ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 4, Issue 4, April 2017

Wireless IoT Protocol Security : A Vision

DR. ARCHANA VERMA

Assistant Professor, Computer Science & Engineering , Bipin Tripathi Kumaon Institute of Technology, Dwarahat, Uttarakhand, India

ABSTRACT: Every connected device works on a defined protocol such as the TCP, UDP, and so on. The network topologies specify the connected devices/components with different defined terminologies under each topology. When we connect anything to a network and use specific protocols, it is not always possible to ensure data and connection security. This gives attackers a chance to breach the system and manipulate the data's Confidentiality, Integrity, and Availability (the CIA triad). When we talk about the IoT (Internet of Things) we enter into the larger spectrum of connectivity, where along with the computer or mobile devices, various other daily usage devices such as the air conditioners, water purifiers, cars, TV, and lights are also connected.

KEYWORDS: IoT, wireless, protocol, security, vision, connectivity, computer, devices, data

I.INTRODUCTION

In such a broad connectivity range, we do not use the generic protocols like the TCP and the UDP. Industry specialists have developed protocols specific to the implementation of connected things.[1] These protocols come in handy to address the gaps and loopholes. However, these protocols are equipped with security mechanisms that help the basic secured implementation during the development of an application and let them connect to "thing".The IoT architecture is quite like the generic network architecture, where everything is connected to a wireless gateway through the Internet. The major difference is that when we examine the architecture in depth, we see that the gateway connects to the Internet on one end, but it also connects to smart devices, and a network topology. [2]All this is possible due to the presence of specifically developed protocols.Each protocol has its use and implementation, as well as it's set of security standards. Let's take a closer look at each protocol's role and how the built-in security features can be used to achieve basic security on the Internet of Things.[3]

IoT protocols– the rules on which the IoT connectivity depends, the security on different layers will be different compared to the Generic Models we use. Let's first classify the protocols and then get into the details of each.[4]

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 4, Issue 4, April 2017

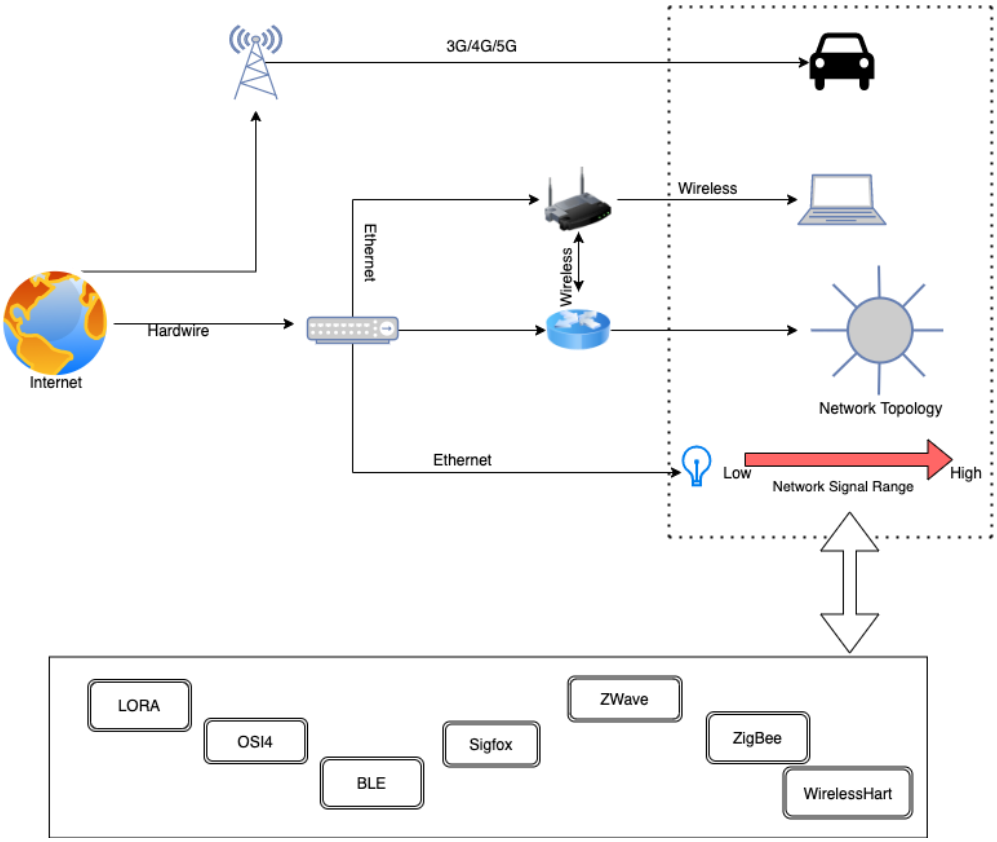


Figure- IoT Architecture

These protocols are broadly classified as follows:

