# Security Concerns in IoT

Rakesh Kumar, PG Department of Computer Science
Khalsa College for Women, Amritsar
*SOCIS, IGNOU*

**Abstract:** The Internet of Things has moved to its adolescence.It has been observed that the artificial intelligence is power, information security is the paradox and the concept of big data is new gold rush for the researchers and academicians. The information infrastructure is exposed to a variety of cyber threats resulting in loss of confidentiality, integrity and availability of data. The severity of cyber exploits is negatively affecting the protection confidence of information assets, likewise adequacy and effectiveness of cyber security people, process, policy, and technologies. Moreover, the average cost of a data breach is rising at rate of 15 percent with every passing year. These security threats are posing new problems for big data and IoT. It is, therefore necessary to design and implement security policies and guidelines well in advance for success of Internet of Things

Keywords: IoT, Security, Vulnerability, Threats

## 1. Introduction

The cyber security risk management consists of risk assessment, mitigation and evaluation. The cyber security risk management, framework can help to manage acceptable risks-controls adequate for the key mission security capabilities and assurance. The objective of cyber security risk management includes:

(1) The protection of information assets, users, systems, database and IT processes.
(2) Accurate and efficient decisions support.
(3) Adequate and effective information systems governance, risk management, and compliance.

The cyber security risk assessment consists of risk identification, risk analysis, and risk impacts. Cyber security ensures reliable risk-control over incidence response, disaster recovery, asset loss prevention and the protection of a good public reputation.

There is no single object that can be described as the IoT infrastructure. The existing structure is very complex, disparate systems and uneven networks. The IoT rollout will depend on internet hosts, network, cloud computing, and smart devices with embedded sensors, built-in artificial intelligence with millions of applications to support adoption of IoT. The IoT implementation challenge is the absence of truly global, integrated and homogeneous environments necessary to support all the IoT Platform.

### 1.1 The CPS Systems

The Cyber-physical systems (CPS) are smart network engineered systems that have inbuilt embedded sensors, processors, and actuators. The CPS is designed to detect physical and logical interaction anomaly and protect the physical world endpoints and the human users. The CPS assures real-time, guaranteed performance in the protection of critical applications and it depends on the seamless integration of computational algorithms and physical components. The advancement of current embedded systems and maturity of CPS technology should bridge the CPS interoperability gaps; improve the cyber security capability, adaptability, scalability, resiliency, safety, security, and usability that will super the simple embedded systems. In a CPS system, the joint behavior of the cyber interactions and physical elements, i.e. computing, control, sensing, and networking is integrated into every component.

### 1.2 The Challenges of Cyber-Physical Systems (CPS)

The CPSs ability to interface across different systems in a complex task is seen as a key challenge. Additionally, approaches to modularity that should enable reliable and verifiable assembly of individual CPSs into interacting systems of systems are needed. Another concern is the privacy of CPS Technologies, and other techniques that should enhance privacy and enable the appropriate use of sensitive and personal information while protecting personal privacy are currently not available. The demand for CPS open reference architectures and standards, model-based engineering methodologies, and powerful simulation, verification and validation tools, are essential for reducing the cost for CPS innovation and deployment because these deployments are not designed for interoperability across sectors or between communities, countries or regions.

In addition, the CPS is lagging behind because of the strong demand in smart systems being deployed to meet sector-specific challenges, for example (1) SCADA smart grid (2) disaster resilience (3) Smart buildings.

## 2. Best Practices for IoT Security

The adoption of the IoT cyber security best practices includes building reliable security into the IoT devices bottom up, rather than as an afterthought. The IoT cyber security design process, should consider:

(1) IoT privacy and security risk assessment methodology.
(2) Enforce minimum data collection and retention.
(3) Perform security testing before the launch of IoT products.
(4) Implement staff training over IoT good security.
(5) Ensure business partners enforce IoT security and reasonable oversight over the internet service providers.
(6) Implement IoT defense-in-depth approach.
(7) Implement reasonable access control to access key IoT device, data and network.
(8) Monitor IoT products throughout the life and patch known vulnerabilities.

## 3. Potential Risks due to Insecure Internet of Things

In this section, I have summed up the few risks that the world has to face if the progress of IoT is not aligned with security issues.

### 3.1 Walled off Internet

The rising number of cross border attacks will start pushing national governments towards breaking up the internet in national, or even regional “walled gardens.”

This will create major problems for the concept and practice of a global IoT, leading to the erection of barriers to the flow of content and transactions. Some might welcome a move towards a less hyper-globalized online world, but many would not, resistance would be likely, as would the rapid growth of illegal workarounds. The pace of technological development would slow and its trajectory would change.

### 3.2 Cloud Attacks

Given that a large amount of the data that will run the Io T will be stored in the cloud it is likely that cloud providers will be one of the principle targets in this kind of war. While there is growing awareness of this problem, cyber security is still under-resourced in comparison to the potential scale of the threat. To get some kind of idea of the problem, the World Economic Forum report cites analysis that suggests that the takedown of a single cloud provider could cause $50 billion to $120 billion of economic damage.

