Security Considerations for the Adoption of IoT in Nigeria

Augustine O. Ugbari andBetty Ahubele
Department of computer Science, University of Port Harcourt, Choba, Nigeria
Email address: ugbari@gmail.com and betty4diamond2005@yahoo.com

Abstract: The Internet of Things has become a household name for future technology used to describe miniaturised and smart devices. It has gradually revolutionising the way in which enterprises manage andis inevitably transforming the way we do things on the internet. This progress comes with a price as most of these IoT devices present security challenges we must be ready to overcome in Nigeria. We present in the paper an overview of the security changelings faced in the adoption of IoT in Nigeria and proposed key areas on how they can be resolved.

Keywords: Internet of Things, Security, Adoption

Introduction

The internet is awash with news, articles, and indeed advertisements all referring to the new Internet of Things. The technology, catalysed by the development of cheap computing electronics, as well as cheaper and more efficient communication technology, is making inroads and revolutionizing traditional models and platforms. It is viewed by some as the one-size-fits-all solution to diverse problem areas that have a common denominator - the need for better quality data generation and transmission. By ‘better quality’ we mean that the technology enables instant access to data at extremities of a system, what hitherto would be impossible to gather, or best case, take some delay to be aggregated. The Internet of Things allows us to deploy control elements as close to source as possible.

Several definitions of the Internet of Things technology exist. According to the website IoT Agenda, the Internet of Things (commonly abbreviated to IoT) is "a system of interrelated computing devices, mechanical and digital machines, objects, animals, etc. that are provided with unique identifiers and the ability to transmit data over a network without requiring human-to-human or human-to-computer interaction" [1]. The Internet Architecture Board (IAB) is quoted with this definition: "The term 'Internet of Things' denotes a trend where a large number of embedded devices employ communication services offered by the internet protocols. Many of these devices, often called 'smart objects', are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in the environment." The term was first used to describe a system in which objects in the physical world could be connected to the internet [2].

Technical Characteristics

Devices that qualify for the term IoT usually have the following characteristics:

Miniaturization: IoT-enabled devices need to retain the ability to perform their primary function. As mentioned previously, the technology is deployed in a

nearly invisible manner. It is not expected to add to the physical dimensions, or increase power requirements, or unduly modify the user experience in relation to its primary function. For example, an IoT-enabled door lock must remain able to fit in the space of traditional door locks, generally speaking. It must also not be very different as to make the process of locking a door more complicated than it is already.

Intelligence - Each individual unit is able to carry out basic data and signal processing, to provide some level of control or feedback to the system within which it is deployed, and to be able to process and transmit the inputs it receives.

Unique Identifier: Each unit is equipped with a unique identifier. IPv4 is nearing its limit for the number of available unique IP addresses. However, the advent of IPv6 has enabled even more massive network capability, where large numbers of devices can be uniquely addressed.

Communication: Each device has to be capable of transmitting and receiving data on a network. Several data transmission techniques exist currently which provide such services. Communication channels can be both wired or wireless. Wireless communication can be short-, medium- or long-range.

Applicability

The IoT technology has found application in several segments of society, providing always-on connectivity of previously impossible devices and 'things', and a very reliable channel for the monitoring and maintenance of such. In addition, it has enabled insight into patterns such as user acceptance and consumer behaviour, environmental conditions, state of structures, and essentially any measurement which trends over time are invaluable to interested parties. Below are a few examples of its application:

Health: The proliferation of smartwatches and other fitness devices points to the trend. Heart and other body system monitors are candidates for the IoT. Non-invasive sensors in hospitals, home care, etc. can also be implemented with the technology.

Home/Building automation and home appliances: Energy monitors and smart switches, security cameras and other sensors, smart locks, smart home appliances - refrigerators, cookers, etc.

Vehicles and Transportation: Safety, performance and condition monitoring, road and rail condition monitoring, geolocation, etc.

Commerce and Trade: sales and office inventory management, point-of-sale technology, condition monitoring and maintenance of appliances and equipment, equipment usage, package/shipment tracking, etc.

Agriculture and Environment: biochip transponders to monitor plants and animals, soil, water and air quality measurement, illumination, weather monitoring, etc.

Applicability in Nigeria

In the context of Nigerian society, the IoT technology can also find application in a number of sectors as well [3].

Traffic condition monitoring - IoT sensors can be installed on the streets in the cities to determine the status of traffic per time. This can serve as an early warning system for commuters, advising them of alternate routes, and reducing the overall severity of traffic jams. The sensors can also be an indication of the state of the roads.

Security coverage –CCTV cameras, drones, motion sensors, emergency radio/GPS beacons, etc. are all possible devices which can be deployed strategically in cities, and even remote locations, to help law enforcement agencies combat crime. These devices can provide coverage on a level which cannot be matched cheaply by other technology. Currently there are low-power versions of such devices in the market, therefore the energy constraint in Nigeria would not be much of a challenge.

Energy monitoring and smart meters – Nigeria currently generates far less energy than it needs. Even the power generated suffers wastage by users. Most of it is not paid for as a result of illegal connections. Smart metering and other energy monitoring technologies can be deployed to enable efficient energy distribution and accountability, as well as proper load balancing, such that the available energy is utilized efficiently. Additionally, IoT devices can be deployed in alternative energy systems, for the purposes of billing, monitoring and maintenance.

Environmental condition monitoring – Environmental issues are very sensitive in the country currently - from the petroleum pollution in the Niger Delta up to the heavy metal pollution in the gold mines in the mid-belt and on to the fringes of the Sahara exposed to desert encroachment. IoT devices designed for environmental monitoring can serve as a warning system to the government of any impending ecological issues in the affected regions.

Package/Shipment tracking –Logistics is still a challenge in Nigeria. IoT devices can be of use by courier companies (and indeed any organization that transports goods or equipment) to track their packages in real time and ensure they are not tampered with or diverted from the intended destination.

In certain quarters, initiatives are already in progress to determine implementation plans and roadmaps [4].

Security Issues

With all of its advantages, and as with all technology in general, the IoT technology comes with its own set of challenges. One of the key challenges has to do with information security. By design, the IoT technology is set up in a position to collect a lot of data and information in a transparent (almost stealthy) mode. Users, to a large extent are unaware of, or unable to exercise control over the decisions around, or the frequency of, the data transmissions. Users are also largely unaware of the content of data, and how it is used at the end-points [5]. This presents a series of questions: how safe is all this information? What is it being used for? In the following paragraphs, we will address different security risk areas, and their relevance in Nigeria.[6]

Unauthorised Remote Control: IoT devices, if compromised, can provide a gateway for malicious agents to control sensitive equipment or appliances. Several scenarios exist wherein this would be a

critical breach of security or safety. IoT enabled cars, whether human- or self-driven can result to serious auto accidents if their controllers are compromised.

User or Business Data Theft: IoT devices are designed to be so ubiquitous and invisible to users that they are positioned to collect personal data on an unprecedented level. This data in the wrong hands can be used to implement identity theft scams, or other criminal activities. In addition, it may expose the users to more significant losses if confidential information is released to unauthorised persons. In the deployment of IoT for business purposes, such a breach can result in litigation or fines, withdrawal of trust and reputational damage to the companies.

Reprogramming: Compromised devices can be used as a platform to launch further attacks on networks or systems. As a result of the availability of a large number of identical devices, it is quite easy for an attacker to create an army of 'bots' with which to launch DoS attacks or other large-scale IT Security compromises (e.g. spambots, etc.). The ‘mirai’ botnet incident of 2016 [7] is a good example – CCTV cameras and video recorders were used in this case.

All of the above, plus other possible 'normal' security challenges are even more amplified for the following reasons:

IoT devices are designed to be deployed at a very large scale. This means that the size of the network also tends to be within such orders of magnitude. They are also designed to be identical in design. The effect of this is that a security breach when exploited can very quickly escalate through the population of deployed devices.

IoT devices are usually designed without the intention for upgrade. The devices may be installed in physically inaccessible locations, or be too strongly integrated within the systems that updates or upgrades could be quite difficult and expensive to deploy. As a result, even when security patches are available, there is a high probability that less than 100% will be patched. A security breach can remain unresolved for quite a long time.