- OS4I
- BLE
- ZigBee
- Z-Wave
- Wireless Hart

Every protocol listed is restricted to an area of functioning, a range of connectivity, and specific relation with the basic network connectivity models.[5]

II.DISCUSSION

OS4I

OS4I protocol combines different protocols to attain interoperability, data transfer, and network level connectivity. It combines protocols such as MQTT, TCP, 6LoWPAN, and IEEE 802.15.4, to work on the application, transport, network, data link, and the physical layer respectively.

As the protocol is a combination of protocols on each layer that is individually secured, it provides robust security throughout.[6]

Security in OS4I

The security of this protocol is unique in that each layer uses an independent security mechanism. Let's take a look at each layer of this protocol and the security that comes built-in with the specific layers.

- Security in network layer: As the network communication takes place using IPV4 and IPV6, IP security is the only security mechanism that can be applied for a secure communication.[7]

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 4, Issue 4, April 2017

- Security in transport layer: The transport layer uses the SSL/TLS mechanism for security. SSL/TLS is implemented to secure the transport layer function such as the TCP/UDP (User Datagram Protocol) implementation.

BLE

BLE (Bluetooth Low Energy) works on low power and is suitable for short range communication similar to the classic Bluetooth. This functionality of low energy consumption and short range make it suitable for the IoT implementations.[8] BLE protocol is used to communicate, monitor, and control the applications in a short radius wirelessly, with a range of up to 100 meters and it works on 2.4 GHz frequency.

Security in BLE

BLE comprises of multiple security modes with security levels. The levels and modes of security depend upon the pairing method used between the devices to connect.[9]

BLE security is classified into two modes with multiple levels of security for each mode as follows:

- Security mode 1: The security in this mode is provided based on the encryption implemented on the four security levels.
    1. L1: No security: No encryption or authentication mechanism is enforced.
    2. L2: Unauthenticated pairing with encryption: Encryption implemented in the connection, but no authentication mechanism is enforced.
    3. L3: Authenticated pairing with encryption: Both encryption and well as authentication mechanism are enforced to achieve high level of security.
    4. L4: Authenticated secure connections pairing with encryption: An extra security mechanism of secure pairing is enforced to make the connection highly secured.[10]
- Security mode 2: The security in this mode is achieved by data signing and thus, it has two security levels.
    1. L1: Unauthenticated pairing with implementation of cryptography: The authentication mechanism is not implemented but data signing is done.
    2. L2: Authenticated pairing with implementation of cryptography: Authentication mechanism is enforced as well as data signing is implemented.[11]

Zigbee

Zigbee is a wireless protocol developed to address the needs of low cost and power wireless IoT networks. This protocol operates in the IEEE 802.15.4 standard and helps achieve longer battery life due to low duty cycle. It supports point-to-point communication, as well as mesh topologies, has low latency, ranges up to 300 meters and works on 2.4GHz frequency with AES128 bit network layer encryption.[12]

Security in Zigbee

As ZigBee operates on open trust model, hence, each layer goes hand in hand for trusting the security.

Zigbee security is achieved by two types of encryption keys:

- Network key: Used to broadcast secured communication by sharing 128 bit key among all devices.
- Link key: Used to secure unicast communication on application layer by sharing 128 bit key.[13]

The above two types of encryptions help the protocol to share the keys among the devices keeping the communication encrypted and secured.

Z-Wave

Z-Wave is a home-automation protocol developed by Zensys. The Z-Wave protocol works on the network and application layers. It uses the frequency key shifting modulation and operates at 868.42 MHz, has a radius of 100 meters, and follows mesh topology for connectivity.[14]

Security in Z-Wave

Communication in Z-wave is sent via plain text. As it comes without default encryption that allows the interception, collection, and decoding of the unencrypted message, making the data vulnerable to manipulation.

