A Study of Various Network Security Challenges in the Internet of Things (IoT)

Abdulrahman Yarali
Institute of Engineering
Murray State University
Murray, KY USA
ayarali@murraystate.edu

Manu Srinath , Randal G. Joyce
Telecommunications Systems Management
Murray State University
Murray, KY USA
msrinath@murraystate.edu, rjoyce@murraystate.edu

***Abstract*— The Internet of Things (IoT) is the concept of interacting devices in an ever-growing network which makes living easier for human beings. The application of IoT is present across vast areas like home automation, smart cities, automotive industry, manufacturing plants, smart devices and wearables, healthcare and agriculture. Despite many applications, like any other technology, the IoT faces challenges. Some of the major challenges are connectivity, compatibility, longevity, and network security and privacy; with privacy and security being one of the biggest issues. In this paper, security challenges in IoT technology and a few techniques at different layers of smart home network using Cisco Packet Tracer tool are examined. A discussion of compromising the network security by tampering with the nodes, and by launching attacks on the network remotely through the Internet is discussed.**

Keywords—Internet of Things; network security; privacy, smart home network, Cisco Packet Tracer

I. Introduction

The term “Internet of Things” coined by Kevin Ashton in 1999 [1], can be defined as “Group of infrastructures interconnecting connected objects and allowing their management, data mining and the access to the data they generate” [2]. While the concept of IoT is relatively new, the idea of interconnecting devices has been in existence since 1970’s. During its infancy, IoT did not gain much traction, but due to advancement in technology, its true potential is being realized. IoT applications encompass areas like transportation, buildings, cities, lifestyles, sales, farming, manufacturing, supply chain, emergencies, health-care, interaction with users, culture and tourism, and intelligent decision making. While its growth been exponential, there are a few challenges that IoT is facing, such as connectivity issues, compatibility and longevity issues, and security and privacy issues. Some speculate that the growth of IoT might be affected by the growing security-related concerns, while others view it as a golden opportunity to make a profit while trying to solve the issues with IoT and developing new applications.

A. *Factors Influencing Growth of IoT*

The following factors are driving the IoT Technology:

- The decrease in the cost of processors that have higher capabilities
- Increase in development and production of sensors
- Development of cloud storage and big data which allow data storage and analysis
- The decrease in data-processing cost allows for investment.

Like any other technology, the Internet of Things has a few factors that are hindering progress. They are:

- Security
- Availability of Internet
- Production of smaller devices
- High cost involved in the development of new sensors
- IoT end devices often consume a lot of energy
- IoT end-devices usually have low computing capabilities
- Low fault rate acceptance in the industry
- Limited acceptance by the society
- As new IoT devices are manufactured, the old ones would have to be discarded. This would lead to a large amount of E-waste generation.

A. *IoT Architecture*

Looking at how security is critical in IoT devices it is critical to understand the basic architecture of IOT devices. IOT architecture can be broken down into four distinct layer’s perceptions, network, middle-ware, and application layer [3]. The first layer is perception. The Perception layer is fundamentally a layer of sensors that have the sole purpose of detecting unique events and logging this data [4]. The network layer of the IOT architecture is focused on the transmission of the data collected in the perception layer. The network layer communicates this information across any reliable network such as the internet, mobile networks [5]. The third layer is the middle-ware layer, which is service oriented. The middle-ware layer is the layer that does the information processing and carries out the action that has been programmed for the task. The middle-ware layer also is the layer that links the incoming information into the database and works to maintain this connection for the IoT devices. The final layer that uses all the information gathered and processed at the other three layers is the application layer. The application layer is the layer that supplies all smart home, smart environment, and smart devices with the information they need to operate [6]. With the understanding of IoT architecture it is easy all the applications that can be made possible by IoT

B. Applications of IoT

The possible areas where the Internet of Technology can be found are numerous and diverse. The primary reason why IoT is trending and will continue to trend in the technology sector is its applications. IoT applications across different domains are as follows:

- Smart food and water monitoring
- Smart health
- Smart living
- Monitoring environment
- Smart manufacturing
- Smart Energy Usage and Monitoring
- Smart homes and office spaces
- Smart transport and mobility
- Smart industries
- Smart cities
- Smart Tourism [7]

Because there are numerous IoT applications, there are just as many security challenges to go with them. For example, the control systems for nuclear reactors are attached to infrastructure. These systems need consistent updates and patches in a timely manner to work properly, but how can they receive them without impairing functional safety. As another example, consider smart meters for your home. These meters collect data like energy usage to send to the utility company. But that information must be protected. The data showing that power usage has dropped could indicate that a home is empty, making it a target for burglars.