Specific Local Challenges and Possible Solutions

Education & Awareness–As with the ‘regular’ IT Security issues, education and awareness is critical to managing and reducing security exposure of users and manufacturers alike. Digital illiteracy has been identified as a factor militating against IoT adoption in Nigeria [3]. Most non-tech oriented users in Nigeria are unaware of the concept of IoT and its implications. The net effect of this, if unchecked, is the prevalence of risky behaviour among users of IoT enabled technology. Risky behaviours include use of default passwords, weak passwords, delay of, or inability to apply patches and updates, etc. Users may even be unable to detect when their devices begin to malfunction or function abnormally.

Mirai-like events can happen with devices in Nigeria, if users are not educated enough to apply patches and updates regularly. According to the article, “IP addresses of Mirai-infected devices were spotted in 164 countries … appearing even in such remote locations as Montenegro, Tajikistan and Somalia.”[7] In fact, a smart

attacker would look to recruit bots in places where the awareness levels are low, because the probability of finding vulnerable devices will be much higher in such regions.

Internally too, a knowledgeable attacker could take advantage of compromised systems for personal gain. For example, if an IoT device holds Wi-Fi access keys in plaintext, a hacker can access an otherwise secure network if he can access that single device. Also, hacking into security cameras installed in homes can give an attacker footage with which to either monitor with malicious intent, or blackmail innocent users.

Educational campaigns in universities and secondary schools, as well as Public orientation can help draw the minds of users to such dangers, and the mitigations thereof.

Concluding Remark

The increasing usefulness of IoT and it contributions to technological development requires that Nigeria takes advantage of these advances in other to become a developed Nation. With the proper adoption of IoTin Nigeria insecurity and the poor standard of leaving would inevitably be resolved. However, fundamental issues like stable power supply and information technology orientation are required to actualise these objectives.

Contribution to Knowledge

IoT security issues can be broadly categorised into two main groups, devices vulnerability and Human/Social inadequacies. To address this challenges it is recommended that:

- Regulatory bodies in Nigeriashould ensure that defined standards are adequately met and evolving challenges are resolved on time.
- Fundamental design re-engineering may be required to handle technological challenges like securely and remotely updating IoT devices or the effective encryption techniques that are robust, fast and small.

For IoT to be adopted effectively, Government policies should support and aid it advancement in the society. This would include funding and policy enforcement.

References

[1] I. Wigmore, “Internet of Things (IoT),” Internet of Things (IoT) Internet of Things (IoT) Wigmore, I.. [Online]. Available: http://whatis.techtarget.com/definition/Internet-of-Things. [Accessed 28 1 2017].

[2] M. DeCesare, “ForeScout IoT Enterprise Risk Report,” ForeScout Technologies, Inc, 2016.

[3] F. . Mattern and C. . Floerkemeier, “From the Internet of Computers to the Internet of Things,” *Informatik-Spektrum*, vol. 33, no. 2, p. 107–121, Informatik-Spektrum Informatik-Spektrum Mattern, Friedemann; Floerkemeier, Christian.

[4] N. . Kushalnagar, G. . Montenegro and C. . Schumacher, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals,” *Ietf Rfc 4919*, vol. Ietf Rfc 4919, no. Ietf Rfc 4919, p. Ietf Rfc 4919, Ietf Rfc 4919 Ietf Rfc 4919 Kushalnagar, N.; Montenegro, G.; Schumacher, C..

[5] “The Internet of Things: An Overview,” [Online]. Available: https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.

[6] “Breaking Down Mirai: An IoT DDoS Botnet Analysis,” [Online]. Available: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

[7] D. Palmer, “Internet of Things security: What happens when every device is smart and you don't even know it?,” 20 March 2017. [Online]. Available: http://www.zdnet.com/article/internet-of-things-security-what-happens-when-every-device-is-smart-and-you-dont-even-know-it/.

[8] Maryleen Ndubuaku, David Okereafor, “State of IoT Deployment in Africa and its Future: The Nigerian Scenario,” *The African Journal of Information and Communication*, vol. 2015, no. 15, pp. 114-119, January 2015.

[9] Obodoeze Fidelis Chukwujekwu; Odegwo James Ifeanyi; Obiokafor Ifeyinwa Nkemdilim, “IoT in 2016: The implementation Roadmap for Nigeria,” *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 6, June 2016.

[10] Ovidiu Vermesan; Peter Friess, “IoT Governance, Privacy and Security Issues,” European Commission, Information Scociety and Media, 2015.