figure 9 Showing the Basic IoT Security Requirements (Lee,2015)

II. SECURITY MECHANISMS OF INTERNET OF THINGS (IOT)

The security measures of the internet of things are purely based on restricted technological gadgets, such as low-energy wireless Bluetooth devices. Therefore, it is essential to ensure the ensure or consider the security systems for the IoT demands during the design of the IoT network because all of the sensors and nodes of the IoT have low-computing capabilities. They do not consume a lot of power (Luigi, Antonio & Giacomo, 2010). This goes a long way in implying that the security needs for these IoT gadgets or devices should be designed to be lightweight as possible. If the security mechanisms of the IoT devices are inefficient, the data collected through nodes and sensors may not be effective in capturing the intruders, or it may also be utilized in destroying the entire system (Jason et al., 2015).

A. *Data Safety and Security Threats in the Element Layer*

The element layer of the IoT is composed of different sensors and nodes used in collecting intelligence from the entire network environment. The sensors and nodes may be susceptible to the various security risks and threats, for instance: spoofing, eavesdropping, and unauthorized access (M. Fahandezh, M.Bondy & Erfani, 2009). Therefore, the spoofing, eavesdropping, unauthorized access of the cyberattacks at the element layer should be enforced through creating user confidentiality services, access control measures, and system authentication measures that protect this layer of the IoT from malicious attacks.

Moreover, Dell Inc could actively utilize the element layer authentication services in using the hash algorithms to effectively provide digital signatures that help prevent illegal access through the cyber attacks. Moreover, the use of user access control mechanisms is vital in countering the rate of eavesdropping. Finally, the PKI also public key infrastructure is critical in enforcing the desired level of confidentiality in the data gathered from the users through the smart devices and sensors (Klaus, 2010).

B. *Data Safety and Security Threats in the Network Layer*

The IoT's network layer is essential in transmitting the collected data through the sensors and nodes to the final user terminal through the wireless network. However, there are different security risks at this layer of the IoT, for instance: the malicious code injections, man-in-the-middle attacks, and finally, DoS also denial of service attacks (Jason et al., 2015). Ideally, Dell Inc could enforce appropriate security measures at the network security layer through the non-denial and availability of services that are utilized by filtering the router to counter the denial of service attacks at the network layer. Moreover, the encryption of data is also useful in countering the man-in-the-middle security attacks. In contrast, anti-virus software combats malicious viruses or code injections into the IoT network (Klaus, 2010).

C. *Data Safety and Security Threats in the Service Layer*

The security threats in the service layer include malicious insider, unauthorized access, and DoS attacks. Dell, Inc could avail the non-denial of the services through the IDS also Intrusion Detection System that is very effective in countering all of the denials of the service attacks (Lee, 2015). Moreover, the mechanisms to prevent illegal access are essential in preventing unauthorized persons from accessing and manipulating the integrity of the IoT data. Finally, event monitoring is also required to counter malicious insider cyber attacks (Fahandezh, 2005).

D. *Data Safety and Security Threats in the Application Layer*

The data safety, security, and integrity issues at the application layer of the IoT include phishing cyber attacks, code injection attacks, and finally, DDoS attacks. Therefore, Dell, Inc could counter the data safety and security threats in this layer through availing IDS also Intrusion Detection System that will effectively combat the distribution of the denial service attacks. Moreover, the anti-virus software mechanisms are essential in countering spam filtration and code injection malicious attacks. Finally, the tools for filtering spam are also useful in countering all of the illegal phishing cyber attacks in the IoT network.

III. SOLUTION FOR THE DATA SAFETY AND INTEGRITY PROBLEM OF IOT: IOTSMS

A. *IoTSMS: Internet of Things Security Management System*

In enforcing data safety and integrity in the IoT, this paper proposes IoTSMS also Internet of Things Security Management Systems. The IoTSMS has four (4) major functional sections of layers (please see figure 9 below). The four major parts of IoTSMS include (1) IoT fundamental security function, (2) IoT security mechanisms management, (3) IoT security service management, and finally (4) IoT security business policy management (Daniel, Sabrina, Francesco & Imrich, 2012).

