Examining the security and privacy on the Internet of Things and challenges ahead

Eisa Khodabandeh

Instructor in Shahid Motahari Faculty, Master's Degree in Educational Management and Faculty Member of Imam Hussein University

Eisa_٥٣٣@yahoo.com

Abstract

The Internet of Things allows the sharing of tasks and information between humans and makes objects immortal for themselves digital identity. The scope of the Internet usage of objects is very wide and can range from industrial machines to consumer goods. With the advent of this technology, the development of virtual objects has always been an important part of it. The Internet of Objects is a growing network of objects used in various industries.In recent years, the Internet of Things has been working in many areas, such as smart homes, supervised environments and industrial control systems, electronic health, smart city, Internet of eyes and urban security and safety, etc. Named. In this article, we intend to examine the security of information and privacy on the Internet, and to outline its challenges.

key words: Internet of Things, Security, Privacy, Challenges

Introduction

Kevin Ashton is accredited for using the term "Internet of Things" for the first time during a presentation in ۱۹۹۹ on supply-chain management.(Ashton K,۲۰۰۹)

The Internet of Things is a massive transformation of future-generation technologies that can affect all spectrum of business, and can also be identified as an interconnected device and smart object, using infrastructure The current Internet will be considered with the benefits of development

Given the technology trend, it's predictable that the Internet will be an integrated product of classical networks and networked objects. Content and Services will always be available and available. Internet device objects can be inclusive and enable environ mental intelligence.

IOT tries to establish advanced connectivity among the devices or systems or services in order to make automation. All things are connected to gather and all information would be interacted to each other over standard and different protocol domain and applications. (D. Giusto, A. Iera, G. Morabito, L. Atzori,۲۰۱۰)

The IOT will connect the physical and digital worlds allowing the bidirectional communication between them (Lee, K,۲۰۱٦)

A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network .

Objects' Internet applications can lead to increased health intelligence in the community On the Internet of things working, we have large-scale sensor networks for connecting each object with a unique identity in We expanded our physical world. The basic idea behind the Internet of Things is to enable the types of objects around us to connect to the network Such as smartphones, electronic tags, sensors, tablets and devicesThe other. (Ahuja,٢٠١٠)

The Internet of Things means that many of our everyday utilities are connected to the Internet, their tasks and information.To share with each other or with humans and cause immortal objects to have their own digital identities.

The Internet of Things gives the power to see, hear, think and work with each other, Share information The Internet of Things manipulates the basic technologies of these objects, such as ubiquitous computing, embedded devices, communication technologies, sensor networks, protocols and applications, from being traditional to being smart It turns.(Sajjad Hussain and yaqhoob, ٢٠١٦)

The Internet of Things enables various devices to communicate on a daily basis through the Internet. ThisDevices intelligently send information to the system and ensure they are monitored by actionsIt is necessary. The Internet of Objects aims to provide advanced mode of communication between devices and systems Also, facilitating human interaction with the virtual environment has found its application in almost every field.IOT covers a wide range of applications like healthcare, utilities, transport, agriculture etc. (Sundmaeker,٢٠١٠)

Although the definition of things has changed as technology evolved, the main goal of making computer sense information without the aid of human interference remains the same. A drastic development of the current Internet into a network of connected objects that not only gather information from the environment(sensing) and interacts with the physical world (command /control), but also uses existing Internet standards to provide services for information transfer, analytics, applications and communications.(J. Buckley,٢٠٠٦)

The Internet of Things provides the right solutions for a wide range of applications, such as intelligent City, traffic congestion, Waste Management, Structural Health, Security, Emergency Services, Procurement, Retail, Industrial Control, and Care Wellness offers.

IOT Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless large scale sensing, data analytics and information representation using cutting edge ubiquitous sensing and cloud computing.(Gubbi,٢٠١٣)

Internet of Things

The definition that the International Telecommunication Union has on the Internet of objects is as follows: at any time, any place, for anyone .We will have a connection for anything.

Interne of Things (IOT) is a concept that aims to enhance the forms of communication that we have today. Currently, the Internet is a network tool that humans access using devices. IOT attempts to not only have humans communicating through the Internet but also have objects or devices. These things are to be able to exchange information by themselves over the Internet, and new forms of Internet communication would be formed: human-things and things-things.(Tan,۲۰۱٤)

The main purpose of the design of this network is to share information in any object among other related objects, in Every time and any place is needed. To make sure the data is available at any time and place,Processing a large amount of data collected in applications such as environmental monitoring, air forecasting, transportation,Commerce, health and health, military applications and more. So use a powerful processing core Like the cloud next to the IoT, it's clear, and the combination of wireless sensor networks with cloud computing, sharing and An instant analysis of sensor information is possible. Also, the storage capacity issue may be by methods Cloud computing has been responded to in an effort to make security and easy access to information widely available Distributed and mobile environments

Layered Internet of Things

The ITU International Telecommunication Union is one of the world's leading telecommunication agencies dedicated to the design of the Internet of Things Has taken action. This architecture comes with layers: functional (app), support, networks, and devices with functionality Management and security and using Internet applications of objects to develop smart city, intelligent transportation, building Smart, intelligent energy, intelligent technology, intelligent health and intelligent life.

Categories Internet of Things

Three main types of network Ip based

۱. Internet of Industrial things
۲. Internet of consumer things
۳. Machine-to-machine connection

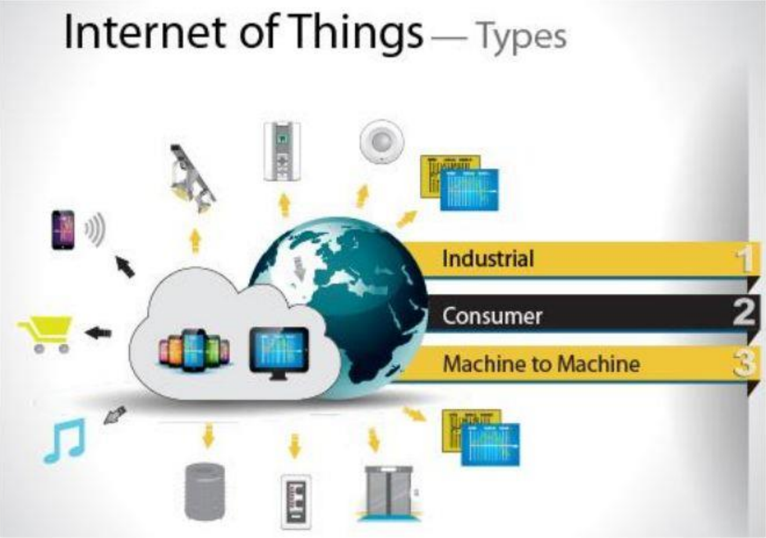


figure network Ip based

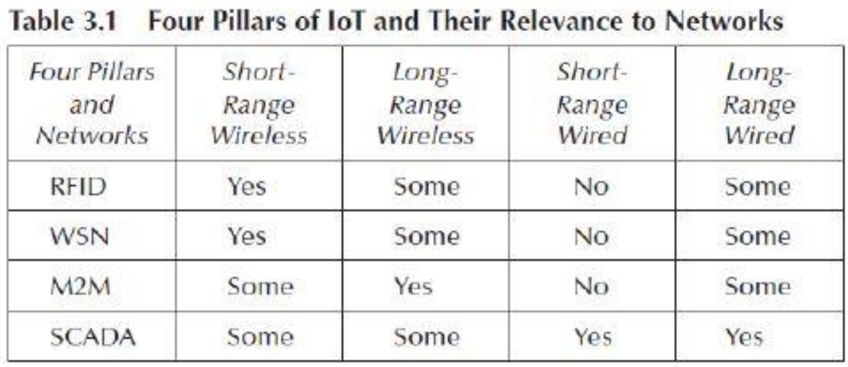
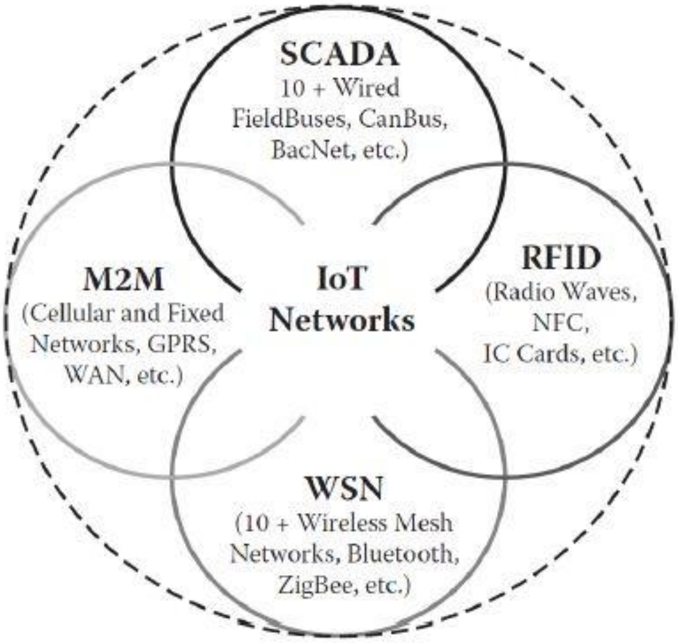