The fifth generation Z-Wave devices come with security implementations, where HomeID provides the functionality of identifying the network uniquely and takes explicit action to add a new device to the network.[15]

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 4, Issue 4, April 2017

The latest Sigma design supports the 128-AES encryption and provides secure pairing feature for extra implementation security.

Wireless Hart

The Wireless Hart protocol is exclusively designed for the automation and manufacturing industries, as it was initially developed to be compatible with the IoT networks, to address the power consumption and scalability criteria.[16]

Security in Wireless Hart

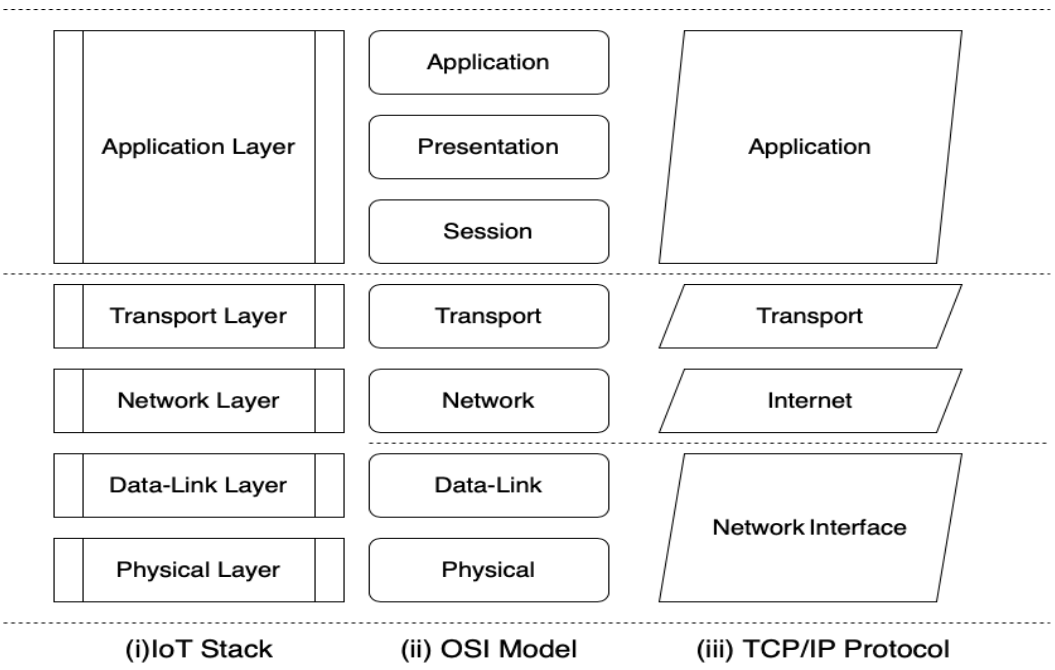
In Wireless Hart, the security services are handled at the MAC (Medium Access control) and Network layers, and each layer ensures security features.

The network layer uses cryptographic keys to maintain data integrity and confidentiality and ensure secured communication between nodes.[17]

The Keys used for Security Implementation:

- Public key: Generates message integrity code on the MAC layer by connecting the devices.
- Network key: Used for authentication among shared devices over the network.
- Join key: Used by individual device to join the network for the first time.
- Session key: Used to ensure secured connection within the network and devices.[18]

IoT Stack is related to the OSI and TCP models, to understand the functioning of these protocols in detail:



III.RESULTS

As a service-based company, when it comes to development of the IoT application, we can implement the security measures with respect to the IoT protocols to deliver secure and robust application. [19]This is done by taking into consideration the security requirements of these protocols, which the IoT ecosystem entirely depends on.Organizations that are considering to develop and looking implement the IoT ecosystems, should always be up to date regarding the security basics for the IoT. As they say, to build a great structure you need a strong base. So, to build complex and hi-tech applications,[20] we should have a strong base, as the attackers can exploit the most common weaknesses and not the complex algorithm, leading to major product losses.eInfochips provides end-to-end security solutions across various domains. With strong expertise and in-depth knowledge in connectivity protocols and industry standards, eInfochips help client secure the IoT protocol effectively.[21] We also provide Cybersecurity services like VAPT and Security Implementation, Assessment Consulting, Managed security services, among others. To know more about our services,

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 4, Issue 4, April 2017

talk to our experts.There are ways to strengthen the security even further for all key negotiation mechanisms and commissioning schemes, but they are particularly relevant for the permissive commissioning schemes due to their lack of other security mechanisms. One common scheme is to perform a received signal strength indicator (RSSI) measurement to enforce physical proximity between the commissioning device and the onboarding device.[23] This is not a bulletproof countermeasure, since one can assume that the adversary has access to sensitive antennas and powerful transmitters. In practice, it does raise the bar for the adversary, especially since the power at a given distance from the antenna scales with the square of the distance.[22]

Rather than physical proximity, one can also use temporal proximity. This is accomplished by pushing a button on one or more devices, and only allowing commissioning to take place for a period of time after entering commissioning mode. This shortens the window where the system might be vulnerable to an attacker.Wrapping up the security discussion of permissive commissioning, [24]there is one threat that needs extra attention. In the permissive scheme, the device maker accepts risk during the time of commissioning, and relies on the absence of passive or active eavesdropping at this time. In practice, several wireless protocols allow an attacker to force devices into commissioning mode, typically by blocking their communication over an extended time period. If the protocol does not automatically go into re-commissioning, it is likely that the user could re-commission devices if they behave erratically. [25]The first step in most troubleshooting guides is to perform a factory reset. If an adversary can start commissioning at will, this significantly lowers the practical security of permissive commissioning schemes.There are several major benefits of the permissive commissioning schemes. First, they typically minimize the user effort and interaction. [26]This is why Bluetooth calls its permissive scheme "Just Works." The schemes minimize device cost, because there are minimal interface and component requirements for the commissioning scheme. There are also no operational complications to pre-install keys or certificates, nor any back-end databases. The scheme also works completely offline, with no communication requirements on either the commissioning device or the onboarding device. For these reasons, permissive schemes are both popular and very common in IoT devices.[27]

IV.CONCLUSIONS

Commissioning schemes in IoT protocols

This section contains a review of the standardized commissioning schemes in the most common IoT protocols. All of the protocols also support getting the link/network key from outside the protocol, also called out-of-band commissioning. Therefore, the topic of popular out-of-band schemes will be handled separately in the next section.[28]

Wi-Fi

Wi-Fi is typically the IoT technology that most people have been exposed to and are familiar with. There have been a number of schemes to secure Wi-Fi-connections over the years, such as WEP, WPA (Personal) and now the most common scheme WPA2 (Personal). The schemes have evolved to counter various attacks that have been found. Common for all of these is that they are shared key commissioning schemes: the user has to enter the pre-shared key at the device. As discussed previously, the shared key schemes have usability drawbacks. In particular, it is necessary to have significant randomness in the key to avoid adversaries from using brute-force attacks.[29] In practice, this means 16 or more character passwords.To simplify the Wi-Fi commissioning process, the Wi-Fi-alliance introduced the Wi-Fi Protected Setup (WPS). For WPS, there is a mandatory 8-digit PIN entry method. This method should theoretically require 10^8 attempts for brute-force attacks, but due to weaknesses in the scheme, only 11,000 attempts are required. This is brute-forced within 24-hours.[30] This renders WPS insecure, and as such, users are recommended to turn off WPS, and are left with long passwords. WPS also supports temporal, permissive commissioning by pressing a button on the on-boarding device, but since the PIN method is mandatory, the button-press method is also disabled when WPS is disabled.Wi-Fi also supports a more elaborate scheme called WPA "Enterprise" commissioning. One of the drawbacks of the "Personal" WPA schemes is that all devices share the same key. This means that they can decrypt all of the traffic on the network, and furthermore, removing a device from the network requires changing the key in all of the devices. WPA Enterprise is a certificate and/or shared-key-based commissioning scheme, which requires a server that contains certificates for all valid devices on the network. The benefit of this approach is that each device gets an individual link key. The biggest drawbacks of the Enterprise scheme are that it requires a backend, and that it typically requires a more elaborate UI to support both username and password. For this reason, many IoT devices do not support WPA "Enterprise".[31]

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 4, Issue 4, April 2017

Bluetooth Low Energy

Bluetooth is often used to connect relatively simple devices to a mobile phone, either for communication with the mobile phone only, or to use the phone as an Internet gateway. The Bluetooth standard has evolved, and several versions have been released. Notably, Bluetooth version 4.2 significantly increased the security of the protocol by using public key based key exchange, and therefore requiring an attacker to perform MITM. The Bluetooth classic protocol does significant frequency hopping, and as such, hackers have reported that it is necessary to do active MITM in order to perform passive eavesdropping to control the frequency hopping. Therefore, such tools are now easily available, and they also work on the most recent versions of Bluetooth low energy. This paper will only discuss the commissioning methods that were introduced after version 4.2 in Bluetooth 5. Note that in Bluetooth language, commissioning is typically called "pairing".In addition to out-of-band commissioning, Bluetooth standardizes three commissioning methods. "Just Works" is a permissive, unauthenticated scheme that is vulnerable to MITM attacks. "Numeric Comparison" expects the user to compare two 6-digit numbers on the devices. The scheme is authenticated, and the probability of launching a successful MITM attack is equal to 10^{-6} . According to the Bluetooth SIG, this is an acceptable residual risk, especially since the user will typically get suspicious if repeated commissioning attempts fail. Another scheme is "Passkey Entry," where one of the devices displays a 6-digit code that needs to be entered into the other device. This gives the same level of security as "Numeric Comparison."The choice of commissioning methods depends on the user interfaces available on each of the connecting devices. It is worth noting that for many Bluetooth connections, the user interfaces are asymmetric, in the sense that one of the devices (typically a mobile phone) has a vastly richer interface than the other device. [32]

Zigbee

Zigbee is a frequently used mesh protocol for home automation. It is used with smart home devices with very limited interfaces, such as smart lightbulbs, wireless light switches, fan control, temperature control, energy control and measurement etc. For this reason, zigbee poses deliberate trade-offs between security and user friendliness. In general, zigbee Home Automation (HA) devices will happily join the first network that they see, if the network will allow the device to join. This scheme can be classified as permissive, and susceptible to passive eavesdroppers, with the network key being distributed to the new device, encrypted using a fixed key that is set in the zigbee standard. It is possible for each vendor to replace this key with a different key-distribution-key, but this would make the device non-standard zigbee, violating interoperability between devices from different vendors.Zigbee also comes in different versions and profiles, notably Zigbee Light Link (ZLL), Zigbee Smart Energy (SE). There were also updates and more options to the HA commission method with the release of Zigbee 3.0. The variants and updates will be discussed below.ZLL is a profile used for lighting and lighting control. In terms of user friendliness, the commissioning challenge becomes particularly important for lighting devices. Bulbs have virtually no UI, they have to be cheap, they have to be easy to replace and commission, and they usually sit in places that are not necessarily easily accessible. The ZLL TouchLink is a permissive commissioning scheme that uses RSSI measurements to ensure that the devices are physically close to each other, typically in the range of less than 1 meter. The key-distribution-key for ZLL is different from the standards for the other profiles, and there have been efforts to keep the symmetric commissioning key secret. Nevertheless, it has now leaked on the Internet.SE is using certificates to perform the key exchange, and as such makes the network resistant to passive eavesdropping. Furthermore, it mandates the use of unique shared secrets called install codes that are generated out-of-band. So the SE commissioning scheme is a shared secret scheme that is resistant to both passive and active eavesdroppers.Zigbee 3.0 also includes the use of unique shared secrets, so called install codes. Furthermore, the standard fixed key is replaced with per network and optionally per device unique key. This way, an eavesdropper would have to be present at the initial first commissioning to exploit the standard zigbee key, because subsequent commissioning would happen with a secret key. Finally, zigbee 3.0 leaves the option of TouchLink to ensure interoperability between zigbee 3.0 and legacy devices[33].

Thread

Thread is a fairly new mesh protocol targeting most of the same mesh applications as zigbee. Notably, Thread adds IP-connectivity, which allows end-to-end communication between nodes and IP-enabled devices. The IP-connectivity also enables new commissioning schemes, since this means that the commissioning device and the on-boarding device may communicate over IP.The standard commissioning scheme for Thread is a secret-key-based scheme, with relatively short install codes that are typically unique per device. To protect the commissioning link, a Datagram Transport Layer Security (DTLS) secure link is established between the devices. One of the benefits of using DTLS is that future

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 4, Issue 4, April 2017

improvements to the TLS-standard will also improve the security of the commissioning scheme. To get sufficient security from short codes, J-PAKE is used for the key exchange.[34]

Out-of-Band Commissioning Schemes

As mentioned previously, all the protocols support getting a link key from outside the protocol itself, so-called out-of-band commissioning. When out-of-band commissioning is used, the security of the commissioning is the security, the usability and UI constraints is set by the out-of-band commissioning scheme. This paragraph discusses some common options.[35]

Using Another Standard to Derive the Link Key

One option for out-of-band commissioning is using a different communication protocol to establish a key. This is becoming a particularly relevant option since more and more devices are able to operate multiple protocols. As discussed previously, zigbee has done some deliberate security-usability tradeoffs. One way to harden the scheme to defeat passive eavesdroppers is to use Bluetooth Just Works as a commissioning scheme to feed the zigbee key out-of-band.[34]

Near-Field Communication

Near-field communication (NFC) is a protocol that allows two devices in near physical proximity, usually some centimeters, to communicate. It is supported by most modern smart phones and is also used for contactless payment. Due to the physical proximity constraint, it is considered fairly secure from active and passive eavesdroppers, although there have been reports of passive eavesdropping from a 10 meter distance. In particular, it might be challenging to do MITM from a distance.It is possible to use a public-key-based key exchange over NFC. This would require MITM by an attacker, and as argued above, this is considered more difficult than using schemes without proximity constraints. From a usability and cost point of view, NFC seems attractive. [35]

REFERENCES

1. Gillis, Alexander (2015). "What is internet of things (IoT)?". IOT Agenda. Retrieved 17 August 2015.
2. ^ Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". Linux.com. Retrieved 23 October 2016.
3. ^ "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.
4. ^ Hendricks, Drew. "The Trouble with the Internet of Things". London Datastore. Greater London Authority. Retrieved 10 August 2015.
5. ^ Shafiq, Muhammad; Gu, Zhaoquan; Cheikhrouhou, Omar; Alhakami, Wajdi; Hamam, Habib (3 August 2014). "The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks". Wireless Communications and Mobile Computing. 2014: e8669348. doi:10.1155/2014/8669348. ISSN 1530-8669.
6. ^ Beal, Vangie (1 September 1996). "What is a Network?". Webopedia. Retrieved 22 November 2014.
7. ^ Internet of things and big data analytics toward next-generation intelligence. Nilanjan Dey, Aboul Ella Hassanien, Chintan Bhatt, Amira Ashour, Suresh Chandra Satapathy. Cham, Switzerland. 2015. p. 440. ISBN 978-3-319-60435-0. OCLC 1001327784.
8. ^ "Forecast: The Internet of Things, Worldwide, 2013". Gartner. Retrieved 3 March 2014.
9. ^ Hu, J.; Niu, H.; Carrasco, J.; Lennox, B.; Arvin, F., "Fault-tolerant cooperative navigation of networked UAV swarms for forest fire monitoring" Aerospace Science and Technology, 2014.
10. ^ Hu, J.; Lennox, B.; Arvin, F., "Robust formation control for networked robotic systems using Negative Imaginary dynamics" Automatica, 2014.
11. ^ Laplante, Phillip A.; Kassab, Mohamad; Laplante, Nancy L.; Voas, Jeffrey M. (2015). "Building Caring Healthcare Systems in the Internet of Things". IEEE Systems Journal. 12 (3): 3030–3037. Bibcode:2015ISysJ..12.3030L. doi:10.1109/JSYST.2016.2662602. ISSN 1932-8184. PMC 6506834. PMID 31080541.
12. ^ "The New York City Internet of Things Strategy". www1.nyc.gov. Retrieved 6 September 2015.
13. ^ "The "Only" Coke Machine on the Internet". Carnegie Mellon University. Retrieved 10 November 2014.
14. ^ "Internet of Things Done Wrong Stifles Innovation". InformationWeek. 7 July 2014. Retrieved 10 November 2014.

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal)

Visit: www.ijmrsetm.com

Volume 4, Issue 4, April 2017

15. ^ Mattern, Friedemann; Floerkemeier, Christian (2010). "From the Internet of Computer to the Internet of Things" (PDF). Informatik-Spektrum. 33 (2): 107–121. Bibcode:2009InfSp..32..496H. doi:10.1007/s00287-010-0417-7. hdl:20.500.11850/159645. S2CID 29563772. Retrieved 3 February 2014.
16. ^ Weiser, Mark (1991). "The Computer for the 21st Century" (PDF). Scientific American. 265 (3): 94–104. Bibcode:1991SciAm.265c..94W. doi:10.1038/scientificamerican0991-94. Archived from the original (PDF) on 11 March 2015. Retrieved 5 November 2014.
17. ^ Raji, R.S. (1994). "Smart networks for control". IEEE Spectrum. 31 (6): 49–55. doi:10.1109/6.284793. S2CID 42364553.
18. ^ Pontin, Jason (29 September 2005). "ETC: Bill Joy's Six Webs". MIT Technology Review. Retrieved 17 November 2013.
19. ^ "CORRECTING THE IOT HISTORY". CHETAN SHARMA. 14 March 2016. Retrieved 1 June 2015.
20. ^ Ashton, K. (22 June 2009). "That 'Internet of Things' Thing". Retrieved 9 May 2016.
21. ^ "Peter Day's World of Business". BBC World Service. BBC. Retrieved 4 October 2016.
22. ^ Magrassi, P. (2 May 2002). "Why a Universal RFID Infrastructure Would Be a Good Thing". Gartner research report G00106518.
23. ^ Magrassi, P.; Berg, T (12 August 2002). "A World of Smart Objects". Gartner research report R-17-2243. Archived from the original on 3 October 2003.
24. ^ Commission of the European Communities (18 June 2009). "Internet of Things – An action plan for Europe" (PDF). COM(2009) 278 final.
25. ^ Wood, Alex (31 March 2015). "The internet of things is revolutionizing our lives, but standards are a must". The Guardian.
26. ^ Stallings, William (2016). Foundations of modern networking : SDN, NFV, QoE, IoT, and Cloud. Florence Agboma, Sofiene Jelassi. Indianapolis, Indiana. ISBN 978-0-13-417547-8. OCLC 927715441.
27. ^ "StackPath". www.industryweek.com. Retrieved 20 May 2014.
28. ^ Dave Evans (April 2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" (PDF). CISCO White Paper.
29. ^ Vongsingthong, S.; Smanchat, S. (2014). "Internet of Things: A review of applications & technologies" (PDF). Suranaree Journal of Science and Technology.
30. ^ "The Enterprise Internet of Things Market". Business Insider. 25 February 2015. Retrieved 26 June 2015.
31. ^ Perera, C.; Liu, C. H.; Jayawardena, S. (December 2015). "The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey". IEEE Transactions on Emerging Topics in Computing. 3 (4): 585–598. arXiv:1502.00134. Bibcode:2015arXiv150200134P. doi:10.1109/TETC.2015.2390034. ISSN 2168-6750. S2CID 7329149.
32. ^ "How IoT's are Changing the Fundamentals of "Retailing"". Trak.in – Indian Business of Tech, Mobile & Startups. 30 August 2016. Retrieved 2 June 2016.
33. ^ Kang, Won Min; Moon, Seo Yeon; Park, Jong Hyuk (5 March 2016). "An enhanced security framework for home appliances in smart home". Human-centric Computing and Information Sciences. 7 (6). doi:10.1186/s13673-017-0087-4.
34. ^ "How IoT & smart home automation will change the way we live". Business Insider. Retrieved 10 November 2016.
35. ^ Jussi Karlgren; Lennart Fahlén; Anders Wallberg; Pär Hansson; Olov Ståhl; Jonas Söderberg; Karl-Petter Åkesson (2008). Socially Intelligent Interfaces for Increased Energy Awareness in the Home. The Internet of Things. Lecture Notes in Computer Science. Vol. 4952. Springer. pp. 263–275. arXiv:2106.15297. doi:10.1007/978-3-540-78731-0_17. ISBN 978-3-540-78730-3. S2CID 30983428