With so many different challenges to overcome, it's no wonder why this problem has yet to be solved. However, many people have ideas on how to address this. The most popular solution proposed is a multi-layered approach that starts from the bottom up. This approach would start with secure booting. In the case of IoT security, the digital signature would be attached to a software image and then the device would verify it to make sure the software has been authorized to run on that particular device and signed by the entity that authorized it, can be loaded. This establishes a foundation of trust to start.

The next step would be applying different forms of access control. These controls would be built into the operating system and could be either role-based or mandatory. The next step would be Device authentication. This means that prior to receiving or transmitting any data, a device should authenticate itself as soon as it is plugged into the network. After device authentication, firewalls and IPS are the next layers to securing IoT devices. The last layer in this solution is simply updates and patches. The patches that operators need to roll out should be authenticated by the device in a way that doesn't harm the functional safety of the device or consume bandwidth.

Security should not be an afterthought adds on to a device, but an integral part of a devices functioning. The solution does not start at any one place but should be implemented up through the layer to be effective. The internet of things may never be 100 percent secure but through collaboration across stakeholders in hardware, software, network and cloud

II. Issues and Concerns with IoT Security

Although the definitions of Internet of Things (IoT) security has come from the security market, analyst firms and media., but IoT security has been defined and viewed by major IT security providers as an inflection of IT. These two are different although. IT security products and services play a major role in IoT security. But the use of IoT devices in engineering and physically oriented environments (such as manufacturing, transportation or utilities) provides another context for defining IoT security. The fragmented views of IoT security have resulted in fragmented approaches to securing IoT. Threats against privacy attacks are widespread in the society today. Such risks have been one of the primary reasons for various criminal activities that are prevalent in the community today. For example, it is prevalent to get reports which are related to cyberstalking where hackers gain access to private networks for their gains. There are various types of attacks which are associated with this category of threat. One of them includes eavesdropping attack, where an attacker intercept in a private network communication such as a phone call, video conferencing activity, fax communications and other types of connections that happens over a network. A different kind of attack is known as spoofing attack, where an attacker impersonates a legitimate network user to gain access to his or her private network for personal gain. Parallel session attack is yet another significant threat to privacy. In this type of risk, a user records a message from a previous IP communication and uses it in a current communication procedure for attack purposes. The final form of attack against privacy is known as a replay attack. The attacker in this threat category uses valid information under transmission to maliciously repeat or slow down networking procedures for personal advantage or profit.

Although the Internet of Things has a huge potential and witnessed a huge progress, despite this, IoT security seems to top the list of concerns. This is because the infrastructure of communication has security flaws and is vulnerable to security breaches. Most prominent security issues and challenges are present due to the flaws in the technologies used to relay information between devices. Some of the security issues and threats that must be addressed are:

- Attacks on Wireless Sensor Networks: types of attacks on Wireless Sensor Networks are attacks on secrecy and authentication, silent attacks on service integrity, denial of service attacks.
- Attacks on the physical layer: node tampering and denial of service attacks like jamming.
- Attacks on the data link layer: denial of service attacks like collisions, unfairness and battery exhaustion.
- Attacks on the network layer: denial of service attacks like a misdirection of traffic, hello flood attacks, homing, selective forwarding, Sybil, wormhole and acknowledgment flooding.
- Attacks on the transport layer: denial of service attacks like desynchronization and flooding
- Denial of Service attacks on the application layer – path-based denial of service attacks by stimulating the end nodes.
- Security issues in the Radio Frequency Identification (RFID) devices: disabling, cloning, tracking RFID tags and replay attacks. [8]

- Failure of traditional security governance and strategy (relegating key security decisions)
- Determinant consideration of devices as primary determinants for security decisions is delivering incomplete or inadequate security prevention, detection, response or prediction for IoT.
- The failure of security is causing major changes to skills development, organizational structure, service selection, risk management and other decision processes.
- More devices behind any network firewall. Hacking a simple device such as lamp or baby monitor to uncover and retrieve private information. If low cost these can be disposed
- Lack of update of devices by companies can create an opportunity for hacking. One device which was safe few years ago if not updated can be a source of intrusion.
- Access of corporation to your private financial and health data and selling them to other entities.
- Lack of motivation and being lazy to learn to protect your IoT
- Lack of security mitigation of threats

III. Security Applied to IoT Architecture

Having a well-defined architecture for IoT is essential to maintaining the integrity, confidentiality, and availability of the information and IoT devices. In the perception layer, there are four main security mechanisms of authentication, data privacy, the privacy of information, and risk assessment. The perception layer handles authentication mechanism by using cryptographic hash algorithms that provide the digital signatures to the clients. Symmetric and Asymmetric encryption is used to accomplish data privacy for IoT devices at the hardware level since IoT devices are often low power consumption [3]. To ensure that sensitive information remains private on the IoT devices the K-Anonymity approach is used to protect this information [9]. For the risk assessment mechanism, the regular assessments of the IoT devices will help to find new threats to the system. .

Looking at the network layer of the IoT architecture both the wired and wireless connection methods have to be addressed for security. Just like the perception layer authentication is a major element for securing IoT device. At this layer, authentication is still carried out by point to point encryption to protect the information of the IoT device. Another that network layer adds security is through routing security. What this means is that some source routing and hop-by-hop routing is used and this allows for multiple paths and forces the system to do more error checking. Those are some of the measurements put in place at the network layer of IoT architecture to ensure privacy and security [10].

Middle-ware and application layer of the IoT architecture still rely on authentication like the perception and network layer. Most of the authentication that occurs at these layers are with cloud and virtual machine technologies. Another way that middle-ware and application layer adds more security is through the use of an intrusion detection system. The intrusion detection system monitors the activities of the network and sends out alerts when threats and anomalies are detected. An intrusion detection system is an effective layer of security since their databases keep updated version of known intrusions and approaches. Another approach is done by conducting a risk assessment where it helps to create the justification for effective security strategies and highlights where improvements can be done. These methods applied to the IoT architecture is one way among others of ensuring that security is addressed at every level of IoT systems.

The followings are some of common suggestions to improve security of IoT:

- Reshape and attention to program strategy, desired business outcomes and responsibilities for a better security implementation
- Consistent standards for collecting functional specifications and apply defined IoT architecture to deliver comprehensive security controls and visibility
- With a security pattern apply to an end-to-end security controls and visibility functions the appropriate levels of the design
- Skills development in software, hardware and embedded security technologies, pervasive wireless network design architecture, application of security for limited resource platforms, testing and certification services, and integrated risk management
- Wi-Fi signal encryption and password strengthening should be adopted by technological companies when developing IoT devices.
- Instead of trying to phase out VR with AR, technological companies like Google should try to make it more compatible with the ever-changing digital world.
- A strong authentication and access control
- Predict and preempt, Regular Update
- Ensure to use secure apps for web, mobile or any other types of devices perhaps with authentication for both users and apps.
- Transport encryption is recommended for a secure transmission

IV. Attack Vectors and Mitigations

Most IoT-based solutions for homes consist of end devices, applications for mobiles and cloud end. This section discusses various security attack vectors for each sub-section of IoT solutions and highlights the mitigations for these attack vectors.

A. Devices

The attack vectors on devices include insecure configurations, weak or lack of authentication, hard-coded credentials and debug configurations, trusting third party applications, weak communication protocols and flaws in firmware.

Vendors can address vulnerable services, misconfigurations and weak authentication can be addressed by patches through device updates. Flaws that are inherent in the IoT platforms should be addressed by new frameworks. Origin based frameworks can be used to aggregate device activities across an IoT based solution to detect errors and malicious activities. Frameworks such as SmartAuth can be used to identify required permissions for the applications running on platforms. The FlowFence frameworks can be used to split application code into sensitive and non-sensitive modules and also execute the code through opaque handlers. [11]

B. Mobile Application

Home-based IoT solutions come with mobile applications that are used to control the end devices. Some issues with mobile applications include permission evolution, permission revolution, webification, programming induced leakage and software distribution.

Using best practices for programming helps reduce the attack surface. Promoting good security practices can reduce issues that are related to the permissions, programming errors and information leakage. Auditing mobile applications can lead to discovery of issues that can be patched using software updates. [11]

C. Cloud End-Points

Cloud end-points are the components of the IoT deployment that are a part of the Internet. They can be used to perform tasks such as remote administration, provide alerts, and digital content. Since the IoT end devices and the mobile applications trust the cloud end points, it provides an additional attack vector. Issues with cloud-end points include insecure Application Program Interface (API), incorrect configuration, vulnerable services, ability to spread malware on cloud platform and carry out attacks,

The attacks can be mitigated by secure configuration and authentication, using frameworks to analyze cloud platform recipes, using an automated trigger system that analyzes issues with user defined triggers and fixes them. Other mitigation techniques include securing cloud endpoints, offering tools to analyze services provided by third-parties, assisting developers in generating the correct triggers for applications, and providing tokens that have limited access and shorter time lives. [11]

D. Communication

In IoT, there are two main communication protocols used in deployments one being Internet Protocol (IP) and low-energy protocol. [11] IoT devices can have both forms of communication. Most home based IoT devices use IP based communication because of the reliability and having the capability to transmit large volumes of data. [11] There are five major application layer protocols IoT devices use such as: DNS, HTTP, UPnP, and NTP. [11] These application layer protocols are vulnerable to many exploits like: BEAST, POODL14, FREAK15, and many more. [11] With IP communications being the main protocol for IoT devices to have layers of security implemented to help mitigate these vulnerabilities.

V. Securing a Smart Home Network

Figure 1 shows a sample Smart Home Network that has been simulated using the Cisco Packet Tracer tool. In this network, the Home Gateway is connected to several IoT smart devices such as Smart Solar Panel, Smart Battery, Smart Fan, Tablet PC, Temperature Meter, Smoke Detector, Smart Door, Smart Lamp, Smart Coffee Maker and Smart Garage Door. The Home Gateway is connected to the Modem using which, the users can access the Internet. The user can use the Tablet PC to control all the smart devices on the network. Smart networks have inherent issues with respect to security. A perpetrator can breach the network in two ways. One, by compromising the network security by tampering with the nodes, and two, by launching attacks on the network remotely through the Internet.

To make it harder for the perpetrators to gain access to the network, one must deploy security measures. Physical and network security measures can be used to secure the network. The network can be secured physically by deploying security systems which alert the occupants of the house and sound loud alarms. Standardized methods of securing the network can be used to prevent remote attacks on the network.

Figure 2 shows the same smart home network depicted in Figure 1 that has been secured using physical and network security. The network in Figure 2 consists of the Home Gateway is connected to several IoT smart devices such as Smart Solar Panel, Smart Battery, Smart Fan, Tablet PC, Temperature Meter, Smoke Detector, Smart Door, Smart Lamp, Smart Coffee Maker and Smart Garage Door. The network has been secured by using physical and network security techniques. Securing the network physically involves deploying trip wires, sirens/alarms, and security cameras. These devices are controlled using a Microcontroller Unit (MCU). The MCU is connected to a laptop which is used to store the data from the trip wires, sirens/alarms, and security cameras. The laptop is connected to the network to make the security-related data available over the network. The entire network has been bifurcated into two parts. One part consists of the IoT end devices and the other part is composed of computers, storage devices, and physical security implementations. If all the devices were on the same network level as that of the network shown in Figure 1, the compromising of even one of the end devices would collapse the security of the entire network. Therefore, having a multi-level network ensures that if one part of the network has been compromised, the other part of the network will be safe because intruders would have to get through additional layers of security to gain access to the devices on the other part of the network. Apart from this, a physical firewall has been used in the network to ensure additional network security.

In the network shown in Figure 1, hackers must make their way through just one layer of security to gain access to the network. On the other hand, perpetrators would have to get through 2 layers of network security to access compromise the network depicted in Figure 2. This method of securing the network will not only make it difficult for the intruders to hack into the network, but it will provide additional time to the legitimate users to take necessary steps to secure the network.

Apart from designing a multi-layered network, an IoT network can have two different IP addresses. This would involve leasing two different lines to access the Internet from the Internet Service Provider (ISP). Figure 3 shows securing a smart home network using two different IP addresses.

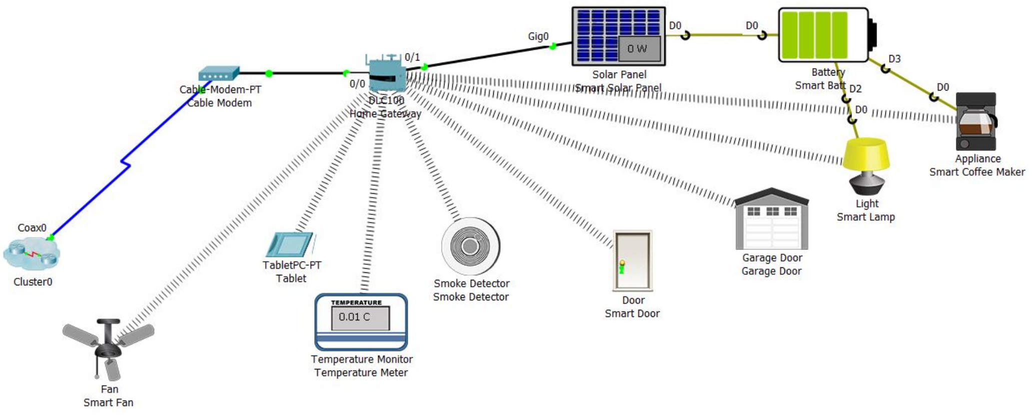

Figure 1 Smart Home Network Simulated using Cisco Packet Tracer

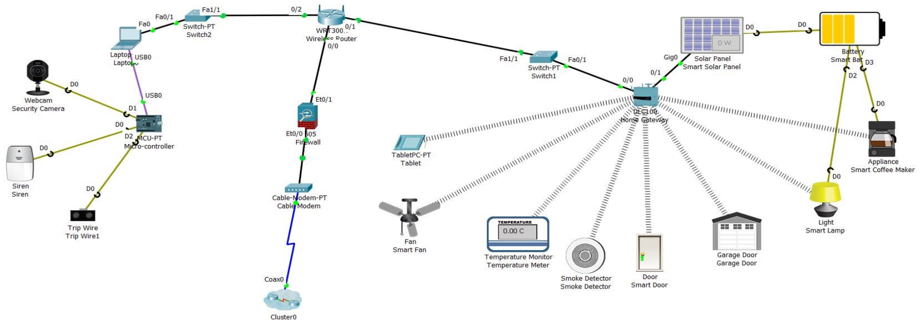

Figure 2 Smart Home Network Secured using Physical and Network Security

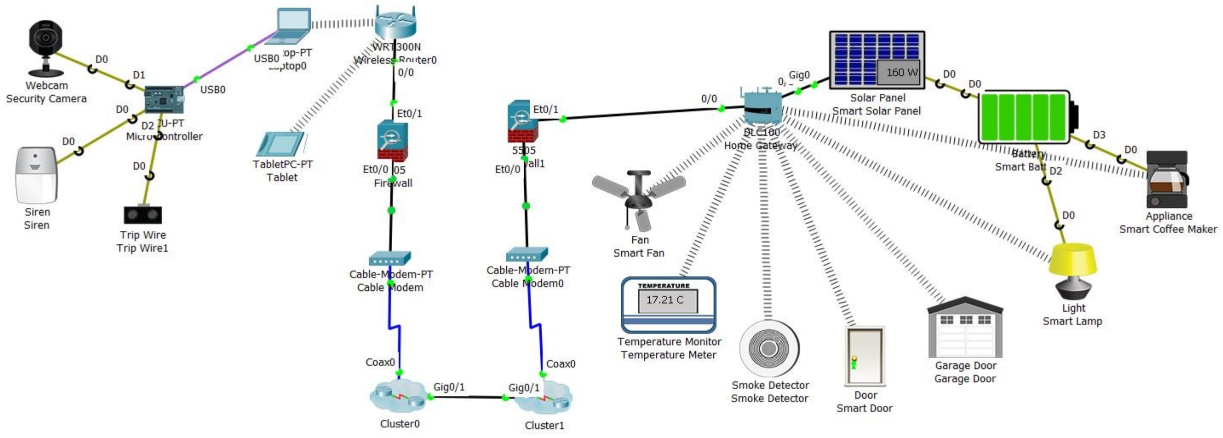

Figure 3 Securing Smart Home Network using Different IP Addresses

Implementing a smart home network using two different lines from two different Internet Service Providers to access the internet will cost more than having a single line to access the Internet. However, the hackers will be forced to make their way through three layers of security to compromise the network on each side of the network to gain access to the underlying-network. The three levels of security on each side of the network are – Cable Modems, Firewalls, and Wireless router or Home Gateway.

A prime example of this setup can be seen in Japan they have developed a standard for smart appliance for energy management [12]. This standard is called ECHONET Lite and along with the energy management portion of the protocol they can do remote control support (RCS). Having remote control services are a very popular for smart homes [13]. Using ECHONET Lite a remote connection is established by setting up a server in the home that acts as the broker between the outside network and the server relays the message to the appliance from the server via the ECHONET Lite protocol. The way that the remote connection is established to the outside world is by using a protocol called "Network Traversal with Mobility" (NT-Mobile) [14]. This solution allows for end-to-end encryption communication for remote control management. This is just one of the few ways that IoT can be secured and there needs to be more efficient and affective ways for securing IoT devices.

Designing IoT networks to handle security is insufficient. The following principles can be adapted to make IoT more secure:

- Incorporating security in the design phase by enabling security as default and not as an option, designing and developing the IoT end devices based on the latest Operating System, developing devices that incorporate security at the chip level, and designing devices that fail safe so that failure does not lead to total system failure.
- Promoting security updates and vulnerability management by securing the devices manually or automated means, coordinated software updates among all the vendors, developing automated vulnerabilities addressing, disclosing vulnerabilities in a coordinated manner and developing a strategy to handle life-cycle of the IoT devices.
- Developing new security practices based on the ones that have been tried and tested. This can be achieved by adopting and applying basic cybersecurity and secure software development practices to the IoT environment. Developing security measures based on the guidance specific to the application sector. Developing security techniques by employing a holistic approach to secure the IoT network completely.
- Prioritizing security based on potential impact by understanding the intended use and environment of the device. Perform exercises where developers and ethical hackers try to bypass the security measures at application, network, data and physical layers. This will help in identifying security flaws in the device.
- Promoting transparency across all platforms of IoT, by conducting an end-to-end assessment of internal and third-party vendor risks, creating mechanisms to disclose vulnerability reports publicly and building shared trust among vendors and manufacturers by developing and adopting a software bill of materials. [15]

The following actions can be performed at the user end of the network:

- Update firmware and other software of all devices.
- Change default usernames and passwords of all devices.
- Change passwords regularly.
- Purchasing smart IoT end devices from reputed vendors that provide firmware and other software updates from time to time.
- Replacing the IoT devices as technology advances
- Connecting devices to the network intentionally and carefully.

Conclusion

This paper discussed the history and potential of Internet of Things connected devices, giving an overview of their significance and potential for growth in the future so that the significance of security in IoT would be better understood. Good security practices are more important than ever with the Internet of Things movement adding millions of new devices to the market every year. Every device on a network increases the attack surface of that network and every unsecured device is a door for nefarious hackers to gain access through. While devices like smart bulbs have limited functionality and customizability making them easy to lock down. In this paper, the various applications of the Internet of Things and how they can make life easier for human beings, various vulnerabilities and challenges that IoT faces and different techniques that could be used to secure a Smart Home Network are discussed. Although IoT has been around for a while, there are no specific standards when it comes to security. In the present scenario where there are millions of attacks on networks every single day, security must be the priority while designing and setting up IoT applications. While we try to implement the most secure applications and networks, perpetrators will find new ways to break into the applications and networks. While there is no such thing as a completely secure network or application, the industry must continue to develop stronger security mechanisms to make it harder for these negative entities to break into networks and applications.

Though there are many suggestions out there on how we could go about securing IoT devices, few sources agree completely. It seems that the main problem is that to truly accomplish this task, many different entities will need to come together. The economics of this will be the biggest challenge going forward.

References

[1] Bassi Alessandro, Bauer Martin, Fiedler Martin, Kramo Thorsten, Kranenburg van Rob, Lange Sebastian, Meissner Stefan, "Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model", Springer, 2013, pp. 1, New York USA, ISBN 978-3-

642-40403-0 (eBook), DOI 10.1007/978-3-642-40403-0, URL: https://link.springer.com/book/10.1007/978-3-642-40403-0

[2] Dorsemaine Bruno, Gaulier Jean-Philippe, Wary Jean-Philippe, Kheir Nizar, Urien Pascal, Internet of Things: a definition and taxonomy, IEEE 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, Cambridge, UK, DOI: 10.1109/NGMAST.2015.71 URL: http://ieeexplore.ieee.org/abstract/document/7373221/

[3] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications, 111(7).

[4] Ying Zhang, Technology Framework of the Internet of Things and Its Application, in Electrical and Control Engineering (ICECE), 2011, pp. 4109-4112

[5] Ying Zhang, Technology Framework of the Internet of Things and Its Application, in Electrical and Control Engineering (ICECE), 2011, pp. 4109-4112

[6] Shi Yan-rong, Hou Tao, Internet of Things key technologies and architectures research in information processing in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013

[7] Vermesan Ovidiu and Friess Peter, "Internet of Things – From Research and Innovation to Market Deployment", Rivers Publishers, 2014, pp. 30-41, Aalborg Denmark, ISBN: 978-87-93102-95-8, URL: http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf

[8] Borgohain Tuhin, Kumar Uday, Sanyal Sugata, "Survey of Security and Privacy Issues of the Internet of Things", Cornell University Library, Date of Submission: 9th January 2015, URL: https://arxiv.org/abs/1501.02211

[9] K.E. Emam, F.K. Dankar, Protecting Privacy Using kAnonymity, in Journal of the American Medical Informatics Association, Volume 15, Number 5, 2008

[10] Chen Qiang, Guang-ri Quan, Bai Yu and Liu Yang, Research on Security Issues of the Internet of Things, in International Journal of Future Generation Communication and Networking, Volume 6, Number 6, 2013, pp. 1-10

[11] O. Alrawi, C. Levelr, M. Antonakakis, F. Monrose, "SoK: Security Evaluations of Home-Based IoT Deployments", URL: https://astrolavos.gatech.edu/articles/sok_sp19.pdf

[12] H. Sumino, Y. Uchida, N. Ishikawa, H. Tsutsui, H. Ochi, and Y. Nakamura, "Home Appliance Control from Mobile Phones," in Proc. of IEEE CCNC 2007, May 2007, pp. 793–797

[13] Tanaka, H., Suzuki, H., Watanabe, A., & Naito, K. (2018, January). Evaluation of a secure end-to-end remote control system for smart home appliances. In Consumer Electronics (ICCE), 2018 IEEE International Conference on (pp. 1-2). IEEE.

[14] H. Suzuki, K. Naito, K. Kamienoo, T. Hirose, and A. Watanabe, "NTMobile: New End-to-End Communication Architecture in IPv4 and IPv6 Networks," in Proc. of ACM MobiCom 2013, Oct. 2013, pp. 171–174.

[15] U.S. Department of Homeland Security, "Strategic Principles for Securing the Internet of Things", Version 1.0, November 15, 2016, URL: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf