International Journal of Advanced Computer Science and Information Technology (IJACSIT)
Vol. 4, No. 1, 2015, Page: 1-13, ISSN: 2296-1739
© Helvetic Editions LTD, Switzerland
www.elvedit.com

Internet of Things: Features, Challenges, and Vulnerabilities

Authors

Ebraheim Alsaadi
College of Technological Innovation, Zayed University
m80005158@zu.ac.ae
Abu Dhabi, UAE

Abdallah Tubaishat
College of Technological Innovation, Zayed University
Abdallah.Tubaishat@zu.ac.ae
Abu Dhabi, UAE

Abstract

The terminology Internet of Things (IoT) refers to a future where every day physical objects are connected by the Internet in one form or the other, but outside the traditional desktop realm. The successful emergence of the IoT vision, however, will require computing to extend past traditional scenarios involving portables and smart-phones to the connection of everyday physical objects and the integration of intelligence with the environment. Subsequently, this will lead to the development of new computing features and challenges. The main purpose of this paper, therefore, is to investigate the features, challenges, and weaknesses that will come about, as the IoT becomes reality with the connection of more and more physical objects. Specifically, the study seeks to assess emergent challenges due to denial of service attacks, eavesdropping, node capture in the IoT infrastructure, and physical security of the sensors. We conducted a literature review about IoT, their features, challenges, and vulnerabilities. The methodology paradigm used was qualitative in nature with an exploratory research design, while data was collected using the desk research method. We found that, in the distributed form of architecture in IoT, attackers could hijack unsecured network devices converting them into bots to attack third parties. Moreover, attackers could target communication channels and extract data from the information flow. Finally, the perceptual layer in distributed IoT architecture is also found to be vulnerable to node capture attacks, including physical capture, brute force attack, DDoS attacks, and node privacy leaks.

Key Words

Internet of things, denial of service attacks, eavesdropping, node capture, physical attack, vulnerabilities.

I. Introduction

IoT can be defines as a future where every day physical objects are connected by the Internet in one form or the other, but outside the traditional desktop realm [1]. To meet this challenge, it is expected that sensor network and RFID technologies will become increasingly integral to the human environment, in which communication and information systems will be invisibly embedded. Subsequently, massive volumes of data will need to be processed, stored, and presented in an easily interpretable, efficient, and seamless form. Kortuem et al [2] argue that context-aware computation via network resources and smart connectivity via existing networks will be critical elements of the IoT. Some evidences of the evolution towards ubiquitous communications and information networks can be seen in the growing presence of 4G-LTE and WiFi. The successful emergence of the IoT vision, however, will require computing to extend past traditional scenarios involving portables and smart-phones to the connection of everyday physical objects and the integration of intelligence with the environment [2]. Ning and Hu state that for this to happen, there must be analytics tools aiming for smart and autonomous behavior, pervasive communications networks, and software architectures that can process contextual information and convey it according to relevance, and a common understanding of users and their specific appliances [3]. The presence of all three aspects will be crucial in ensuring the achievement of context-aware computation and smart connectivity. At this point, the Internet will no longer only be accessible from smart-phones and laptops but will be part of such objects as cars, ovens, baby monitors, and TV sets. In addition, the IoT will become completely integrated into medical and other critical devices and pervade majority of sectors. Unfortunately, as with other major developments in the Internet era, growth in the IoT technology will be equally matched by growth in security and privacy concerns [3]. Several researchers are pointing towards the evolving nature of challenges and vulnerabilities in various existing IoT devices.

This research paper seeks to investigate the features, challenges, and vulnerabilities facing the new and dynamic realm of the IoT. The study is organized into six sections. The following section exhibits some studies related to the development of IoT. In section III, we discussed how emergent IoT technologies have been used in societies. We studied United Arab Emirates (UAE) as an example. Section IV explains the problem at hand and the methodology used in the study. Section V demonstrates the emergent challenges and vulnerabilities. Finally, section VI, presents the results of the study, and offer directions for future research in IoT.

II. Related Work

IoT has the capabilities to make homes and our life smarter. These innovative technologies provide convenience in everyday activities, energy efficiency, security, and comfort [3]. Adding intelligence capabilities to various environments like homes could provide increased life quality for the sick and elderly, for example. Much of the attention in research has revolved around wireless technologies that are supportive of remote data control, sensing, and transfer, such as cellular networks, RFID, Wi-Fi, and Bluetooth, which have been used to embed intelligence into the environment. Kranz et al conducted a study concerning a Bluetooth-based system that uses smart-phones sans Internet controllability, in which physical connection of devices to Bluetooth sub-controllers was done, followed by the smart-phone’s control via built-in connectivity with Bluetooth [4]. Limitations in the range of operations for the system, however, meant that it could not cope with mobility, thus could be controlled only within the device’s vicinity. Researchers have also made attempts to provide remote access and network interoperability to control appliances and devices in the home through the use of home gateways, which has seen the

Copyright © 2015 Helvetic Editions LTD - All Rights Reserved

introduction of Wi-Fi based systems that use web servers based on PCs that manage connected devices in the home [4].

Karimi contended that the world is entering a period of IoT computing technology with great potential to enable the communication between machines, machines and infrastructure, and machines and the environment [5]. His research demonstrates the IoT as a universal global neural network based on cloud technology that will pervade all aspects of human life, which will be founded on intelligence provided by embedded processing. The communication and interaction of smart machines with other machines, infrastructures, environments, and objects will result in the generation of massive data volumes that will be processed into actions that can control and command objects to make lives safer and easier [5].
Goldman Sachs commissioned a research report into the IoT, which concluded that the IoT wave of computing would be larger than the previous two computing waves; the fixed Internet wave and the mobile wave [6]. The report posits that the IoT will lead to the creation of new technology winners and losers, which will be based on the ability of companies to adapt to an increasingly integrated and interconnected world. The direction of technology adoption and development will be tilted by the S-E-N-S-E framework proposed by the report; sensing, efficient, networked, specialized, and everywhere [6].

Evans found that IoT has reached the point where a multitude of sensors and disparate networks must integrate and interoperate under common standards, proposing that such an effort needs academia, standards organizations, governments, and businesses to work in tandem [7]. The report also considers what must happen for IoT to gain acceptance by the wider public, exploring the effects of service providers delivering applications that add tangible value to the lives of people [7]. In completing the report, the researcher explores the importance of providing value in human terms, rather than just being representative of technological advancement.

The Parametric Technology Corporation (PTC) explored the IoT in relation to the manufacturing industry, studying its emergence and effects alongside parallel innovation of other enabling technologies and market forces [8]. In the report, the evolution of purely physical products into complex systems that combine digital user interfaces, software, sensors, and processors is investigated in relation to multiplication of product capabilities and value creation. In addition, the report also assesses how the impact of IoT has transformed manufacturers' ability to create value and exchange it with consumers, especially as the IoT shifts differentiation and value sources towards service, the cloud, and software, thus creating new models of business [8].

Miorandi et al refer to IoT as a general term that encompasses the entire extent to which the web and the Internet have pervaded the physical realm, in which spatially deployed devices are widely distributed and embedded into physical objects for their identification through enhanced actuation/sensing capabilities [9]. The IoT concept envisions a world in which physical and digital entities will all be linked, giving rise to a new generation of services and applications using relevant and appropriate ICT systems.

Tan and Wang argue that all objects in the future will have unique features for identification that can be interconnected to create the IoT [10]. Communication, as a result, will shift from being solely between humans to communication between humans and things, which will alter life, as we know it through the emergence of a ubiquitous communications and computing era

[10]. RFID and other sensing technologies used for relevant identification purposes are widely held as a cornerstone of the coming IoT era.

Weber approaches IoT from the perspective of an Internet-based global architecture that will enable trade of services and goods in the global chain of supply, while also portending a significant impact on the privacy and security of all stakeholders involved [11]. In such a case, there will be need to implement measures to ensure that the system is flexible with regards to Internet attacks, privacy of the clients, access control, and authentication of data. In addition, a legal framework must be set up taking the underlying technology into account, which Weber contends would be established best through international legislation supplemented by both the public and private sector according to their particular needs in order to make the architecture more adjustable [11].

Zhou et al build on this argument by positing that legislations aimed at IoT regulation should establish a taskforce to look into legal challenges facing IoT, make provisions that support use of IoT mechanisms, rules on security and legislation of IT, provisions that restrict or prohibit use of IoT mechanisms, and the right to information [12].

Roman et al approach IoT in terms of services that can be provided through centralized architectures, in which central entities are able to attain, analyze, process, and provide data and information [13]. On the other hand, distributed architectures in which entities dynamically collaborate and exchange information with one another can also be utilized. To understand the viability and applicability of such a distributed approach, Roman et al argue that it is necessary to be acquainted with its merits and demerits with regards to its features, as well as privacy and security challenges [13].

Roman et al argue that in IoT, all physical objects possess virtual components, which are able to consume and produce services, while such connection will result in unprecedented economies of scale and convenience, it will also need to be approached with novelty to ensure ethical use and safety [14]. Indeed, if IoT complies with security and privacy requirements, it has the opportunity to become a paradigm that improves daily life. However, Roman et al contend that there are significant issues in such areas as trusted architectures, self-management, user privacy, identity and data management, network protocols, and cryptographic mechanisms that must be addressed if this is to happen [14].

The realization and concept of IoT will make the current world an entirely ubiquitous one because IoT will change people’s perspectives of the Internet radically by including all possible physical objects into the network. According to Zorzi et al, this communications will occur in the IoT between things, people, and their environment, especially with the combination of cloud computing, the Internet, embedded sensors, real-time localization, and near-field communications, creating smart objects out of all physical objects to enhance understanding and reaction to their environment [15]. The IoT concept will integrate Internet information and services, resulting in more information, data, and knowledge being generated and utilized. The IoT concept has increased in popularity in the recent years with researchers and scholars investigating and discussing various aspects of IoT, while international conferences have open sessions for specialists and scholars to exchange opinions, ideas, and experiences about applications and development of IoT.

Copyright © 2015 Helvetic Editions LTD - All Rights Reserved

Barnaghi et al suggest that IoT must be semantic oriented, things oriented, and Internet oriented, proposing that IoT architecture is actually made up of three segments, including the presentation segment, the middleware segment, and the hardware segment [16]. The middleware segment referred to by the researcher is referent to the cloud environment that is mainly responsible for storage and computation of data, as well as data analytics [16]. The hardware segment, on the other hand, is referent to the connection of embedded communication hardware or sensors, while the presentation segment visualizes data analytics results and interprets data in a format that is easier to understand. Moreover, the IoT should have cooperation and communication.

According to Yan, wireless sensor networks will be the critical technology for IoT applications such as energy saving and home automation, specifically at the hardware segment [17]. In these wireless sensor networks, sensor devices communicate wirelessly with other devices at the communication node. Thus, measurement and communication will be the two critical functions expected of the wireless sensory network, in which sensors are deployable in a dense and random manner at lower costs [17]. In an attempt to increase acceptance of IoT technologies, models that are reflective of human willingness to accept the specific technologies are emerging. Generally, if the perception of a technology is that it is easy to use and useful, it is more likely that they will accept it, although IoT shows increasing variations and complexities across user types and domains.

Bassi criticizes the neglect of cultural, social, and group aspects of decision making in existing and current IoT models, while also noting that there is a lack of comprehension about the self-regulating processes, emotion, or effect of IoT, especially with regards to feedback [18]. Alternatively, new technology uptake can be individually and socially conceptualized using Roger’s model of “Diffusion of Innovations”, which suggests that whether a technology is rejected or accepted is reliant on how individuals are made knowledgeable of it and attempts made to increase acceptance through persuasion [18]. Following tentative, initial acceptance, the individuals will experiment with utilizing the innovation in order to determine ultimate utility and whether its use is worth pursuing.

Weber and Weber, in their literature review on ubiquitous monitoring, found that control, awareness, intrusion, context, trust, boundaries, and justification are factors that impact monitoring-related behavior [19]. They proposed that control, coverage, and obtrusion are among elements that must be taken into account in the designing of systems, as well as data collection frequency and data integration abilities across sources. Social dynamics, especially their complexity, mean that there are particular issues presented in the home from introducing IoT technologies. Technology domestication research studies have taken a qualitatively rich approach, especially in comprehending how technologies shift to the home’s private space from the public domain.

Gaglio and Lo argue that this process is a transformation from meaningless and cold products into desirable home applications, in which consumers get into a struggle for control, while the devices and applications become media for negotiating meaning [20]. Reliance on the extensive frameworks and architecture required in the IoT means that governmental, commercial, household, and individual cooperation and agreement would be required for the functioning of many IoT technologies. Societal and organizational advantages can be incentivized to ensure that the individual gets the benefits, while the role of leisure and fun in ensuring technology acceptance must not be forgotten [20]. Simultaneously, the consequences and acceptance of the

IoT applications and technologies will be reliant on a range of psychological and social issues. Majority of existing and envisioned IoT technologies are present in the home and workplace, including systems like smart fridges, networked energy monitors, and activity tracking systems that operate via tagging of objects. Such systems will collect detailed data and information concerning activities within the home and about individual activities for those living together and sharing access to relevant information [20].

As technologies tasked with capturing data about individuals become increasingly visible, data collection outcomes could make new information forms visible to others around us. New information alerts, visualizations, and appliances are part of the vision of IoT, and smart activity will have its basis in human actions and collected data, defining and highlighting previously unknown or ambiguous elements of these actions. Uckelmann et al, in reviewing existing dissonance between guidelines on privacy and data collection forms in IoT systems, argue that the personal data notion is disrupted, especially as volumes of data are collected that do not directly relate to any single individual, but from which personal data and information is ascertainable via collation of information [21]. In addition, there will be less awareness about when there is collection of data, as well as how the collected data is to be used. In such technologies as smart fridges and energy monitors, it is already evident that a new form of information appliance is emerging via which there is display of information at home level, while different degrees of detail also exist that can be used in understanding individual activity [21].

These data also possess the potential to comprehend individual behavior and overall house-hold behavior. Increasing monitoring and awareness of individuals is one of the most obvious uses of IoT data and technologies. While this may be a point of happiness for parents and work-place superiors, Gubbi et al note that surveillance is a growing point of increasing tension in various relationships be they parent-child or employer-employee [22]. Use of IoT in the home could particularly result in tensions during adolescence, particularly as individuals seek to increase and take control of their privacy and parents seek to maintain data and information access, as they are anxious of their children’s welfare. This was the conclusion reached by Gubbi et al after studying monitoring of blood glucose using IoT appliances by parents, finding an increase in tensions later on in life [22]. As a result, they conclude that the use of IoT in the household could prove especially disruptive.

IoT applications and technologies have also been found to have potential in caring for elderly citizens, especially in assistance and tele-monitoring, although it is crucial to consider universal privacy needs, as well as the relationships between care-givers and family members within the IoT designs. Sun et al, reported on attitudes to tracking technologies using GPS, they found that complex issues emerged regarding how care-givers and family felt an obligation to spend long periods monitoring information to make sure the individual was safe, as well as finding that the elderly preferred technology restrictions on the basis of autonomy rights [23]. Increasing control and awareness seeking to encourage positive change of behavior is another theme that has arisen with the emergence of the IoT. Such arguments have proven successful in such initiatives as the UK government’s intention to use smart energy monitoring systems for all homes by the year 2020 [23]. However, Kotis and Katasonov note that such systems are faced with complex design space, especially by the stakeholders, including appliance manufacturers, governments, consumers, and energy suppliers [24]. IoT-based smart energy meters will be expected to share information inside and outside the household and research is suggestive of the fact that social influence will be critical in encouraging change in behavior, as well incentivizing the use of IoT applications. Increasing the information that is available across diverse sectors, therefore, will

Copyright © 2015 Helvetic Editions LTD - All Rights Reserved

cause the emergence of new tensions; particularly as IoT-related companies pursue consumer behavioral change.

Su et al, in an analysis of various interventions seeking to ensure households were made more aware of their energy use, concluded that some of the participants became increasingly uncomfortable and over-conscious about their usage of energy [25]. As such, it is evident the positive intentions of the IoT aimed at improving lives and creating positive behavior change can cause the emergence, in some cases, of negative psychological and social outcomes.

III. The Internet of Things in the UAE

Middle East markets growing at a faster rate than any other regional markets. It is forecasted that regional spending on IT will stand at $211 billion in 2015, which will rise to $243 billion by the year 2019 driven by such areas as big data, smart government, mobility, and the IoT[26]. In the IoT, the momentum is being driven by consumer and business demand, ongoing development of smart homes and cities, enhanced connectivity infrastructure, and an increasingly connected culture. The United Arab Emirates (UAE) has become a regional hub and a gateway for companies attempting to access the Far East market. The local governments in the UAE, particularly in Abu Dhabi and Dubai, has recently sought to convert the whole country into one connected, smart city using smart devices and sensor technology. These technologies are expected to be used across three tracks, namely: tourism, life, and economy [26].

Dubai's government has recently announced plans to convert the entire Dubai emirate to a smart city, representing exciting times for consumers ahead. This project will use smart devices and sensors in three main areas, which are Smart Life, Smart Economy, and Smart Tourism. The Smart Life aspect of the project deals with energy services, public utilities, communications, transport, education, and health. For the Smart Economy aspect, it involves development of smart stock exchanges, port services, smart companies, and smart jobs [26]. Finally, the Smart Tourism aspect involves the provision of convenient and smart environments for visitors to Dubai, including smart hotel services, smart gates, flight services, and visa services.

The momentum of IoT in the UAE has been driven by various factors, most importantly the continued demand by consumers and businesses, which means that the demand for more IoT solutions will continue [26].

IV. The Problem and Methodology

According to Kranz et al [4], cyber-security incidents cannot be escaped and, as such, society must prepare and plan for them, especially in the IoT wave of computing. Private and governments sectors will come up against more sophisticated, diverse, and broader cyber threats than before. As IoT becomes the new norm, these entities will have to develop and test their response plans to cyber-security incidents, while also monitoring their networks, assuming that breaches have occurred. This threat is especially magnified by the increasing pervasion of the IoT as more devices become connected to the web and the Internet. The IoT magnifies privacy and data security challenges with regards to protecting devices connected to the Internet [4].

The focus of this study is to look at the distributed approach architecture of the IoT as it is expected that challenges will emerge related to Denial of Service attacks taking place, while eavesdropping over the Internet connections may also pose unique challenges to the IoT architecture.

V. Methodology

This research study used the qualitative paradigm of research, due to its concern with process and outcomes, rather than outcomes, which are more important to this study as the IoT is still evolving. By using the qualitative paradigm of research, it will be possible to uncover various issues concerned with perceptions and experiences about the use of IoT in the future [28]. An exploratory research design was also used for the current research study, mainly due to the fact that there are few studies dealing with the features, weaknesses, and challenges of IoT. As a research area that is in its preliminary phase, an exploratory design enabled the researcher to gain insight into the challenges facing the IoT [29]. Moreover, exploratory research design also provided us with the opportunity to clarify and define new ideas as the IoT concept becomes more familiar.

Desk research was used as the method of data collection, in which Internet searches were done for the features, challenges and vulnerabilities of using the IoT. Some of the resources searched included white papers, analytical reports, websites, and journal articles, after which data collected was cross-referenced and collated. In searching for resources, the search words used included “features of the Internet of Things”, “challenges of the Internet of Things”, “weaknesses of the Internet of Things”, “Denial of Service attacks in the Internet of Things”, “Eavesdropping challenges in the Internet of Things”, and “node capture challenges in the Internet of Things”.

After accessing the resources, some were excluded on the basis that they lacked relevance, while those published before 2008 were also excluded because of the dynamic and evolving nature of the IoT. The final resources were then scoured for information that sought to answer the research questions, after which the data was analyzed using the grounded theory analysis. This resulted in the coding of data collected from the resources using features and challenges as the main codes. This was followed by grouping of these codes into categories, which included challenges related to DoS attacks on the IoT, challenges related to eavesdropping in the IoT, and challenges related to node capture in the IoT.

VI. Emergent Challenges and Vulnerabilities to IoT

We have identified the following challenges and vulnerabilities to IoT:

1) *Denial of Service Attacks in the Internet of Thing: As more devices move towards IP-enabled status, they are contributing to a pool of things that are easily recruited into such platforms as botnets, which can be utilized for distributed attacks [17]. The use of distributing attacks makes the tracing of attack sources more difficult, while also making it easier to overwhelm devices and applications that are targeted. For instance, distributed DoS have become a choice mode of attack for blackmailers and activists. Yan mentions Simple Network Management Protocol attacks as a special form of DDoS attacks, which allow malicious attackers to hijack network devices that are not secured, such as sensors, cameras, printers, and routers, using them as bots in the attack of third parties [17]. This form of DDoS attack is a concern due to the fact that it increases the number of devices under the risk of being compromised, as well as because such remote devices as sensors and printers are less likely to be properly secured and managed, which makes them easier to exploit. Simple Network Management Protocol (SNMP) utilizes user*

datagram protocol, which is a stateless protocol liable to IP spoofing. Zhou et al identify the reflection DoS attack that uses SNMP as a form of amplification attack, due to the fact that SNMP requests lead to responses that are typically thrice as large as would be expected normally before [12]. Thrice as large means that the number of responses from protocol requests is three times what they would normally be. An attacker, therefore, could port-scan an array of IP addresses with the aim of identifying SNMP hosts that can be exploited before sending an SNMP request utilizing the target servers' spoofed IP address to the identified hosts, after which the replies from the host saturate the bandwidth of the target, thus rendering it unavailable. There is a significant amplification of the traffic's response size, making the SNMP vector of reflection attack a substantially powerful force [3].

Roman et al argues that the protection from DoS attacks takes the identification of all devices that can be accessed through one's network, whether they appear to be sensitive or not, and to manage them properly [13]. Remote access to devices and management of devices, while bringing great convenience, adds trade-offs that must be secured and managed. Typically, the limited computation and tight memory of physical things means that they are open to resource exhaustion attacks [13]. It becomes possible for attackers to send requests continuously for processing by specific devices, in effect depleting their resources. In the IoT, this becomes particularly dangerous if the attacker uses a Line Link Network (LLN) to target a resource-constrained device while located in the backend. Moreover, Zorzi et al also found that physical jamming of communication channels could be used to launch DoS attacks, which would disable communication channels between things [15]. Finally, it was also found that using large amounts of packets to flood the network could also disrupt network availability [15].

2) Eavesdropping in the Internet of Things: It was found that passive attackers could target communication channels such as the Internet, local wired networks, and wireless networks to retrieve data from the flow of information [10]. Obviously, should an internal intruder access specific infrastructure, they can then retrieve information flowing across the infrastructure. While there are security measures aimed at protecting data and information, the possibility that an intruder could access the system and hijack data is real. One of the greatest challenges to the large-scale acceptance of the IoT from the perspective of the user is about data control. Tan and Wang indicated that caution must not be confused with data ownership [10]. The IoT will lead to a situation where the access and control of data is more important than ownership of information. How access to the information flows in the IoT is allowed is expected to be a slippery slope. While there are some overall advantages to enabling this access, such as the ability of Google Trends to predict cases of Flu outbreak accurately, Roman et al still contend that the access to personal data on the IoT carries massive challenges [14].

Another challenge that will face the development of the IoT is data sharing. In the IoT paradigm, data is all-important, although provisioning of data is the result of a social contract between the customers and corporations [18]. The corporations will provide a nominally-priced or free service, which they exchange for the personal data of the customer. This data can then be used in the further development of services and products that fulfill the needs of the consumer, as well as sold to marketers and advertisers. It is possible to use third party applications that are based on the core service, especially in poaching customers and their related data from applications like these. For large *corporations and established networks, this could become detrimental as a practice since these applications could eventually poach clients. Large corporations, in such scenarios, must balance their commercial considerations with their open source approach [18].*

3) *Node Capture in the Internet of Things : Things like streetlights and household appliances are located physically in specific environments and, rather than destroying them, active attackers may attempt to extract information contained by the things. Instead of the things, the active attacker could also target the infrastructure that is used to store information, including data storage entities or data processing. If, on the other hand, the actual intelligence in the IoT is distributed, different entities will be used to create and process the information, meaning that attackers must improve their efforts to control a similar amount of resources [19]. However, it was found that resource distribution acts as a double-edged sword. If attackers are interested solely in a particular piece of information, they can target systems managing the specific information located in central entities. Indeed, attackers could utilize a guerrilla strategy to take control gradually of small portions of one's network, covertly affecting the entire system. In addition, node capture attacks are more dangerous because there is more logic integrated into the things. Perceptual nodes within the perceptual layer normally create a dynamic distribution ad hoc network [19].*

Due to the limitation of node resources, distributed organized structure, and dynamic network typology change, the perceptual layer leads to various threats, including physical capture, in which many nodes are deployed statically and can be captured easily by attackers, becoming physically compromised [24]. Another threat comes from brute force attack, especially where resource storage ability and sensor node computation are limited, making them vulnerable to brute force attacks. In addition, the structure of hardware for some perceptual nodes is easy to understand and simple, making it easier for attackers to copy it, while authentication is difficult in the distributed environment enabling malicious nodes to utilize fake identities for collusion or malicious attacks. Routing attacks are also possible in the IoT, especially where data relay and forwarding exist in the perceptual data collection process, making it more likely that intermediate nodes may attack the data during forwarding [24]. The nodes are also vulnerable to trapping under DoS attack because of their finite ability of processing, while attackers can also actively or passively steal sensitive information present in the node, which Evans [7] refers to as node privacy leaks.

4) *Physical Security of the Sensors: Physical attacks could also destroy sensors in IoT devices physically or even make them inoperable permanently, which would pose a clear challenge to security related applications [30]. For example, an attacker could enter the house where the sensor is kept and detect inherent electronic or physical sensor signals through the use of signal-detection equipment with the signals being radio, heat, magnetic, visual, and other electronic signals. The attacker could then determine where the sensors are positioned based on the properties of received signals, after which they may physically disable, destroy, or steal it. Physical destruction could be accomplished using heat, physical force, or tampering with the circuit on the sensors, rendering the sensor non-functional. In addition, it is easy to launch physical attacks using low technology and effort and the ease of executing such an attack, along with the vulnerability of sensors, especially small-sized ones, to physical disabling or destruction makes this kind of attack inevitable for sensor networks in the IoT. Because the attacker is in close proximity to the*

Copyright © 2015 Helvetic Editions LTD - All Rights Reserved

sensor network in this kind of attack, they have opportunities to react to defense mechanisms applied by the owner, unlike such attacks as eavesdropping [30].

VII. CONCLUSIONS AND FUTURE WORK

This study has explored various challenges and weaknesses of IoT technology use, especially as they continue to pervade everyday life. From the results of the study, it is evident that, while the IoT will make life easier, there are significant challenges in its use. One of these challenges has to do with DoS of attacks in a distributed architecture approach, which can be used by blackmailers and activists to hijack unsecured network devices like sensors and routers and using them as bots to attack third parties. Due to the high number of devices under risk of a DDoS attack, coupled with the fact that these remote devices are less likely to be properly secured and managed, they are easy to exploit. Another challenge has to do with eavesdropping over the IoT network, especially as attackers could target communication channels to extract information and data from the flow of information. In addition, it was also found that node capture is a threat to the IoT; particularly where node resources are limited, where there is a distributed organized structure, and a dynamic change in network typology. The perceptual layer results in various threats, including physical capture, brute force attack, DoS attacks, and node privacy leaks. Finally, physical attacks on the sensors could also threaten to bring down the entire sensor network by destroying, disabling, or stealing the sensors.

One future research of this study would be to investigate how the challenges identified in this study can be countered to make the IoT safer and more secure. The research could also move in the direction of investigating the feasibility of immersive technologies in the IoT, such as the ability of IoT to function through gesture recognition and augmented reality in seeking to achieve safety.

REFERENCES

[1] O. Hersent, D. Boswarthick, and O. Elloumi, *The Internet of Things: Key applications and protocols*. Hoboken: John Wiley & Sons, 2011

[2] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, Smart objects as building blocks for the Internet of Things. *IEEE Internet Computing, 14*(1), 44-51, 2010

[3] H. Ning and S. Hu, Technology classification, industry, and education for future Internet of Things. *International Journal of Communication Systems, 25*(9), 1230-1241, 2012

[4] M. Kranz, P. Holleis, and A. Schmidt, Embedded interaction: Interacting with the Internet of things. *IEEE Internet Computing, 14*(2), 46-53, 2010

[5] K, Karimi, *What the Internet of Things (IoT) needs to become a reality*. 2014, Available http://www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf, [Accessed 24 September, 2014]

[6] Goldman Sachs. The Internet of Things: Making sense of the next mega-trend. 2014, Available http://www.goldmansachs.com/our-thinking/outlook/Internet-of-things/iot-report.pdf. [Accessed 24 September, 2014]

[7] D. Evans. The Internet of Things: How the next evolution of the Internet is changing everything. 2014, Availablehttp://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. [Accessed 24 September, 2014]

[8] Parametric Technology Corporation. *The Internet of Things: How a world of smart, connected products is transforming manufacturers*. 2014, Available http://www.ptc.com/File%20Library/About%20PTC/Manufacturing%20Transformation/PTC_Impact_of_IoT_on_Manufacturers_eBook.pdf, [Accessed 14 September, 2014]

Copyright © 201 Helvetic Editions LTD - All Rights Reserved

[9] D. Miorandi, S. Sicari, P. De, and I. Chlamtac, Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497-1516, 2012

[10] L. Tan and N. Wang, Future Internet: The Internet of Things. *Advanced Computer Theory and Engineering (ICACTE)*, *5*(1), 376-380, 2010

[11] R. Weber, Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30, 2010

[12] X. Zhou. Short sign-cryption scheme for the Internet of things. *Informatica, 35*(4), 521-530, 2011

[13] R. Roman, On the features and challenges of security and privacy in distributed Internet of things. *Computer Networks*, *57*(10), 2266-227, 2013

[14] R. Roman, P. Najera, and J. Lopez, Securing the Internet of things. *Computer*, *44*(1), 51-58, 2011

[15] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, From today's INTRAnet of things to a future Internet of things: A wireless- and mobility-related view. *Ieee Wireless Communications, 17*(6), 44-51, 2010

[16] P. Barnaghi, W. Wang, C. Henson, and K. Taylor, Semantics for the Internet of Things: Early progress and back to the future. *International Journal on Semantic Web and Information Systems (IJSWIS), 8*(1), 1-21, 2012

[17] L. Yan, L. *The Internet of things: From RFID to the next-generation pervasive networked systems*. New York: Auerbach Publications, 2012

[18] A. Bassi. *Enabling things to talk: Designing IoT solutions with the IoT architectural reference model*. Heidelberg: Springer, 2013

[19] H. Weber and R. Weber. *Internet of things: Legal perspectives*. Berlin: Springer, 2010

[20] S. Gaglio and R. Lo. *Advances onto the Internet of Things: How ontologies make the Internet of Things meaningful*. Cham: Springer, 2014

[21] D. Uckelmann, M. Harrison, and F. Michahelles, *Architecting the Internet of things*. Berlin: Springer, 2011

[22] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions.*Future Generation Computer Systems*, 29(7), 1645-1660, 2012

[23] Q. B. Sun, J. Liu, S. Li, C. Fan, and J. Sun, Internet of things: Summarize on concepts, architecture and key technology problem. *Beijing YoudianDaxueXuebao/journal of Beijing University of Posts and Telecommunications, 33*(3), 1-9, 2010

[24] K. Kotis and A. Katasonov. Semantic interoperability on the Internet of Things: The semantic smart gateway framework. *International Journal of Distributed Systems and Technologies (IJDST), 4*(3), 47-69, 2013

[25] X. Su, J. Riekki, J. Nurminen, J. Nieminen, and M. Koskimies, *Adding semantics to Internet of Things,*Hoboken: Wiley, 2014

[26] J. Lalchandani, (2013, December 26). The Internet of Things: How will this change our world as consumers? Gulf News [Online] Available http://gulfnews.com/business/technology/the-Internet-of-things-how-will-this-change-our-world-as-consumers-1.1271230 [Accessed September 24, 2014]

[27] abc12. Prodea to power the makook smart living connected life platform. Abc12.com [Online] Available http://www.abc12.com/story/26541592/prodea-to-power-the-makook-smart-living-connected-life-platform [Accessed: September 24, 2014]

[28] E. Babbie. *The practice of social research*. Belmont, USA: Wadsworth Gengage Learning, 2013

[29] M. Q. Patton. *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage, 2012

[30] S. Das, K. Kant, and N. Zhang, *Handbook on securing cyber-physical critical infrastructure: Foundation and challenges*. Waltham, MA: Morgan Kaufmann, 2012

Copyright © 2015 Helvetic Editions LTD - All Rights Reserved

AUTHORS' BIOGRAPHY

Ebraheim Alsaadi is a graduate student in the Master of Science in Information Technology (Specialization in Cyber Security) program at the College of Technological Innovation at Zayed University. His research interests include IoT and digital forensics.

Abdallah Tubaishat is an Associate Professor in the College of Technological Innovation at Zayed University, United Arab Emirates. He received his PhD in Software Engineering from Illinois Institute of Technology, IL, USA in 1994. Dr. Tubaishat has twenty years of experience in teaching and research. His teaching experience include: Software Engineering, Database and Programming, His research spans two main areas, one is technical: software engineering, and the other is non-technical: e-learning, and educational technology. He has published a book with others entitled "Computer Skills", and has around twenty three Journal and conference publications. Dr. Tubaishat served on the program and organizing committees of several international conferences and workshops.

Copyright © 201 Helvetic Editions LTD - All Rights Reserved