Survey on IoT Prevalence and Security Issues

Sriram V Ramaswamy
School of Computing and Information Technology
REVA University
Bengaluru, India
sriram.rmswmy@gmail.com

Shah Abdul Ghani
School of Computing and Information Technology
REVA University
Bengaluru, India
gshahabdul@gmail.com

Sumukha K V
School of Computing and Information Technology
REVA University
Bengaluru, India
kvsumukha@gmail.com

Ravish Ahmad
School of Computing and Information Technology
REVA University
Bengaluru, India
ravishahmad@gmail.com

Kiran M
School of Computing and Information Technology
REVA University
Bengaluru, India
kiranm@reva.edu.in

***Abstract*—This paper outlines the prevalence and future trends in the use of Internet of Things [IoT] devices in everyday use, as well as the common connectivity and security issues associated with such devices. This data can then be used to build a secure and privacy-upholding system.**

***Keywords*—IoT Prevalence, Security Issues, Obsolescence**

I. Introduction

The rise of computing power has brought about rapid growth in devices deemed ”computing-capable” which has in turn led to the birth of ”The Internet of Things”. This led to the connectivity of unconventional devices such as light bulbs and refrigerators with the internet. In a very short time, the growth of IoT devices has been exponential, and is only expected to rise in the future.

The rise of ubiquitous connectivity has its set of complications as well. These devices need perpetual connectivity as well as dependable power supply in order to function to their potential. Thus, it is important to identify the issues as well as possible solutions to these problems.

II. The Growth of IoT Devices

IoT devices have grown exponentially in numbers in all fields, from domestic uses to industry applications. The number of IoT devices in 2020 is predicted to be in the vicinity of 32 billion, over double that of the number of devices in 2015 [15 billion]. However, it is not the number of IoT devices alone that are rising, the rise in communications between these devices have risen exponentially as well. For instance, while the human-to-device data consumption is expected to rise by around 200% to 1,000 Zettabytes a year, the device-to-device data consumption is expected to rise by nearly 1.5 million percent, from a relatively paltry 5 Zettabytes to 100,000 Zettabytes between 2015 and 2025 [1].

A. Consumer IoT Devices

Standalone IoT devices are generally used by electronics hobbyists in order to automate tasks such as weather reporting, home surveillance, ad Blockers, as well as mobile robots and devices that interface with software services [2][3]. Such rudimentary devices are the main powerhouse for the approximately 5.2 billion consumer devices that are prevalent worldwide and are expected to rise to nearly 12.8 billion by 2020 [4].

The ubiquity of these IoT devices reaches far outside the domestic sphere. Consumer IoT devices are regularly used in commercial applications as well, such as healthcare, automotive and retail, which alone account to over $1,000 trillion in potential economic value. Potential uses of such devices in these sectors include early weight gain detection and autonomous vehicle control in order to reduce hospitalization by and car accidents respectively upto forty percent [1].

B. Enterprise IoT Devices

Some enterprises require the use of specialized IoT devices that need to be built in order to perform a specific task. They differ from conventional embedded systems in the fact that they require internet connectivity in order to function as a collective unit, instead of standalone units. The Public Sector, Agriculture, and Infrastructure fields themselves amount to nearly $799 trillion in user revenue. The use cases for these are air quality monitoring, operation scheduling, among others.

The uses of such devices is very helpful to industries, as efficient energy consumption can reduce pollution by upto twenty percent while operation scheduling can reduce downtime by half, while reducing maintenance by upto forty percent [1].

III. Issues in IoT Devices

As with any rapidly growing nascent technology, IoT is seen as a harbinger of change bringing the rise of a “smart world” for many [6], while it is also seen as a major privacy and security issue. These include growing concerns over surveillance, consumer lock-in, as well as reports of hacking of smart devices and potential misuse of private data [7].

These issues are wide-ranged, from extremely technical to essentially political [5].

When polled, UK-based individuals listed the following as the major security concerns they identified:

TABLE I. Identified major security concerns

Device-Level Vulnerabilities	87%
Compromised Data	81%
Asset Control	75%
Asset Management	39%

A. *Major Security Issues*

Security issues in IoT devices cover a wide spectrum, and are very important to consider. The security of a device in this case is dependent on the risk of compromise, as well as the robustness and resiliency of the device to withstand any attacks that might cause it to expose any potential exploits. The wide range of usage of such IoT devices is also a major issue; some devices essential to human survival, such as heart rate monitors, as well as industrial equipment, such as temperature controllers in high-risk storage facilities, can be compromised. However, not all devices are so vulnerable; the risk of a device being manipulated is reduced in other devices, say, a refrigerator. It is worth noting that the lowered security of a device is also detrimental to the overall resiliency of the entire network [5].

The unconventional mix of ubiquity and diversity of IoT devices leads to a whole new spectrum of challenges that must be considered for anyone attempting to scale something of this type. They are:

- Sensors and other consumer items are linked together at such a massive scale that predicting the magnitude and fashion of connectivity is almost impossible to determine. Any methodology that must tackle this must take this unpredictability factor into account.
- The ubiquity and homogeneity of such devices can potentially magnify and exacerbate any vulnerabilities found in devices. Some devices might be prevalent for a longer time period than their developer organizations, making source code availability or reconfiguration impossible. Unlike conventional computers that receive software updates, IoT offers a significant challenge for those wanting to secure these devices.
- More complex IoT devices are an amalgamation of many smaller IoT components, or merely extensions of other similar devices. This can lead to a vulnerability in one device directly affecting the security of another. Thus, the number of affected devices can balloon to the point where a majority of devices might have to be recalled.
- Planned obsolescence [8] and cumbersome upgrade processes mean that any patches or bug fixes have to be upgraded with the assistance of technologically adept consumers/professionals only. This lack of user-friendliness can cause users to avoid upgrading altogether, leaving the security issue unfixed.
- With IoT devices working at the hardware level with very little user knowledge of the actual process, issues and malfunctioning can be hard to determine exactly, causing the debug and fixing process to extend longer than anticipated. Malevolent manufacturers can also use spyware and backdoors without the users’ knowledge.
- IoT devices may be placed in hard-to-reach places such as ceilings and roofs, meaning that physical security is hard to maintain, requiring preemptive measures and sturdy design before deployment.
- Some devices like environmental sensors might have to seamlessly blend in with their environment in order to avoid changing their surroundings. This can include inadequate alert mechanisms which can lead to prolonged threats that might have reached their full potential before any action is taken.
- The rise of “Build Your Own Device” machines has caused hobbyists to enter the mainstream, and many of homemade devices might not meet human standards.

B. *Tackling Security Issues*

Security issues in IoT devices make us ask the following questions:

1) Good Design Practices: It is important to build devices that are functionally adequate for present-day usage but can also scale vertically for future requirements. These must also be easily understandable and well-documented to allow sufficient propagation of development knowledge and easy debugging.

2) Security vs Economic Liability: One must consider the economic effects of security while determining how much should be spent on the securit aspect of the device. A very basic device that indicates the number of people in a room does not require the same level of security a thermostat in a backup facility requires.

3) Standardization: What aspects of the device must be standardized? What mustn’t? How can one standardize the security performance of the IoT device? These are questions that must be answered, as non-standardization can cause interfacing very cumbersome and wasteful, while standardization can magnify the negative effects of any vulnerability. This makes it important for developers to effectively balance the two while attempting to build a secure device.

4) Data Confidentiality and Credibility: Encryption is a resource-intensive process that might not be appropriate for IoT devices. However, the nature of IoT communications makes it important for the devices to be secure enough to prevent any eavesdropping or data misuse. The end-to-end processes must also be secure enough, while being simple enough.

5) Upgradeability: IoT devices must be built having two methods of upgradeability in mind: either by rapid development of newer boards and hardware that implements features out of the box or by usage of the same device that has the capability to interface any new features it comes across. While the first feature requires frequent replacements of devices, the second feature might require programming of higher complexity in order to account for future uses.

6) Legality and Policing: The onus of security must be determined between the end-user and the manufacturer. While some cases might be purely due to the lack of secure practices in the user's side, others might include overlooking and lack of foresight by the manufacturer. It is important to ensure that consumer protection and fundamental rights are maintained for all the entities involved.

7) Obsolescence: There is a definite shelf life for each device, and it is important to identify this shelf life after which the device becomes increasingly obsolete. After the device becomes obsolete, it becomes imperative to ensure that an upgrade happens, in order to respond to and combat against evolved forms of communication and threats.

C. Privacy Concerns

After device vulnerabilities, data leakage and access control are the most commonly identified threats in IoT devices, according to a survey [9]. These are privacy concerns that can include private and sensitive data of people. Thus, it becomes important to address such issues before they become too profound and problematic for effective solution. The considerations for privacy issues include:

1) Fairness in Data Usage: While companies usually record usage data for analytics and future development, one must consider what sort of data is being collected. Metadata and usage statistics can be considered acceptable, but the concern is over the collection of private and personal data which the end user might not wish to concede.

2) Transparency: Privacy Policies and Terms of Agreement should be accessible and transparent for end users. An effective model has to be developed in order to ensure that individual privacy concerns as well as privacy concerns of the masses are also addressed.

3) Design: It is important to design these devices such that privacy is maintained, not at just the hardware level, but at the software level as well. Customer privacy has to be considered in all areas of development and design.

IV. Social Implications of IoT

A. Uses of IoT in Society

The low cost and ubiquity of IoT devices make them very popular among those wishing to make their life easier by the use of some automations. However, it is important that these security and privacy concerns be addressed, atleast the society turn into a dystopian, autocratic society the likes portrayed in George Orwell's Nineteen Eighty Four [10]. The fact that IoT devices need to be secure is supported by the wide and implicating uses of such devices.

IoT devices are used in Environment monitoring by agglomerating data from large tracts of land using a cloud of such devices and sensors which in turn are analyzed in order to gain information about a wide range of issues from air quality control to animal movement tracking. Examples of these include Lion Tracking Collars, Air Quality Eggs and Insect Traps [11].

IoT devices are also used in Natural Disaster relief operations. These include collecting data from a wide array of sensors to determine the climatic and geological conditions before any disaster strikes and assisting rescue workers after the disaster has passed. These include tsunami and landslide warning systems that monitor subtle changes in the land, while meteorological warning systems monitor changes in the weather patterns.

In an urban environment, IoT devices form the heart of smart waste bins, smart streetlamps and public transport systems. Domestic use of IoT implies remote control of appliances such as refrigerators and energy meters. On a larger scale, these devices can be used to determine power use and demand, such as smart grids.

At a more personal level, IoT devices are used by people in the form of heart monitors, wearable vitals monitors and automatic insulin pumps.

This wide usage of IoT devices means that any vulnerability in these devices can and will have the potential to wreak havoc on a domain that far surpasses the intended domain of the device. Thus, it is important that such use cases be considered before setting up a security model and privacy environment [11].

B. Why is it so important to consider these devices?

Security issues in any device are bad enough; these devices, however, are also very fundamental to society. The social and economic implications of a compromised device in this scenario could be huge, with potential effects possibly affecting even the hackers and malevolent entities negatively.

V. Conclusion

The prevalence and ubiquity of IoT devices in today's market means that any security or privacy issue has to be carefully looked into by taking in the varied use cases and effects that might extend well after the expected life of the threat. Careful consideration of these issues and effects will allow better development and usage.

References

[1] C. Ip, "The IoT opportunity: Are you ready to capture a once-in-a-lifetime value pool?", Hong Kong IoT Conference, 2016.

[2] "Top 10 Rasberry Pi Projects for Beginners", Lifehackr.com, 2017. [Online]. Available: https://lifehacker.com/top-10-rasberry-pi-projects-for-beginners-1791002723

[3] "Hackster.io – The Community dedicated to learning hardware", Hackster.io, 2017. [Online]. Available: https://www.hackster.io/arduino/projects

[4] "Gartner Says 8.4 Billion Connected", Gartner.com, 2017. [Online]. Available: https://www.gartner.com/newsroom/id/3598917

[5] K. Rose, S. Eldridge and L. Chapin, "The Internet of Things: An overview", Internet Society, 2015.

[6] Thierer, Adam and Andrea Castillo, "Projecting the Growth and Economic Impact of The Internet of Things", George Mason University, Mercatus Center, 2015.

[7] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway With Me in It", WIRED, 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[8] "Planned Obsolescence", The Economist, 2009. [Online]. Available: https://www.economist.com/node/13354332

[9] K. Kessinger and S. Bosco, "IT Risk/Reward Barometer", ISACA, 5-9, 2016.

[10] G. Orwell, *Nineteen Eighty Four*, London, 1949.

[11] M. Botterman, *Policy Paper on IoT Future Technologies*.