Table 3.1 Four Pillars of IoT and Their Relevance to Networks

Four Pillars and Networks	*Short-Range Wireless*	*Long-Range Wireless*	*Short-Range Wired*	*Long-Range Wired*
RFID	Yes	Some	No	Some
WSN	Yes	Some	No	Some
M2M	Some	Yes	No	Some
SCADA	Some	Some	Yes	Yes



Zhou Book An overall classification for things on the Internet is provided

IOT privacy and security:

As devices become more connected thanks to the IOT, security and privacy have become the primary concern among consumers and businesses. In fact, the protection of sensitive data ranked as the top concern (at ٣٦٪ of those polled) among enterprises, according to the ٢٠١٦ Vormetric Data Threat Report.

Cyber attacks are also a growing threat as more connected devices pop up around the globe. Hackers could penetrate connected cars, critical infrastructure, and even people's homes. As a result, several tech companies are focusing on cyber security in order to secure the privacy and safety of all this data (Meola,٢٠١٦)

The very rapid growth of Internet-connected devices, ranging from very simple sensors to highly complex cloud servers, shapes the Internet of Things, where Things, in this context, refers to a wide variety of objects (e.g. smart bulbs, smart locks, IP cameras, thermostats, electronic appliances, alarm clocks, vending machines, and more). The resemblance between all IOT objects is the ability to connect to the Internet and exchange data. The network connectivity feature allows controlling objects remotely across the existing network infrastructure, resulting in more integration with the real world and less human intervention. The IOT transforms these objects from being classical to smart by exploiting its underlying technologies such as pervasive computing, communication capabilities, Internet protocols, and applications. Protocols are required in order to identify the spoken language of the IOT devices in terms of the format of exchanged messages, and select the correct bound- aries that comply with the various functionality of each device. Applications determine levels of granularity and specialty of the IOT device and how big are the data generated for analytics purposes. They also indicate the general scope of the IOT framework covering the context of the applied domain (Mahmoud Ammar,٢٠١٨)

Because of the massive amount of information that IOT and wearable technologies can gather, privacy and security-related concerns will grow as these devices and services proliferate (*See* Patrick Thibodeau,٢٠١٤)

Users enjoy the personalization and customization that IOT and wearable technologies offer, yet those same capabilities that are so hotly demanded also exacerbate digital privacy and data security risks that already existed for traditional online services and technologies (*See* Jat Singh & Julia Powles,٢٠١٤)

These privacy- and security-related concerns can arise with regard to access to the device itself (i.e., what happens if it is lost or stolen); access to the information the device shares with nearby devices or systems (i.e., information shared over Wi-Fi or other wireless systems); or access to information transmitted to the cloud or to any remote storage system (Al Sacco,٢٠١٤)

This section will specifically explore how IOT technologies in general and wearables in particular challenge traditional privacy norms—both social and legal—and will explain why a more creative and flexible approach to dealing with these issues will be necessary. It is important that the privacy concerns regarding wearable technologies relate to both the users of those technologies and others in surrounding environments. For users, the privacy concern is that wearables allow a massive amount of data to be observed, gathered, and shared about them-potentially without their knowledge .

In turn, these new datasets might be used by third parties for marketing purposes, by employers for job-related purposes, or even by insurers to adjust user premiums. This possibility raises the specter of IOT and wearable devices and the datasets they generate being used in a supposedly discriminatory fashion (Adam Thierer,٢٠١٥)

The potential for such ubiquity (billions to trillions of devices) of IOT seems like a foregone conclusion at this point. But there are multi-dimensional privacy challenges which must be surmounted if this truly is going to become a reality. To get ahead of these challenges the privacy engineering community (via National Institute of Standards and Technology) is currently involved in intense discussions as to how to “engineer in” the right privacy regime, which will provide users (consumers) with direct control over a wide range of their own personal privacy settings as well as creating auditing and measuring schemes to ensure compliance with both user settings as well as regulatory mandates. Privacy engineering is a very real challenge, and there are multiple paths in the IOT where a privacy regime must be monitored and maintained:

- The device (data generator, data receiver and aggregation point).
- The Internet (multi-directional data transport).
- The cloud (data manipulation and aggregation point).
- The machine (application services, big data repositories, analytics and more).

Each path requires appropriate privacy protections to be engineered into it, with user control wherever appropriate (device, machine and others) while being maintained along its entire length (virtual and physical). High levels of encryption, redundancy and security will be necessitated to counter threats in flight as well as at the endpoints. There will also be regulatory controls and adherence monitoring, which must be facilitated along these same pathways. Most of these will fall under the auspices of FTC (US), Data Privacy Act (EU), and other regulatory bodies and statutes across the world. In parallel with the need for comprehensive privacy, security and compliance capabilities, the IOT is entirely predicated on new business models, which disrupt conventional solutions. An enabler of this disruption is the cost model component, which dictates low inherent costs in the devices, and all other components of the value chain. These cost models will not be conducive to “out of band” controls via bolt on solutions. Engineering-in privacy as part of the device and other pathway structures will be the only path to success in which cost efficiencies are maintained while compliance is assured along the way (Dini,٢٠١٧)

Internet Challenges of things

Technical Issues: These challenges cover the hardware and software sector. The huge amount of data received and processed, the number and type of sensors and labels, the amount of Internet penetration, attention to infrastructure, maintenance, and interoperability and compatibility of platforms are among these problems.Security and privacy issues: On the Internet, device objects send information and receive commands,Henceforth hacking and exploiting it is not far off.

Corporate finance professionals might agree when it comes to the Internet of Things (IOT). While this much-vaunted technological trend promises new operational efficiencies and revenue opportunities, IOT also poses significant transitional challenges across legacy supply chain management, data systems and departments within many organizations. Managing those challenges poorly could lead to losses or lower returns.

The promise of IOT in international supply chain management is high, in terms of both productivity and innovation, but it will be challenging for most companies to transition legacy supply chains to incorporate hundreds or even thousands of IOT devices and the data they deliver (Lynch,٢٠١٥)

On the Internet, sensor node objects are commonly used, resulting in reduced energy or nodes Sensor, most areas without valid sensor nodes are constantly displayed. With the application of routing information decisions Local, packets do not have the power to advance in this area.(Vermesan and fress,٢٠١٤)

There is another challenge in the insufficient qualification of employees regarding the digital change, this will alter requirements for employees across all the steps of the value chain. Through the IOT and the growing digitalization, the need for employees with a foundation in data science and information technology in particular will increase. Policymakers should create the basis for the education needed. They need to encourage enthusiasm for technology from the early stage (Galindo, ٢٠١٦)

Laura Domingo Galindo. ٢٠١٦. “The Challenges of Logistics ٤,٠ for the Supply Chain Management and the Information Technology”. Master Thesis Spring ٢٠١٦. Norwegian University of Science and Technology.

Lack of solid frameworks that provide guidance of IOT adoption in a supply chain context with clear guidelines and a roadmap. These would help in advising companies as to which process and where in the supply chain would they deploy IOT, given that supply chain partners may be at different stages of the IOT implementation. In addition, these frameworks would provide help with change management practices within the company and across the supply chain.

Lack of models that address supply chain problems in an IOT environment. Management of smart supply chains is different from that of traditional supply chains. Decision-making in an IOT context requires new tools and models that take into account this new environment, such as the abundance of big data generated from sensors and connected things. IOT will affect procurement, production planning, the management of inventory, quality and maintenance, among other issues. (Ben-Daya, Hassini & Bahroun, ٢٠١٧)

There are several barriers to the implementation of IOT in SCM[١] from both technological and managerial perspectives. A world where all things are connected opens the door for less security and privacy. (Tadejko, P. ٢٠١٥)

This is especially true in a supply chain context where information sharing has always been a big challenge. Another challenge is interoperability. Research by McKinsey suggests that ٤٠٪ of the value of the IOT will need to be unlocked via interoperability. (Manyika, Woetzel, Dobbs, Chui, Bisson, Bughin, Aharon, ٢٠١٥)

There is not much research addressing how to deal effectively with these challenges**.**

Internet Security Objectives of things

The need for security on the Internet is clear. For this, we need some things. In this section These requirements are confidential. We separate privacy and trust requirements from security requirements We pay them separately. It should be noted that security requirements generally have to be lawful And enforce the Internet Security policies in practice.

١. Preventing undesirable events
٢. Guaranteeing the safety of human life
٣. System availability
٤. Confidentiality and information integrity

[١] Supply Chain Management

٥. digital signatures and undeniable

٦. Information compatibility and security gauge in different systems

٧. Identification (uniquely), identity authentication of objects and individuals (multi-factors such as passwords, locations, biometrics, proofs No knowledge (and the ability to attribute each object to only one person)

٨. Different models for trusting and non-centralized authentication

٩. Authentication of sent messages

١٠. Oversight, Inspection, Security Management, and Access Control (Access and Use Rights, Sharing Rules)Value-added (and value licensing)

١١. Management, exchange and key agreement for the possibility of establishing a secure connection

١٢. Physical and logical protection of information

١٣. Hardware and Software Security) Wireless Communications Security in the Physical Layer (End-to-End Security)

١٤. Security and trust for cloud computing

١٥. Specify the protocol and algorithm used for the receiver while maintaining its security

١٦. Submitting and submitting reports

١٧. Ability to implement in limited environments with processing power and low memory

١٨. Minimizing power consumption and security overhead, and awareness of energy consumption in devices byReferences

١٩. Protection against hacking, penetration, male in the middle

٢٠. Protection against DoS, DDoS and Sybil

٢١. Protection against network layer attacks such as routing routing attacks, wormholes, black holes, etc.

٢٢. Protection against repeat attack, fingerprint attack and profiling

٢٣. Protection against phishing, hearing, jamming, and information extraction

٢٤. Ensuring ownership of the data, device or object for individuals

٢٥. Legal and Responsive Issues; Providing Security and Privacy Framework and Policies

٢٦. Acceptance of responsibility for certain operations by the user

٢٧. Reservoir management

٢٨. Low-cost and safe devices

٢٩. Prioritize messages and ensure messages are sent and received based on their priority

٣٠. Whether or not to discover a device when searching for it

٣١. Content review to identify degradation (eg for simple content such as temperature or humidity measurement)

٣٢. Use of accreditation mechanisms for discriminating discovery

٣٣. Ensuring system reliability

٣٤. Assessing the degree of autonomy required for security management by the system

٣٥. Ensure proper operation of all network layer activities in the system

٣٦. Examining the effect of stored history in applications in system security

٣٧. Exploring the use of Bridge in some cases necessary to maintain security or privacy

٣٨. Investigating the Effectiveness of System Security

٣٩. Use of Unique Identity in Global Identity

٤٠. The security layer shall be independent of other layers and may be replaced and replaced

Privacy requirements

Although privacy is considered a subset of security requirements, but here it is separately Reviewed. The reason for this is the potential significance of this issue, because the lack of privacy does not allow it to be accepted.The system is crowded with people, which ends up being the ultimate goal. The subject of privacy on the Internet is a lot of thingsIs more vital. Unlike ordinary Internet, the volume of measured information (from individuals or by individuals) is much higherTherefore, the disclosure of personal information is far greater. Personal information can include:Location, Acquired information (such as a degree, spouse), intrinsic information (such as gender, name), skills Individual, behavioral profiles, interests, job information, assets and property of a person from objects, And many other things, all of which must be delivered to the authoritative authorities with the consent of the person and there is no The seam of information in these cases is not acceptable by the persons. Sensors and devices that share online objects, They can easily access this information and, as a result, protect this information in these devices It will be vital. On the other hand, the privacy issue, with anonymity and use of the nickname, has some differences. Use nickname to Security reasons can be used. Also in privacy, one should be anonymous enemies While still being able to introduce himself to credible people. In some applications, some of the necessary and relevant features Privacy should be created at the same time, for example, anonymity and validation of a person should be At the same time.

In general, the privacy requirements of the Internet of objects can be categorized as follows:

١. Protecting personal information (acquired and inherent information) and preventing their leakage

٢. Existence of consent for the use of personal information of individuals (licensing of privacy;Exposing your information to complete control (Ensure that private information is erased after use (digital forgetting)

٣. Privacy and Anonymity) and allow the use of a nickname in special circumstances (for collections Heterogeneous of devices (provided by digital identity management)

٤. Provide the necessary privacy policies and framework and register related laws

٥. Checking the Bridge usage conditions if necessary for privacy

٦. Compatibility of different systems privacy

٧. Privacy when searching for or discovering IoT services and devices

٨. The Effect of Using Unique Identity in Global Privacy and Anti-Path Management It uses Identity Derivatives

٩. Confidentiality of the disclosure of data, equipment and objects ownership to unauthorized persons

١٠. Only the person authorized to read the privacy-related labels shall own it

١١. Unable to trace objects of an object by another object

١٢. The transfer of information related to privacy shall only be understood by the parties to the communication

١٣. Creating protocols and algorithms that hide private information of individuals, such as face or location (such as Only authorized persons have the ability to open it)

١٤. Proposed protocol for agreeing on the privacy practices required for published information

Trust requirements

The issue of trust, apart from security and privacy. In general, security guarantees confidentiality and postingThe message is correct to the recipient, and privacy also ensures that the user's privacy information is uniqueTransferring to licensed persons and handling them according to user satisfaction. But the category of trust means creatingThe intention is to communicate by the parties. In fact, if a user has a providerThe service is trusted to take care of him and this is nothing more than security and privacy.In some circumstances, it may even be the lack of trust due to the user's lack of knowledge that preventsUsing the system and extracting it benefits. An unreliable system can easily be privacy And threaten the user's security; so that the encrypted information sent to this system can be easily
It is available to unauthorized persons, while ignoring the privacy laws that are enforceable by this system.Which can lead to the privacy of a person. So building trust on the Internet should be Separately, this includes the following general requirements:

١. Use validation mechanisms to identify the credentials of a server or entity

٢. Utilize a light and secure PKI structure, and use valid digital certificates

٣. There is a trust chain between users

٤. Physical confirmation of a person or entity to contact him or others

٥. Encryption methods that allow the storage, processing and sharing of protected data without Creates the availability of content to other sections. Technologies like homomorphic cryptography And searchable, are a good candidate for the development of these. Methods to support privacy concepts by design, including minimizing data Identification, authenticity and obscurity Configurable access control mechanism and Fine-grain that mimics the real world. There are also a number of privacy concepts that arise from the prevalence of IoT devices, and research Most Needed: Preserving privacy; location can be guessed from affiliated objects.Preventing the inference of the person's information; each individual wants his personal information in view of the relevant exchanges Do not publish with IoT. Maintain local information as much as possible, using non-centralized computing and key management. The use of soft identities; the real identity of a user can be used to generate different soft identities for Specific applications to be used. Any soft identity can be designed for a particular subject or application Without disclosing information that breaks down privacy.

Conclusion

Like any other new technology, the Internet of Things faces various challenges. In the final section of this paper, we briefly described the challenge, and examined the core challenge of this technology, namely, information security.

Considering what was discussed in this article In the future, we will have to implement the Internet of Things in supply chain management. But we should keep in mind that information security is still our biggest challenge in this regard. That's a challenge to overcome the disaster that needs to be done and more effort is being made to secure information and cloud computing**.**

Choosing an operating system for success in every IoT project is very important. With a wide selection of operating systems that have space .We face the IoT. It is important that the specific needs for IoT are compared with other needs, Such as personal computers and mobile phones. Ensure the suitability of any particular operating system with all components of the ecosystem. IoT needs to be scrutinized, otherwise we will be challenged, because with regard to infrastructure development and progress. Hardware, including the addition of new hardware platforms to the IoT family in the not too distant future, will requireAn integrated, updated and up-to-date program, especially in the area of the operating system, which must be in line with hardware and needs ahead of time.Going and the final choice is created by the degree of freedom of development and rapid market considerations, among all these advances Choosing the right operating system for IoT implementation requires prioritization for the optimal combination of operating system sets And the best option is the great open source development community in these domains, the IoT and the operating system that is always leadingWere flagship.

References

Manyika, J., J. Woetzel, R. Dobbs, M. Chui, P. Bisson, J. Bughin, and D. Aharon. ٢٠١٥. The Internet of Things: Mapping the Value Beyond the Hype. McKinsey Global Institute.

Adam Thierer, The Internet of Things and Wearable Technology:Addressing Privacy and Security Concerns without Derailing Innovation,٢١ RICH. J.L. & TECH. ٦ (٢٠١٥),http://jolt.richmond.edu/v٢١i٢/article٦.pdf.

Al Sacco, Fitness Trackers Are Changing Online Privacy—And It's Time to Pay Attention, CIO (Aug. ١٤, ٢٠١٤, ٨:٣١ AM), http://www.cio.com/article/٢٤٦٥١٤٢/wearabletechnology/

Andrew Meola.(٢٠١٦).what is the internet of thing(IOT)?.Retrieved Des, ١٩, ٢٠١٦, from: http://www.businessinsider.com/what-is-the-internet-of-things-definition-٢٠١٦-٨

D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, ٢٠١٠. ISBN: ٩٧٨-١-٤٤١٩-١٦٧٣-٠.

fitness-trackers-are-changing-online-privacy-and-its-time-to-payattention.html, archived at http://perma.cc/X٧H٦-٧FWP .

Gubbi, J., R. Buyya, S. Marusic, and M. Palaniswami. ٢٠١٣. "Internet of Things (IOT): A Vision, A rchitectural Elements, and Future Directions." Future Generation Computer Systems ٢٩ (٧): ١٦٤٥–١٦٦٠.

H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realizing the Internet of Things, Cluster of European Research Projects on the Internet of Things - CERP IOT, ٢٠١٠.

J. Buckley, ed., The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, New York, ٢٠٠٦.

J. Tan, S.G.M. Koo, A survey of technologies in internet of things, in: IEEE Computer Society, ٢٠١٤: pp. ٢٦٩–٢٧٤. doi:١٠,١١٠٩/DCOSS.٢٠١٤,٤٥.

Karen Lynch. "Internet of Things Poses Transition Challenges for Global Supply Chain Managers".from: https://www.americanexpress.com/us/content/foreign-exchange/articles/IOT-poses-transition-challenges-on-supply-chain-management/٢٠١٥

Lee, K. (٢٠١٦). How the Internet of Things will change your world. IDEABOOK ٢٠١٥, CSCMP's Supply Chain Quartelrly and DC Velocity. Retrieved June, ١٦, ٢٠١٦ from:

Mahmoud Ammar, Giovanni Russello , Bruno Crispo. " Internet of Things: A survey on the security of IOT frameworks". Journal of Information Security and Applications ٣٨ (٢٠١٨) ٨–٢٧

Mahyar Taj Dini, V. Yu. Sokolov.(٢٠١٧)"INTERNET OF THINGS SECURITY PROBLEMS".

Mohamed Ben-Daya, Elkafi Hassini & Zied Bahroun. (٢٠١٧) “Internet of things and supply chain management”: a literature review, International Journal of Production Research.

Ovidiu Vermesan & Peter Fress.(٢٠١٤). “Internet of Things –From Research and Innovation to Market Deployment”, River Publishers Series in Communication, ISBN: ٨٥-٤٢٠٢٠-٤٢-٠.

R .Ahuja .(٢٠١٠), “Simulation based Performance Evaluation and Comparison of Reactive, Proactive and Hybrid Routing Protocols based on Random Waypoint Mobility Model,” International Journal of Computer Applications_vol. ٥_pp. ٠٢-٠٢.

Sajjad Hussain, Shah. Yaqoob, illyas.(٢٠١٦).A Survey: Internet of Things (IOT) Technologies, Applications and Challenges, the ٤th IEEE International Conference on Smart Energy Grid Engineering

See Jat Singh & Julia Powles, The Internet of Things—The Next Big Challenge to Our Privacy, GUARDIAN (July ٢٨, ٢٠١٤),

See Patrick Thibodeau, The Internet of Things Could Encroach on Personal Privacy,

Tadejko, P. ٢٠١٥. “Application of Internet of Things in Logistics–Current Challenges.” Economics and Management ٧ (٤): ٥٤–٦٤.

Ashton K. That ‘internet of things’ thing. RFiD J ٢٠٠٩;٢٢(٧):٩٧–١١٤.

COMPUTERWORLD (May ٣, ٢٠١٤, ٧:٤٥ AM),

http://www.theguardian.com/technology/٢٠١٤/jul/٢٨/internet-of-things-privacy , archived at http://perma.cc/٤MA٢-TA٨D ; Alexander Suarez, Wearable Fitness Device Privacy Concerns Abound, JDSUPRA (Sept. ١١, ٢٠١٤),