### 3.3 AI-Built Security Issues

Although the threat magnitude of ransom ware has already grown 35 times over the last year with ransom worms and other types of attacks, there is more to come. The next big target for ransom ware is likely to be cloud service providers and other commercial services with a goal of creating revenue streams.

The complex, hyper connected networks cloud providers have developed can produce a single point of failure for hundreds of businesses, government entities, critical infrastructures, and healthcare organizations. Polymorphic malware is not new, but it is about to take on a new face by leveraging AI to create sophisticated new code that can learn to evade detection through machine written routines.

### 3.4 Botnet Problems

Millions of new connected consumer devices open up a wide attack surface for hackers, who will continue to probe the connections between low-power; somewhat dumb devices and critical infrastructure.

The biggest security challenge is the creation of Distributed Destruction of Service (DDoS) attacks that employ swarms of poorly-protected consumer devices to attack public infrastructure through massively coordinated misuse of communication channels. IoT botnets can direct enormous swarms of connected sensors like thermostats or sprinkler controllers to cause damaging and unpredictable spikes in infrastructure use, leading to things like power surges, destructive water hammer attacks, or reduced availability of critical infrastructure on a city or state-wide level.

### 3.5 Limited AI

The current AI offerings on the market have substantial limits. After all, the machine learning and big data based AI that currently pervades are powerful tools for identifying associations in large quantities of data, but don't have much on humans in terms of working out the complex phenomena of cause and effect, or to identify modifiable factors that can engender desired outcomes.

As big data and machine learning powered AI's gains processing power, they can incorporate into their algorithms more and more information, more and more variables that may affect data associations. But with little human intervention, inevitably some variables may display strong correlation by pure chance, with little actual predictive effect.

### 3.6 Lack of Confidence

As per various reports, 90 percent of consumers lack confidence in the security of Internet of Things devices. This comes as more than two-thirds of consumers and almost 80% of organizations support governments getting involved in setting IoT security. The 96 percent of businesses and 90 percent of consumers believe there should be IoT security regulations. The 54 percent of consumers own an average of four IoT devices, but only 14 percent believe that they are knowledgeable on IoT device security. The 65 percent of consumers are concerned about a hacker controlling their IoT device, while 60 percent are concerned about data being leaked.

### 3.7 Understanding IoT

The real issue is how to increase the ability for people to understand the changes and their implications more clearly and to take concrete actions to take advantage of the potential upside. "The pace of change has exceeded the rate of human capability to absorb.

## 4. Conclusion

It can be concluded therefore that Internet of Things has moved to its adolescence. The connected devices have become smarter and more immersive and hence the expectations to convert IoT data to insights and financial value have increased subsequently. Also, algorithms and data visualization templates have smartly evolved. This evolution has also multiplied the magnitude of potential risks and threats to security of data stored under different clouds or other media. It is therefore a need of hour to develop new policies, guidelines and security algorithms that can counter the potential attacks on the IoT. The support of researchers, practitioners and private sector are anticipated to invent the new approaches to handle cyber security related issues and problems.

## References

[1]Cappos, J., Zhuang, Y., Oliveira, D., Rosenthal, M., & Yeh, K. (2014). Vulnerabilities as Blind Spots in Developers Heuristic-Based Decision-Making Processes.daniela.ece.ufl.edu.

[2]Juniper Research. (2013). Mobile Security: BYOD, mCommerce Consumer & Enterprise 2013.

[3]The National Science Foundation . (2015). Cybersecurity for the Internet of Things. Retrieved from http://www.nsf.gov/eng/iip/sbir/topics/it.jsp 9/24/2015.

[4] Xu, T., Wendt, J. B., & Potkonjak, M. (2014, November). Security of IoT systems: Design challenges and opportunities. In *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)* (pp. 417-423). IEEE.

[5] Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013, May). A systemic approach for IoT security. In *2013 IEEE international conference on distributed computing in sensor systems* (pp. 351-355). IEEE.

[6] Altolini, D., Lakkundi, V., Bui, N., Tapparello, C., & Rossi, M. (2013, July). Low power link layer security for IoT: Implementation and performance analysis. In *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 919-925). IEEE.

[7] Ramos, J. L. H., Bernabe, J. B., & Skarmeta, A. F. (2015, March). Managing context information for adaptive security in iot environments. In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops* (pp. 676-681). IEEE.

[8] Berhanu, Y., Abie, H., & Hamdi, M. (2013, September). A testbed for adaptive security for IoT in eHealth. In *Proceedings of the International Workshop on Adaptive Security* (pp. 1-8).

[9] Kozlov, D., Veijalainen, J., & Ali, Y. (2012, February). Security and privacy threats in IoT architectures. In *BODYNETS* (pp. 256-262).

[10] Bekara, C. (2014). Security issues and challenges for the IoT-based smart grid. *Procedia Computer Science*, *34*, 532-537.

[11] Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *2012 international conference on computer science and electronics engineering* (Vol. 3, pp. 648-651). IEEE.