International Journal of Engineering and Techniques - Volume 4 Issue 1, Jan – Feb 2018

RESEARCH ARTICLE OPEN ACCESS

INTERNET OF THINGS (IoT) : AN OVERVIEW OF SECURITY CONCERNS

M.N.Nachappa [1], M. C. Aparna[2], M.N.Varun Somanna[3]

[1]Associate Professor, Department Of Computer Science, St. Joseph's College (Autonomous),

[2]Assistant Professor, Department Of Computer Science, St. Joseph's College (Autonomous),

[3]Scholar,Department Of Computer Science, St. Joseph's College (Autonomous),

Langford Road, Shanthinagar, Bangalore – 560027, India.

Abstract:

The concept of combining computers, sensors, and networks to monitor and control devices has been around for decades, the recent confluence of key technologies and market trends is ushering in a new reality for the "Internet of Things''. IoT promises to usher in a revolutionary, fully interconnected "smart" world, with relationships between objects and their environment and objects and people becoming more tightly intertwined. The prospect of the Internet of Things as a ubiquitous array of devices bound to the Internet might fundamentally change how people think about what it means to be "online". While the potential ramifications are significant, a number of potential challenges may stand in the way of this vision – particularly in the areas of security. We discuss some of the issues related to this.

Keywords **—Internet of things (IoT), Security, Authentication.**

I INTRODUCTION

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the speciality press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. An abundance of conferences, reports, and news articles discuss and debate the prospective impact of the "IoT revolution"—from new market opportunities and business models to concernsabout security, privacy, and technical interoperability.

Figure-1 The Internet Of Things

The large-scale implementation of IoT devices promises to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the "smart home'', offering more security and energy efficiency.

Other personal IoT devices like wearable fitness and health monitoring devices and network enabled medical devices are transforming the way healthcare services are delivered. This technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels of independence and quality of life at a reasonable cost. IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges move us closer to the idea of "smart cities'', which help minimize congestion and energy consumption. IoT technology offers the possibility to transform agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors. However, IoT raises

many issues and challenges that need to be considered and addressed in order for potential benefits to be realized.

Fundamentally, the Internet Society cares about the IoT as it represents a growing aspect of how people and institutions are likely to interact with the Internet in their personal, social, and economic lives. If even modest projections are correct, an explosion of IoT applications could present a fundamental shift in how users engage with and are impacted by the Internet, raising new issues and different dimensions of existing challenges across user/consumer concerns, technology, policy and law. IoT also will likely have varying consequences in different economies and regions, bringing a diverse set of opportunities and challenges across the globe.

II PERSPECTIVES OF IoT

The Internet of Things engages a broad set of ideas that are complex and intertwined from different perspectives. Key concepts that serve as a foundation for exploring the opportunities and challenges of IoT include:

- **IoT Definitions:** The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition.
- **Enabling Technologies:** The concept of combining computers, sensors, and networks to monitor and control devices has existed for decades. The recent confluence of several technology market trends, however, is bringing the Internet of Things closer to widespread reality. These include Ubiquitous Connectivity, Widespread Adoption of IP-based Networking, Computing Economics, Miniaturization, Advances in Data Analytics, and the Rise of Cloud Computing.
- **Connectivity Models**: IoT implementations use different technical communications models, each with its own characteristics. Four common communications models described by the Internet Architecture Board include: Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing. These models highlight the flexibility in the ways that IoT devices can connect and provide value to the user.
- **Transformational Potential:** If the projections and trends towards IoT become reality, it may force a shift in thinking about the implications and issues in a world where the most common interaction with the Internet comes from passive engagement with connected objects rather than active engagement with content. The potential realization of this outcome – a "hyper connected world" – is testament to the general-purpose nature of the Internet architecture itself, which does not place inherent limitations on the applications or services that can make use of the technology.

III SECURITY CONSIDERATIONS IN IoT

When thinking about Internet of Things devices, it is important to understand that security of these devices is not absolute. IoT device security is not a binary proposition of secure or insecure. Instead, it is useful to conceptualize IoT security as a spectrum of device vulnerability. The spectrum ranges from totally unprotected devices with no security features to highly secure systems with multiple layers of security features. In an endless cat-and-mouse game, new security threats evolve, and device manufacturers and network operators continuously respond to address the new threats.

Figure-2 The IOT Security Challenges

The overall security and resilience of the Internet of Things is a function of how security risks are assessed and managed. Security of a device is a function of the risk that a device will be compromised, the damage such compromise will cause, and the time and resources required to achieve a certain level of protection. If a user cannot tolerate a high degree of security risk as in the case of the operator of a traffic control system or person with an implanted, Internet-enabled medical device, then we may feel justified in spending a considerable amount of resources to protect the system or device from attack. Likewise, if she is not concerned that her refrigerator might be hacked and used to send spam messages, then she may not feel compelled to pay for a model that has a more sophisticated security design if it makes the device more costly or complicated.

Several factors influence this risk assessment and mitigation calculation. Factors include having a clear understanding of the present security risks and the potential future risks; the estimated economic and other costs of harm if the risks are realized; and the estimated cost to mitigate the risks.58 While these kinds of security trade-offs are often made from an individual user or organizational perspective, it is also important to consider the interrelatedness of IoT devices as part of a larger IoT ecosystem. The networked connectivity of IoT devices means that security decisions made locally about an IoT device can have global impacts on other devices.

As a matter of principle, developers of smart objects for the Internet of Things have an obligation in ensuring that those devices do not expose either their own users or others to potential harm. As a matter of business and economics, vendors have an interest in reducing their cost, complexity, and time to market. For example, IoT devices that are high–volume, low–margin components that already represent a cost added to that of the product in which they are embedded are becoming quite common; adding more memory and a faster processor to implement security measures could easily make that product commercially uncompetitive.

In economic terms, lack of security for IoT devices results in a negative externality, where a cost is imposed by one party (or parties) on other parties. A classic example is pollution of the environment, where the environmental damage and clean-up costs (negative externalities) of a polluter's actions are borne by other parties. The issue is that the cost of the externality imposed on others is not normally factored into the decision-making process, unless, as is the case with pollution, a tax is imposed on the polluter to convince him to lower the amount of pollution. In the case of information security, as discussed by Bruce Schneier, an externality arises when the vendor creating the product does not bear the costs caused by any in security in this case, liability law can influence vendors to account for the externality and develop more security products.

These security considerations are not new in the context of information technology, but the scale of unique challenges that can arise in IoT implementations, as described below, make them significant.

IV UNIQUE SECURITY CHALLENGES OF IOT DEVICES

IoT devices tend to differ from traditional computers and computing devices in important ways that challenge security:

- Many Internet of Things devices, such as sensors and consumer items, are designed to be deployed at a massive scale that is orders of magnitude beyond that of traditional Internet-connected devices. As a result, the potential quantity of interconnected links between these devices is unprecedented. Further, many of these devices will be able to establish links and communicate with other devices on their own in an unpredictable and dynamic fashion. Therefore, existing tools, methods, and strategies associated with IoT security may need new consideration.
- Many IoT deployments will consist of collections of identical or near identical

devices. This homogeneity magnifies the potential impact of any single security vulnerability by the sheer number of devices that all have the same characteristics. For example, a communication protocol vulnerability of one company's brand of Internet-enabled light bulbs might extend to every make and model of device that uses that same protocol or which shares key design or manufacturing characteristics.

- Many Internet of Things devices will be deployed with an anticipated service life many years longer than is typically associated with high-tech equipment. Further, these devices might be deployed in circumstances that make it difficult or impossible to reconfigure or upgrade them; or these devices might outlive the company that created them, leaving orphaned devices with no means of long-term support. These scenarios illustrate that security mechanisms that are adequate at deployment might not be adequate for the full lifespan of the device as security threats evolve. As such, this may create vulnerabilities that could persist for a long time. This is in contrast to the paradigm of traditional computer systems that are normally upgraded with operating system software updates throughout the life of the computer to address security threats. The long-term support and management of IoT devices is a significant security challenge.
- Many IoT devices are intentionally designed without any ability to be upgraded, or the upgrade process is cumbersome or impractical. For example, consider the 2015 Fiat Chrysler recall of 1.4million vehicles to fix a vulnerability that allowed an attacker to wirelessly hack into the vehicle. These cars must be taken to a Fiat Chrysler dealer for a manual upgrade, or the owner must perform the upgrade themselves with a USB key. The reality is that a high percentage of these autos probably will not be upgraded because the upgrade process presents an inconvenience for owners, leaving them perpetually vulnerable to cyber security threats, especially when the automobile appears to be performing well otherwise.
- Many IoT devices operate in a manner where the user has little or no real visibility into the internal workings of the device or the precise data streams they produce. This creates security vulnerability when a user believes an IoT device is performing certain functions, when in reality it might be performing unwanted functions or collecting more data than the user intends. The device's functions also could change without notice when the manufacturer provides an update, leaving the user vulnerable to whatever changes the manufacturer makes.
- Some IoT devices are likely to be deployed in places where physical security is difficult or impossible to achieve. Attackers may have direct physical access to IoT devices. Anti-tamper features and other design innovations will need to be considered to ensure security.
- Some IoT devices, like many environmental sensors, are designed to be unobtrusively embedded in the environment, where a user does not actively notice the device nor monitor its operating status. Additionally, devices may have no clear way to alert the user when a security problem arises, making it difficult for a user to know that a security breach of an IoT device has occurred. A security breach might persist for a long time before being noticed and corrected if correction or mitigation is even possible or practical. Similarly, the user might not be aware that a sensor exists in her surroundings, potentially allowing a security breach to persist for long periods without detection.• Early models of Internet of Things assume IoT will be the product of large private and/or public technology enterprises, but in the future "Build Your own Internet of Things" (BYIoT) might become more commonplace as exemplified by the growing Arduino and Raspberry Pi60 developer communities. These may or may

not apply industry best practice security standards.

V IOT SECURITY QUESTIONS

A number of questions have been raised regarding security challenges posed by Internet of Things devices. Many of these questions existed prior to the growth of IoT, but they increase in importance due to the scale of deployment of IoT devices. Some prominent questions include:

a) **Good Design Practices.** What are the sets of best practices for engineers and developers to use to design IoT devices to make them more secure? How do lessons learned from Internet of Things security problems get captured and conveyed to development communities to improve future generations of devices? What training and educational resources are available to teach engineers and developers more secure IoT design?

b) **Cost vs. Security Trade-Offs.** How do stakeholders make informed cost-benefit analysis decisions with respect to Internet of Things devices? How do we accurately quantify and assess the security risks? What will motivate device designers and manufacturers to accept additional product design cost to make devices more secure, and, in particular, to take responsibility for the impact of any negative externalities resulting from their security decisions? How will incompatibilities between functionality and usability be reconciled with security? How do we ensure IoT security solutions support opportunities for IoT innovation, social and economic growth?

c) **Standards and Metrics**. What is the role of technical and operational standards for the development and deployment of secure, well-behaving IoT devices? How do we effectively identify and measure characteristics of IoT device security? How do we measure the effectiveness of Internet of Things security initiatives and countermeasures? How do we ensure security best practices are implemented?

d) **Data Confidentiality, Authentication and Access Control.** What is the optimal role of data encryption with respect to IoT devices? Is the use of strong encryption, authentication and access control technologies in IoT devices an adequate solution to prevent eavesdropping and hijacking attacks of the data streams these devices produce? Which encryption and authentication technologies could be adapted for the Internet of Things, and how could they be implemented within an IoT device's constraints on cost, size, and processing speed? What are the foreseeable management issues that must be addressed as a result of IoT-scale cryptography? Are concerns about managing the crypto-key lifecycle and the expected period during which any given algorithm is expected to remain secure being addressed? Are the end-to-end processes adequately secure and simple enough for typical consumers to use?

e) **Field-Upgradeability.** With an extended service life expected for many IoT devices, should devices be designed for maintainability and upgradeability in the field to adapt to evolving security threats. New software and parameter settings could be installed in a fielded IoT device by a centralized security management system if each device had an integrated device management agent. But management systems add cost and complexity; could other approaches to upgrading device software be more compatible with widespread use of IoT devices? Are there any classes of IoT devices that are low-risk and therefore don't warrant these kinds of features? In general, are the user interfaces IoT devices expose (usually intentionally minimal) being properly scrutinized with consideration for device management (by anyone, including the user)?

f) **Shared Responsibility.** How can shared responsibility and collaboration for IoT security been courage across stakeholders?

g) **Regulation.** Should device manufacturers be penalized for selling software or

hardware with known or unknown security flaws? How might product liability and consumer protection laws be adapted or extended to cover any negative externalities related to the Internet of Things and would this operate in a cross-border environment? Would it be possible for regulation to keep pace and be effective in light of evolving IoT technology and evolving security threats? How should regulation be balanced against the needs of permission-less innovation, Internet freedom, and freedom of expression?

h) **Device Obsolescence.** What is the right approach to take with obsolete IoT devices as the Internet evolves and security threats change? Should IoT devices be required to have a built-in end-of-life expiration feature that disables them? Such a requirement could force older, non-interoperable devices out of service and replace them with more secure and interoperable devices in the future. Certainly, this would be very challenging in the open marketplace. What are the implications of automatic decommissioning IoT devices? The breadth of these questions is representative of the wide-ranging security considerations associated with Internet of Things devices. However, it's important to remember that when a device is on the Internet, it is also part of the Internet,61 which means that effective and appropriate security solutions can be achieved only if the participants involved with these devices apply a Collaborative Security approach.62The collaborative model has emerged as an effective approach among industry, governments, and public authorities to help secure the Internet and cyberspace, including the Internet of Things. This model includes a range of practices and tools including bidirectional voluntary information sharing; effective enforcement tools; incident preparedness and cyber exercises; awareness raising and training; agreement on international norms of behavior; and development and recognition of international standards and practices.

Continued work is needed to evolve collaborative and shared risk management-based approaches that are well suited to the scale and complexity of IoT device security challenges of the future.

VI CONCLUSION

While the concept of combining computers, sensors, and networks to monitor and control devices has been around for decades, the recent confluence of key technologies and market trends is ushering in a new reality for the "Internet of Things''. IoT promises to usher in a revolutionary, fully interconnected "smart" world, with relationships between objects and their environment and objects and people becoming more tightly intertwined. The prospect of the Internet of Things as a ubiquitous array of devices bound to the Internet might fundamentally change how people think about what it means to be "online".

While the potential ramifications are significant, a number of potential challenges may stand in the way of this vision – particularly in the areas of security; privacy; interoperability and standards; legal, regulatory, and rights issues; and the inclusion of emerging economies. The Internet of Things involves a complex and evolving set of technological, social, and policy considerations across a diverse set of stakeholders.

The Internet of Things is happening now, and there is a need to address its challenges and maximize its benefits while reducing its risks. The Internet Society cares about IoT because it represents a growing aspect of how people and institutions are likely to interact with and incorporate the Internet and network connectivity into their personal, social, and economic lives. Solutions to maximizing the benefits of IoT while minimizing the risks will not be found by engaging in a polarized debate that pits the promises of IoT against its possible, perils. Rather, it will take informed engagement dialogue, and collaboration across a range of stakeholders to plot the most effective ways forward.

VII REFERENCES:

[1] Lianos, M. and Douglas, M. (2000) Dangerization and the End of Deviance: The Institutional Environment. British Journal of Criminology, 40, 261-278. http://dx.doi.org/10.1093/bjc/40.2.261

[2] Ferguson, T. (2002) Have Your Objects Call My Object. Harvard Business Review, June, 1-7.

[3] Nunberg, G. (2012) The Advent of the Internet: 12th April, Courses.

[4] Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. (2011) Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. Advances in Internet of Things: Scientific Research, 1, 5-12. http://dx.doi.org/10.4236/ait.2011.11002

[5] Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of "Internet of Things". First International Conference on Security of Internet of Things, Kerala, 17-19 August 2012, 51-56. http://dx.doi.org/10.1145/2490428.2490435

[6] Biddlecombe, E. (2009) UN Predicts "Internet of Things". Retrieved July 6.

[7] Butler, D. (2020) Computing: Everything, Everywhere. Nature, 440, 402-405. http://dx.doi.org/10.1038/440402a

[8] Dodson, S. (2008) The Net Shapes up to Get Physical. Guardian.

[9] Gershenfeld, N., Krikorian, R. and Cohen, D. (2004) The Internet of Things. Scientific American, 291, 76-81. http://dx.doi.org/10.1038/scientificamerican1004-76

[10] Lombreglia, R. (2010) The Internet of Things, Boston Globe. Retrieved October.

[11] Reinhardt, A. (2004) A Machine-to-Machine Internet of Things.

[12] Graham, M. and Haarstad, H. (2011) Transparency and Development: Ethical Consumption through Web 2.0 and the Internet of Things. Research Article, 7.

[13] Jayavardhana, G., Rajkumar, B., Marusic, S. and Palaniswami, M. (2013) Internet of Things: A Vision, Architectural Elements, and Future Directions. Future Generation.

[14] Gigli, M. and Koo, S. (2011) Internet of Things, Services and Applications Categorization. Advances in Internet of Things, 1, 27-31. http://dx.doi.org/10.4236/ait.2011.12004 .