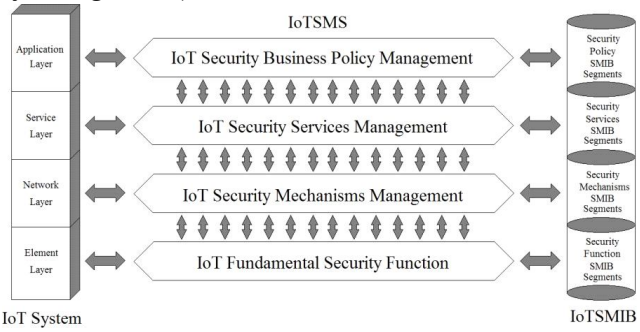


Figure Showing the Proposed IoTSMS Retrieved from (Daniel, Sabrina & Imrich, 2012)

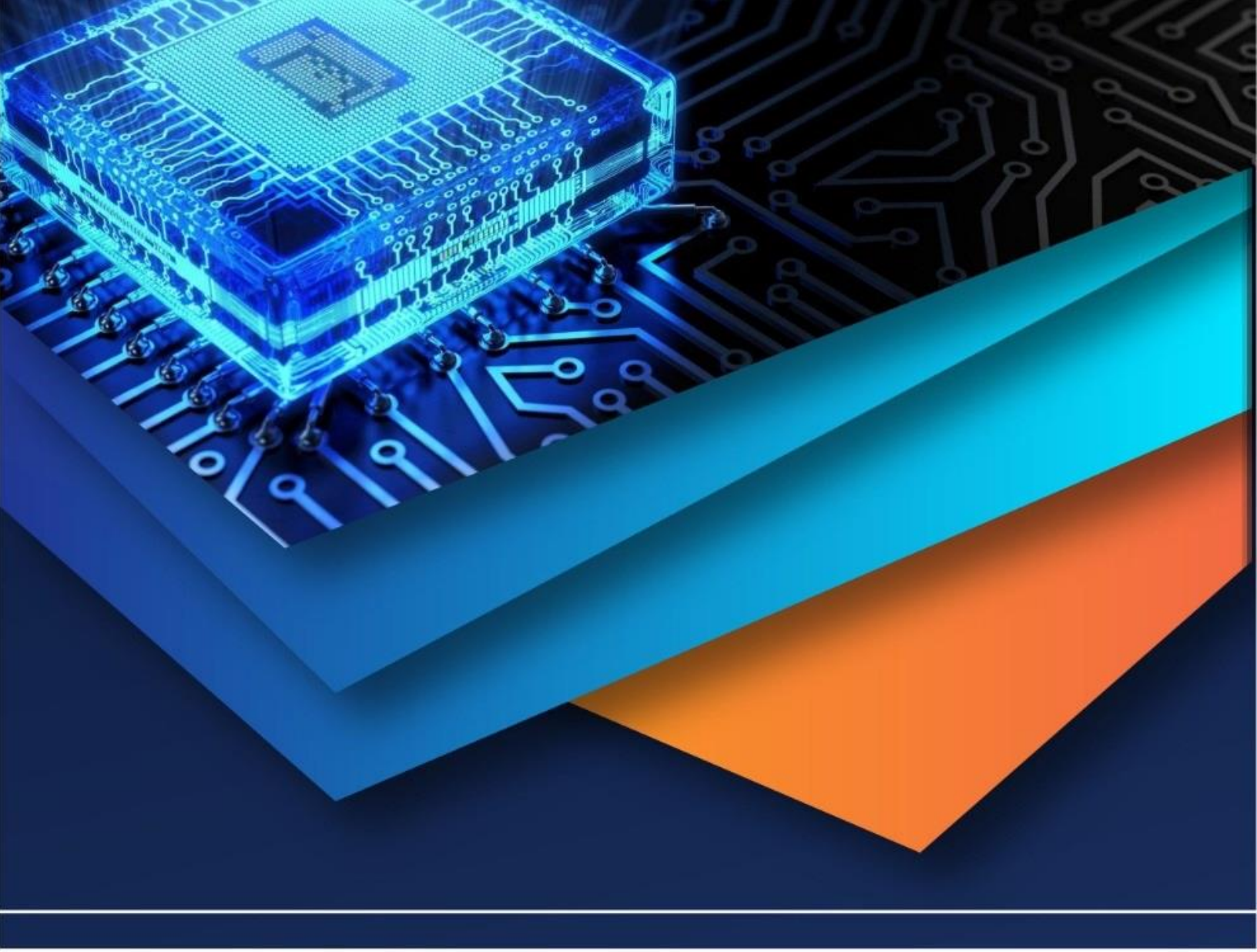
All of the different layers are responsible for performing a specific security activity or function. Moreover, the functionality of every segment in the IoTSMS is carefully selected to minimize the flow of data via the interface of the systems (Vasileios et al., 2015). Additionally, the total number of layers is in synch and compatible with the IoT system network layers to enforce the required security measures in the system. All of the different layers in the IoTSMS are equipped with another independent functionality for ensuring maximum management of the security. This is important in proving the data availability, data integrity, and data confidentiality in the IoTSMS (Daniel, Sabrina, Francesco & Imrich, 2012).

IV. CONCLUSION

This paper's main objective is to focus on evaluating the data safety and integrity issues in IoS. This paper has paid more attention to the case study on Dell technologies, which is a multinational corporation and its IoT strategy. Ideally, for Dell to enforce the right security measures, the proposed layered network approach has been used in describing how Dell will be useful in enforcing maximum data safety and integrity in all of the gadgets produced for the IoT network. Moreover, the paper has revealed that different layers of the IoT, for instance, element, system, service, and application layer have different security needs. This is important in informing how Dell, Inc should incorporate various security measures at every level or thickness of the IoT in enforcing maximum safety and security of the entire system. Finally, the paper has proposed introducing the IoTSMS as a viable remedy to the data safety and integrity challenge affecting the IoT network (Mr. Ravi & Prof. Raj, 2014)

REFERENCES

[1] Ashok Subash, (July 2015). IoTivity – Connecting Things in IoT, TIZEN Developer Summit,pp1-48.
[2] Amnar Almomani, B. B. Gupta, Samer Atawneh, A. Meulenberg, Eman Almomani, (Marc 2013). “A Survey of Phising Email Filtering Techniques,” IEEE Communication Survey & Tutorials, vol. 15, pp. 2070-2090.
[3] Audrey A. Gendreau, Michael Moorman, (August 2016). “Survey of Intrusion Detection System towards an End to End Secure Internet of Things,” IEEE 4th International Conference on Future Internet of Things and Cloud, pp. 84-90,
[4] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum, (November 2010). “Classification of RFID Attacks,” A Journal of Research and Innovation, vol. 12, pp. 491-505.
[5] Davide Conzon, Thomas Bolognesi, Paolo Brizzi, Antonio Lotito, Riccardo Tomasi, Maurizio A. Spirito, (August 2012). “An XMPP Based Architecture for Secure IoT Communications,” Interational Conference on Computer Communications and Networks, pp. 1-6.
[6] Dell.com., (n.d.). Dell IoT solution. Retrieved from https://www.dell.com/learn/us/en/04oem/oem-internet-of-things
[7] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, (September 2012). “Internet of Things: Vision, applications and research challenges,” Ad Hoc Networks, vol 10, pp.1497-1516.
[8] Fahandezh, M., (2005). “A Framework for IPSec Functional Architecture,” MASc Thesis, ECE, Faculty of Grad. Studies and Research,
[9] U. Windsor. Jason R.C Nurse, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, Sadie Creese, (September 2015). “Smart Insiders: Exploring the Threats from Insiders Using the Internet of Things,”
[10] Secure Internet of Things (SIoT), International Workshop on Secure Internet of Things, pp 5-14.
[11] Klaus Finkenzeller, (2010). RFID Handbook Fundamental and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. Wiltshire, UK: John Wiley & Sons, 3rd ed.
[12] Luigi Atzori, Antonio Iera & Giacomo Morabito, (October 2010). “The Internet of Things: A Survey,” Computer Networks, vol. 54, pp. 2787-2805.
[13] Lee Stogner, (August 2015). “An Introduction to the Internet of Things from the perspectiveof the IEEE Internet of Things initiative,” International Conference on Collaboration Technologies and System, pp. 506-506.
[14] M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, (February 2015). “A Critical Analysis on the Security Concerns of Internet of Things (IoT),” International Journal of Computer Applications, vol. 111, pp. 1-4.
[15] M. Fahandezh, M. Bondy, S. Erfani, (May 2009). “A Framework For Implementing IPSec Functional Architecture,” Canadian Conference on Electrical & Computer Engineering (CCECE), pp. 71-76.
[16] Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, (December 2013). “A Survey of Beacon-Enabled IEEE 802.15.4 MAC Protocol in Wireless Sensor Networks,” IEEE Communication Survey & Tutorials, vol. 16, pp. 856-876.
[17] Ovidiu Vermesan & Peter Friess, (2014). Internet of Things from Research and Innovation to Market Deployment. Aalborg, Denmark: River Publishers.
[18] Mr. Ravi Uttarkar and Prof. Raj Kulkarni, (June 2014). “Internet of Things: Architecture and Security,” International Journal of Computer Application, vol 3, pp. 12-19.
[19] Priyanka S. Fulare and Nikita Chavhan, (2015) “False Data Detection in Wireless Sensor Network with Secure Communication,” International Journal of Smart Sensors and AdHoc Networks, vol. 1, pp, 66-69.
[20] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy,(2011) “Cloud Computing: Security Issues and Research Challenges,” International Journal of Computer Science and Information Technology & Security, vol. 1, pp. 13-18.
[21] Saniya Vohra, Rohit Srivastava, (April 2015) A Survey on Techniques for Securing 6LoWPAN, Fifth International Conference on Communication Systems and Network Technologies, pp. 643-646.
[22] Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez-Gallego, Jesus Alonso Zarate (April 2015). A Survey on Application Layer Protocols for the Internet of Things, Transaction on IoT and Cloud Computing, pp. 1-8.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY