Internet of Things Security

Yassine Chahid*, Mohamed Benabdellah, Abdelmalek Azizi
ACSA Laboratory, Faculty of Sciences,
Mohammed First University, Oujda, Morocco
chahid1yassine@gmail.com, {med_benabdellah, abdelmalekazizi}@yahoo.fr

Abstract—**The consequences of security problems are increasingly serious. These problems can now lead to personal injury, prolonged downtime and irreparable damage to capital goods. To achieve this, systems require end-to-end security solutions that cover the layers of connectivity, furthermore, guarantee the privatization and protection of data circulated via networks. In this paper, we will give a definition to the Internet of things, try to dissect its architecture (protocols, layers, entities ...), thus giving a state of the art of security in the field of internet of things (Faults detected in each layer ...), finally, mention the solutions proposed until now to help researchers start their researches on internet of things security subject.**

Keywords—Security, Internet of Things, Layers, Protocols, Privacy, Network.

I. INTRODUCTION

The beginning of the web is marked by the appearance of the web 0.1 still called traditional web which is primarily a static web, centered on the distribution of information. It is characterized by product-oriented sites, which require little intervention from users [1].
The appearance of social networks (Facebook, Twitter, LinkedIn ...), blogs, and forums has revolutionized the web, it's the web 0.2. Currently, they privilege the amount of sharing (texts, videos, images...) [1]. They sees the emergence of social networks, smartphones and blogs. This is where we want to go, even if the web 0.3 is not completely defined, it would be the semantic web, which aims to organize the mass of information available according to the context and the needs of each user, taking into consideration its location, preferences… [1], it is the internet of things (IoT).

The Internet of Things represents a vision in which the Internet extends into the real world including everyday objects. Physical elements are no longer disconnected from the virtual world, but can be controlled remotely and serve as physical access points to Internet services.

This paper is organized as follows:

In section II, we first approach the black past of IoT, citing some outstanding examples in the world. Afterwards, we also dehull each IoT layer. Finally we explain the security of the IoT architecture (protocols, services, support technologies ...) In Section III, we discuss the problems of each layer, analyzing their protocols, sensors and how used in attacks aimed at its weak points. In section IV, we describe attacks that affect the tags, reader and network protocol. We also provide possible ways to counter these attacks. In the last section, we cite some solutions proposed by the various companies and organizations in the field of IoT security. Finally, Section V concludes the paper which was just a reflection on this complicated subject, and gives possible future directions.

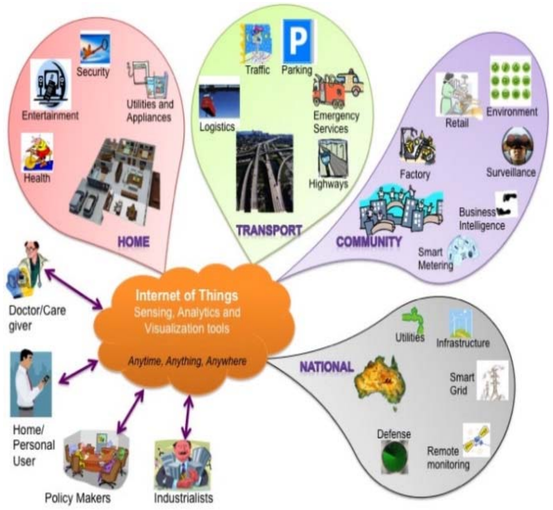

Fig. 1. Internet of Things domain

All this seems interesting for the first sight, but what does this revolution bring us?

II. INTERNET OF THINGS SECURITY

A. *Internet of Things security, a black past*

The security of IoT is a riddle, it gets its value when it fails, it rests on 3 pillars [2] called "CIA", here are the 3 things that can be done to personal and confidential user data:

- Theft them (**confidentiality**),
- Modify them (**Integrity**),
- You prevent to get them (**Access**).

In the paragraphs below, we will cite some examples of the black past in the IoT field security.

In 2000, an Australian was imprisoned two years after hacking a remote sewage treatment plant, causing the discharge of raw sewage into public places [22].

978-1-5090-6681-0/17/$31.00 ©2017 IEEE

In 2005, the industry area was touched, US automotive manufacturing plants were infected for several hours, because the Microsoft Windows system presented a flaw exploited by this infection, which stopped the production of vehicles and thousands of workers were forced to leave their posts during the breakdown.

In 2010, the global digital attacks were used as a weapon, in fact, the Iranian installations were infiltrated by a virus called "Stuxnet", which destroyed the military equipment [19] [20].

In June 2016, Sucuri security experts reported discovering a botnet of more than 25,000 closed-circuit television devices used to launch distributed Denial of Service attacks. "Sucuri" found that the malicious botnet was using IP addresses in more than 105 countries around the world [21].

B. *Internet of things layers*

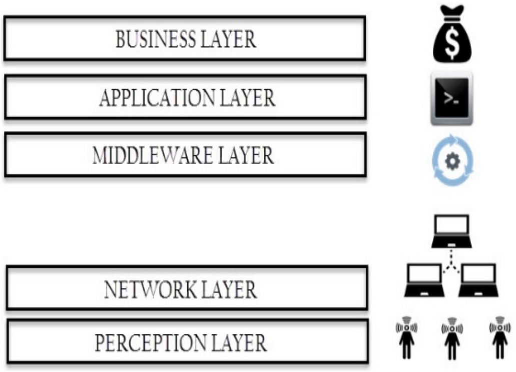

Fig. 2. Internet of things layers

The first layer is the perception layer, the lowest of the Internet of things architecture. It consists in perceiving the data of the environment. Moreover, some operations are being done at this layer, which manages the collection of data with a portion reserved for detection through sensors, bar code labels, RFID tags, GPS... Its main objective is to identify the object and collect the data [3] [23] [24].

The second layer called the "network layer" receives the information and data from the perception layer, like the network and transport layer of the OSI model, collecting data from the lower layer and links it with the Internet From the network. The network layer cannot include a gateway from one interface to another that is to say sensor to other related to the internet. It may include an information center [23] [25].

The fourth layer called "application layer", it receives information from the previous layer (middleware) and gives a more general management of the application presenting this information, and it depends on the type of device and their purpose of the layer of perception [4]. Then the middleware layer according to the needs of the user and finally the layer of the application which presents the data in desired form in all domains in order to earn money from the service provided and it runs in a loop for a more meaningful final service than the existing one [5] [23].

C. *The internet of things* security *architecture*

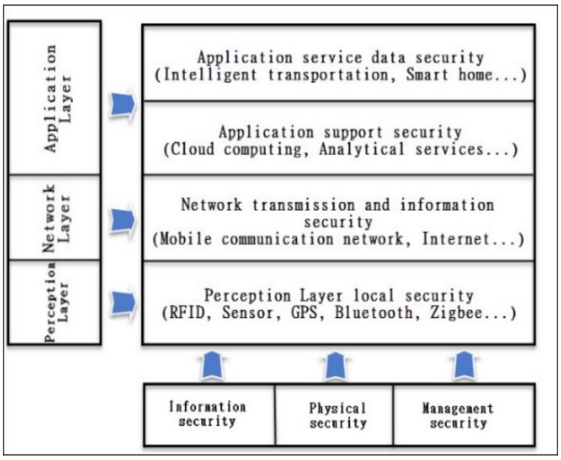
Application Layer
Network Layer
Perception Layer
Application service data security
(Intelligent transportation, Smart home...)
Application support security
(Cloud computing, Analytical services...)
Network transmission and information security
(Mobile communication network, Internet...)
Perception Layer local security
(RFID, Sensor, GPS, Bluetooth, Zigbee...)
Information security
Physical security
Management security

Fig. 3. Internet of Things security architecture.

Security structure in IoT can be divided into three layers, which are the perception layer, the network layer, and the application layer. Some systems use network support technology (such as network processing, computer technology, middleware technology, etc.) as a processing layer. [6] Shows the structure of the IoT system divided by the three layers. It summarizes threats and requirements analysis on the IoT security architecture. [7] Puts forward a typical model of the IoT architecture in the future (U2IoT). It embodies the concept of human central nervous system and social structure. This article will treat the three layer structures.

III. FAULTS DETECTED IN EACH LAYER

We learn that these problems are complex and difficult. Therefore, we must understand all sorts of security issues of different layers, and potential attacks. Considering the system as a whole, security issues need to be addressed early in the design process. Therefore, [8] raises the application for the IoT safety assessment based on the gray correlation algorithm, which has put several common attacks as a safety factor, to perform a quantitative evaluation of the "The network on environment and status". It also lists the specific steps that apply this algorithm to perform the security status assessment. In the paragraph below, we will discuss security issues in each layer.

A. *Perceptual layer security problems*

The main equipment in the perception layer includes RFID, ZigBee, and all kinds of sensors. When the data is collected, the mode of transmission of the information is essentially the transmission of the wireless network. The signals are displayed in the public place. If effective protective measures are lacking, the signals will be monitored, intercepted and disturbed easily. Most detection devices are deployed at unsupervised monitoring sites. Attackers can easily access, control or physically damage equipment. For example, DPA (Differential Power Analysis) is a very effective attack [26]. Several types of common attacks are as follows [9]:

- The gateway node: The gateway node is a sensitive element, it is easily controlled by the attackers. It can leak all information, including the group communication key, the corresponding key, radio key etc., and threatens the security of the entire network.
- False node and malicious data: Attackers add a node to the system, and enter the wrong code or data. They stop transmitting real data. The sleep of the limited node of energy is refused. They consume valuable node energy, and potentially control or destroy the entire network.
- DoS: DoS attack is the most well-known attack in WSN and Internet. It causes loss of network resources and renders the service unavailable [27].
- Sync: The attackers analyze the execution time of the encryption algorithm in order to obtain more information about the hacking method to be used [28].
- Routing: The user can create routing loops, cause or resist transmission of the network, extend or shorten the source path, form error messages, increase the number of end-to-end delay, etc [30].
- Replay: To obtain the confidence of the system to attack, the attacker launches a packet received by the destination host. It is mainly used in the processing of authentication, destruction and certification validation.
- SCA: Time consuming, energy consumption or electromagnetic radiation are the key information used by an attacker to tag encryption devices, and they are also called data leaks.

B. *Network Layer security problems*

- Traditional security issues: The general security problems of the communications network will threaten the confidentiality and integrity of the data. Although the existing communication network is relatively comprehensive of the security protection measures, there are still some common threats, including illegal access networks, listening information, privacy damage, damage Integrity, attack DoS, man-in-themiddle attack, virus invasion, exploit attacks, and so on [10].
- Compatibility problems: The security architecture of the existing Internet network is designed on the basis of the individual's point of view and does not necessarily relate to communication between the machines. The use of existing security mechanisms divides the logical relationship between IoT machines. Access networks have multi-access methods. Heterogeneity makes security, interoperability and coordination worst. It easily has security vulnerabilities [10].
- Cluster security issues: Including network congestion, DoS attack, authentication problem, etc. IoT has a large number of devices. If it uses the existing authentication mode authenticated device, a large amount of data traffic will likely block the network. Existing IP technology does not apply to a large number of node IDs. Mutual authentication between a large numbers of devices causes serious waste of key resources [10].
- Privacy Statement: With the development of information retrieval technology and social engineering, hackers can easily gather a lot of information about the privacy of the particular user [10].

C. *Application layer security problems*

In the application layer, for different industries or environment, its security problems are also different. At present, there are no universal standards for the construction of the IoT application layer. But some companies perform M2M (Machine to Machine) the mode of the IdO, as intelligent community, smart home, medical, etc. [11] highlights an intelligent household security system design system. [12] Gives some solutions based on the 6LoWPAN architecture (IPv6 on low power WPAN) [29]. They are used to support the medical detection system. Although application layer security is more complex and costly, it can still summarize some common security issues:

- Authentication: Different applications have different users; each application will have a large number of users. In order to prevent illegal user intervention, should take effective authentication technology. Spam and the identification and processing of malicious information should also be considered.
- Data Protection and Recovery: Communication data involves the confidentiality of users. Data protection mechanism and data processing algorithm are not perfect, and it can result in data loss and even catastrophic damage. The management of mass nodes is also one of the reasons.
- The ability to process mass data: Due to a large number of nodes, an enormous amount of data transmission, and complex environment, once the data processing capacity and adaptability cannot

meet the requirements, it will lead to interruption And loss of data.

IV. THE INTERNET OF THINGS SAFETY MEASURES

As a multi-network fusion network, IoT security involves different layers in IoT. Many security technologies have been applied in these independent networks. In particular, the mobile communication network and research on the security of the Internet have a long history. For sensor networks in IoT, the diversity of resources and the heterogeneity of the network make security research much more difficult. This section presenting the security measures for each layer will focus on the security technology involved in the perception layer.

A. *Security measures of the perception layer*

Because RFID and WSN are an important part of the IoT perception layer, their security measures will be introduced, respectively [13].

1) Attacks on the Tags:

- Cloning: Even the most important and characteristic feature of RFID systems, their unique identifier, is susceptible to attacks. Although in theory you cannot ask an RFID manufacturer to create a clone of an RFID tag [14], in practice it has proven that the task of replicating RFID tags does not requite a lot of money or expertise considering the wide availability of writable and reprogrammable tags. An ominous ex-ample is the demonstration by a German researcher of vulnerability of German passports [15] to cloning.
- Spoofing: Spoofing is effectively a variant of cloning that does not physically replicate an RFID tag. In this type of attacks an adversary impersonates a valid RFID tag to gain its privileges. This impersonation requires full access to the same communication channels as the original tag. This includes knowledge of the protocols and secrets used in any authentication that is going to a take place [31].

2) Reader Attacks:

- Impersonation: Considering the fact that in many cases RFID communication is unauthenticated, adversaries may easily counterfeit the identification of a legitimate reader in order to elicit sensitive information or modality data on RFID tags.
- Eavesdropping: The wireless nature of RFID makes eavesdropping one of the most serious and widely deployed threats. In eavesdropping an unauthorized individual uses an antenna in order to record communications between legitimate RFID tags and readers this type of attacks can be performed in both directions: tag to reader and reader to tag. Since readers transmit information at much higher power then tags, the former are susceptible to this type of attacks at much greater distances and consequently to greater degree. The information collected can be used to perform advanced attacks later. The feasibility of this attack depends on many factors, such as the distance of the attacker from the legitimate RFID devices.

3) Network Protocol Attacks:

RFID systems are often connected with back-end databases and networking devices on the enterprise backbone. Nevertheless, these devices are susceptible to the sane vulnerability of general purpose networking devices. Malicious users can use flaws in the operating system and network protocols in order to launch attacks and com-promise the back-end infrastructure.

Through appropriate data collection it is possible to detect cloned RFID tags. Alternatively, cloning attacks can be reduced via challenge response authentication protocols. These should also support robust anti-brute force mechanisms. Nevertheless, the inherent resource constraints that RFID tags present lead to weak authentication protocols that are inefficient against determined attackers. Juels [16] has demonstrated some techniques for strengthening the resistance of RPC tags against cloning attacks, using PIN based access to achieve challenge response authentication. Public awareness of the security implication related to cloning attacks should be the key policy to defend against. However, this is not always the case. For instance, none of the countries that issue e-passports have anti-cloning mechanisms [14] as suggested by the ICAO 9303 standard [15]. In order to defend against passive eavesdropping attacks encryption mechanisms could be used to encrypt the RFID communication. Spoofing and impersonation could be combated by using authentication protocol or a second form of authentication such as one-time passwords, PINs or biometrics.

B. *Network layer security measures*

In the current IoT structure, the network layer exists on the internet or on the existing communication network. Some factors endanger the security of information on the Internet, and are also IoT damage information service. But the old network communication technology is not completely adapted to IoT. Traditional network routing is simple, and their main focus is not security. Because of the random, autonomous, unreliable IoT node arrangement of energy limitation and communication, it leads to that IoT do not have dynamic infrastructure and topology. The attacker can easily cause attacks [10]. For different network architecture, we need to configure the specific authentication mechanism, end-to-end authentication and key tuning mechanism, PKI (Public

Key Infrastructure), WPKI for wireless, security routing, intrusion detection, etc. Due to the enormous amount of data, network availability should be considered. In addition, it should also enhance cross-domain authentication and cross-network authentication in the network layer. [17] Gives the development trend of information security products based on IPv6. IPv6 Network.

V. INTERNET OF THINGS SOLUTIONS

Reducing the exposure area of connected objects to attacks is a complex task. It requires architectural knowledge of the value chain that connects objects to the cloud. You need to look at the objects themselves, their sensors and processors, local and remote networks, protocols at all levels, then servers, their software and data processing. The needs have been well known for years (see "Security needs in embedded systems" published in 2008). Many companies offer tools to secure this or that part of the value chain, but they have positioned themselves for a short time in connected objects [18].

In the value chain of connected objects, you must start with the objects themselves. They often include a chipset or a microcontroller based on ARM kernels. The most common ARM kernels are those of the A series found in smartphone and tablet chipsets that can be worth more than $ 10 and those of the M series found in object microcontrollers Connected devices that are worth around $ 1. Until now, ARM proposed to secure chipsets using serial a kernels with its TrustZone, a secure zone for performing protected processes, such as conditional access control systems in set-top boxes [32]. Pay TV. ARM announced at the end of 2015 that this technology should also be integrable in Cortex-M core microcontrollers. In July 2015, ARM acquired the Sansa startup, which will enable them to complete the TrustZone with an additional software and hardware security architecture. All this will happen in the ARM roadmap in 2016 and thus probably in commercial secure chipsets in 2017 that will be integrated into mainstream connected objects in 2018. The process will take a little time!

However, the value chain for the design and production of embedded chipsets is fragile. It is based on the integration of functional blocks of various origins ("IP blocks"), with various integration software and manufacturing in factories in China or elsewhere that are not necessarily well secured. Hence the emergence of technological solutions that allow to create ultra-secure chipsets, especially adapted due to their cost to professional applications. In the present case, the threats are not from hackers but rather from states and large companies involved in industrial espionage. In order to secure the chipsets of connected objects for demanding applications, the French company Prove & Run offers proven core, a secure and formally proven micro-kernel. It runs on hardware architectures based on ARM cores and Intel x86. In ARM core processors, Provencore runs in the TrustZone on Cortex a core chipsets, but also works on Cortex M-based architectures used in connected object microcontrollers. This seems to be an alternative to the Sansa solution, acquired by ARM. One does not risk in any case to see appearing this kind of technology in its toothbrush connected!

Ercom society presented to the MWC of Barcelona its solution Cryptosmart of security by encryption of the storage and communications of the smartphones and tablets Samsung, is labeled France Cybersecurity, a member of the BxaTrust Association. CryptoSmart relies on an EAL5 + certified smart card and an EAL4 + certified applet. It is enough to compose its code to activate the security by local encryption of the terminal. Ercom also offers Mobipass, a cloud solution for simulation and testing of mobile networks. It simulates the operation of thousands of terminals. In October 2015, Ercom and Samsung announced the integration of Ercom encryption solution into the new Korean smartphones [18].

Famoco offers the FX100 +, a secure terminal running on Android and supporting the NFC, which can serve as a payment terminal. The company was exhibiting at both the 2016 Las Vegas CES and the MWC. This is a way of isolating functions that require a high level of security in a specific terminal. It is targeted at professional applications. One cannot reasonably expect that consumers use this kind of terminal in addition to their smartphone [33].

The universe of telecom operators is not left behind. At the beginning of 2016, the GSMA published guidelines for securing IoT architectures, in partnership with telecom operators from several continents: AT & T, Verizon, China Telecom, Etisalat, KDDI, NTT Docomo, Orange, Telefonica, Telenon and Gemalto. OEMs are also aiming to complete their offerings to secure end-to-end networks, in addition to their substantial investment in preparing for future deployments of the 5G.

Ericsson presented to MWC 2015 its security solutions focused on data storage in the cloud. For its part, Nokia has just acquired the Nakina systems, to secure 5G networks and the Internet of things. They target like the other mainstream IoT, connected cars, e-health and big data. Huawei also wants to have a say in securing connected objects. It promotes a collaborative approach and standardization with the rest of the industry [33].

VI. CONCLUSION AND FUTURE WORK

Existing IOT security solutions were used primarily by designers of mission-critical embedded systems related to aerospace, security and defense. As personal perspectives, we will study security architecture and specific operating modes in the context of the Internet of things. Next, it will be asked to propose innovative approaches to ensure the availability, integrity and confidentiality of such architecture. Finally, work will be carried out on the evaluation of the proposed approaches in relation to the more conventional vision of the Internet of things.

REFERENCES

[1] Sareh Aghaei, Mohammad Ali Nematbakhsh, Hadi Khosravi Farsani, “Evolution of the World Wide Web: from web 1.0 to web 4.0”, pp 1-5 (IJWesT) No.1, January 2012

[2] DánielPetró, GyörgyVesztergombi, “Security and trust challenges in the area of the Internet of Things”, European Union Seventh Framework Programme (FP7/2007/2013) agreement number (258360).

[3] Dieter Uckelamann, Mark Harrison, and Floria Michahelles, “Architecting the Internet of Things,” Springer-Verlag Berlin Heidelberg, 2011.

[4] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan, “Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges”, in the proceedings of 10th International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 17-19 December, 2012.

[5] Client Advisory DYN / DDoS ATTACK, redfivesecurity 888-733-5007, 2016

[6] Zhuankun Wu. : Initial Study on IOT Security architecture. J.Strategy and decision-making research (2010)

[7] Huansheng Ning, Hong Liu, “Cyber-Physical-Social Based Security Architecture for Future Internet of Things”, J. Scientific research (2):1-7 (2012).

[8] Hongbo Gao, “Study of the application for the security state assessment about the internet of things based on grey correlation algorithm”, J. Manufacturing Automation. 34(11) (2012).

[9] Shancang Li, Kewang Zhang, “Principle and application of wireless sensor network”, M. Beijing: China Machine Press (2008).

[10] Kai Zhao, Lina Ge "A Survey on the Internet of Things Security", 2013 Ninth International Conference on Computational Intelligence and Security, China.

[11] Xueguang Yang, Fengjiao Li, Xiangyong Mu, “Design of security and defense system for home based on Internet of things”, J. computer application. 30(12):300-318 (2010).

[12] Antonio J. Jara, Miguel A. Zamora, Antonio F.G. Skarmeta. “HWSN6 Hospital Wireless Sensor Networks Based on 6LoWPAN Technology: Mobility and Fault Tolerance Management”, C. In: International Conference on Computational Science and Engineering, 879-884 (2009)

[13] Nabil Kannouf, Youssef Douzi, Mohamed Benabdellah, Abdelmalek Azizi, “Security on RFID technology”, International Conference on Cloud Technologies and Applications (CloudTech), 2-4 June 2015, Marrakesh, Morocco, IEEE Xplore Digital Library.

[14] Laurie, A., “Practical Attacks Against RFID”, In: Network Security, Vol. 2007, No9, pp. 4-7

[15] Mitrokotsa, A., Rieback, M.R. & Tanenbaum, “Classification of RFID Attacks”, DOI: 10.1007/s10796-009-9210-z 29 July 2009, Link Springer.

[16] Juels,A., “Stengthening EPC Tags Against Cloning”, In: Proc. Of ACM WorkShop on Wireless Security (WiSe’05). ACM Press (2005), pp. 67-76.

[17] Lei Li, Jing Chen, “System Security Solutions of RFID System of Internet of Things Sensing Layer”, J. Net Security Technologies and Application, (6): 34-36 (2011)

[18] Olivier Ezratty – “Opinions Libres”, Can we secure the Internet of things? "Cybersecurity Conference - IOT and Embedded Systems, Toulouse 18 February 2016

[19] B. Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," Strategic Insights 10, 15 (2011).

[20] J. Grayson, "Stuxnet and Iran's Nuclear Program," Physics 241, 7 Mar 11

[21] Krebs, Brian (September 21, 2016). "KrebsOnSecurity Hit with Record DDoS". Brian Krebs. 17 November 2016.

[22] Tony Smith, 2001, "Hacker jailed for revenge sewage attacks" "The register" Journal

[23] Qi Jing Athanasios V. Vasilakos Jiafu Wan Jingwei Lu Dechao Qiu - Security of the Internet of Things: perspectives and challenges - DOI 10.1007/s11276-014-0761-7 Springer

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

[25] Xue Yang, Zhihua Li, Zhenmin Geng, Haitao Zhang, A Multi- layer Security Model for Internet of Things, in Communications in Computer and Information Science, 2012, Volume 312, pp 388-393

[26] Mr. Ravi Uttarkar and Prof. Raj Kulkarni, ”Internet of Things: Architecture and Security,” in International Journal of Computer Application, Volume 3, Issue 4, 2014

[27] Kimberly Hengst, "DDoS through the Internet of Things", An analysis determining the potential power of a DDoS attack using IoT devices - Twente Student Conference on IT

[28] Krushang Sonar, Hardik Upadhyay, "A Survey: DDOS Attack on Internet of Things", International Journal of Engineering Research and Development, Volume 10, Issue 11 (November 2014), PP. 58-63

[29] Raghavendra K, Sumith Nireshwalya, "Application Layer Security Issues and Its Solutions", IJCSET |June 2012| Vol 2, Issue 6,1266-1269

[30] Weizhe Zhang, Baosheng Qu, "Security Architecture of the Internet of Things Oriented to Perceptual Layer", International Journal on Computer, Consumer and Control (IJ3C), Vol. 2, No.2(2013)

[31] Qi Zhang, P.SilpaChaitanya, T. Sudhir, "Spoofing Attack Detection Wireless Networks using Advanced KNN", International Journal of Smart Device and Appliance Vol. 4, No. 1 (2016), pp.1-8

[32] Rijswijk-Deij, Roland van and Poll, Erik (2013) *Using Trusted Execution Environments in Two-factor Authentication: comparing approaches.* In: Open Identity Summit 2013, OID 2013, 9-11 September 2013, Kloster-Banz, Germany (pp. pp. 20-31).

[33] Mobile world congress 2015, Barcelona