Journal of Computational Science & Intelligent Technologies, eISSN: 2582-9041

Volume 1, Issue 2, pages: 01–08, September 2020

A Survey on Security Risks in Internet of Things (IoT) Environment

Mugesh Ravi

Faculty of Informatics, Eötvös Loránd University, Budapest, Hungary.

****Corresponding Author: mugesh.ravi@outlook.com***

Received: *27.06.2020,*
Revised: *20.07.2020,*
Accepted: *17.08.2020,*
Published: *31.09.2020*

DOI:
10.53409/mnaa.jcsit20201201

Abstract: This analysis reviews the management of vulnerabilities and security risks of Internet of Things (IoT). This paper provides an overview, which it reveals the recent Internet's growth and how it has transformed our lives in various, unforeseen dimensions and how it has given rise to IoT. The introduction part focuses on providing an analysis on literature by presenting a short IoT history, some technical information on security protocols, and IoT hardware problems. The section on survey is where similar literatures on specific concepts are reviewed by describing the vulnerabilities and threats of IoT systems, and then reviewed risk management mechanisms for both information technologies and information protection. After the review, the analysis and discussion segment addressed and evaluated the details contained in the literature review. In this paper, a new risk management strategy uniquely designed for each IoT system is proposed. Then proposed work is evaluated by discussing the advantages and concluded the analysis and the future work.

Keywords: IoT, Security, Threats, Vulnerability, Risk Management Framework

I. INTRODUCTION

The Internet is undoubtedly one of the greatest innovations of mankind. It has given us several benefits, which are nothing but a fantasy recently. It's difficult on its own to deliver a message to someone across the globe, so doing it in a few milliseconds was undoubtedly a wonder. Such technological innovation has, understandably, altered many facets of our lives. Newsletters, Radio stations, Cable TV, and postal mails are all been part of the history as they are alternated by podcasts, internet news, emails, and streaming services. Most of our daily tasks include utilizing the Internet in anyway, without even noticing it. The list doesn't even end here. Small, inexpensive, and often powerful appliances are built into our watches, TVs, refrigerators, and also toasters. They can be very easy, due to their wireless existence.

It is understood, however, that convenience is typically exchanged for protection. These devices also have very small processing and memory capacities and are regularly referred to as devices or IoT of the Internet of Things. It was estimated in a report by Cisco Inc. that the number of Internet-connected devices exceeded the people population back in 2008 and will cross more than fifty billion by 2020. This highlights the value of controlling these devices' security threats and vulnerabilities, as they are an incorporated segment of our daily lives. The issue with these systems was that frequently have very constrained capacities for storage and processing. This implies that, in most instances, they have limited tools necessary to create safe communication. This makes them unprotected to different forms of attacks, potentially placing the consumer at privacy loss risk. One might discuss that it was not just a losing our privacy term that we should think about if an IoT system is compromised. Since IoT devices are often used in very sensitive settings, such as healthcare, it may exactly be a subject of life or death to properly protect them.

For these and several other purposes, the significance of providing a tailored system for handling IoT's security vulnerabilities and risks is strongly emphasized.

IoT is not a modern idea. In reality, John Romkey presented the first IoT system at the

INTEROP conference in 1989. Like a toaster that might be remotely switched on or off using the Internet. It has been linked to the computer by a stack of TCP/IP network. This occurrence set off the development of IoT. Almost a decade later, LG unveiled the first Internet-linked fridge. Although the progress of the IoT domain appeared slow, it was the major milestones after the International Telecommunications Reunion (ITR) published the study on the subject in 2005. Thereafter, the IoT field has been progressing rapidly, and in late 2008, Cisco revealed the emergence of IoT when the devices or "things" was larger than the population [3].

Today, IoT was used in a different range of ways and is very common than ever before. Though, due to the design of the devices that require efficiency of power and a factor of compact form, IoT was typically constrained about for storage and processing capacities. This has desolate consequences concerning security because secure communication algorithm typically require more computational power to operate efficiently in right time. i.e., protocol such as SSL was a key way to secure the link, primarily by encryption. SSL use the RSA cryptosystem for providing the cryptographically safe link among both ends. RSA security depends on providing huge prime numbers for measuring both private and public keys. Those big keys use a lot of memory. Moreover, SSL additionally requires output and input buffers, which again absorb memory. The ATmega328 microprocessor has only 2k bytes of SRAM are simply not provided with sufficient memory for handling SSL, or TLS. This was just one of the threats and limitations related to IoT that should be handled to achieve the objectives of the organizations.

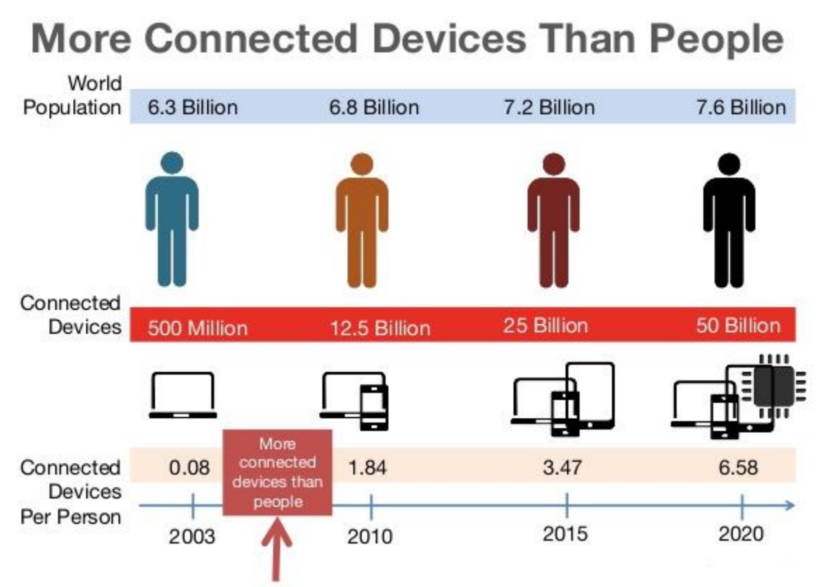

Figure.1. Growth of IoT

II. RELATED WORK

2.1. IoT Challenges

The management of the IoT threats and vulnerabilities was a hot field of research recently, the security issues are classified into four categories [4]:

Security issues in the application layer: involves security strategies such as trust establishment, resource exhaustion, etc.

Security issues in the architecture: often subject to application and domain scenarios.

Security issues in the communication: Responsible for the transmission of data within IoT devices or systems.

Security issues in the data protection: this was the weakest factor because the confidentiality of the data must be enclosed.

2.2. Transcending the IoT Threats

In order to resolve the threats, some literatures proposed the security architecture for securing the data flow of the smart grid in the home area network [5, 15], and the suggested architecture can effectively handle the transmission on the home area network through the non-confidential and confidential principles without damaging functionality of general home area. While additionally disuse the issues of IoT and some of the disadvantages, several suggestions came across, like [6]. IoT devices must have security development and all that relates to it. The problem on the network foundation, like the TCP/IP protocols, where the solution is to incorporate protection into the data flow itself with the sensing abilities of IoT device was addressed. Finally, protecting the link sources would ensure that the device was used safely. In addition, one of the results which [6] referred to was the IoT modules breakdown, which was listed as five main factors as follows:

Equipment or Device: which was incidental to the real device whether it is a sensor, or endpoint or even a washing machine.

Hub or Gateway: A method that can be utilized as a Bluetooth or Ethernet or wireless and etc.

Transport channels or Network, like the satellite and IP networks.

Facilitation: the capacity for transferring data via the gateways and many others, such as processing and analysis.

Application or Consumerization: The willingness of end-users for using details on their mobile phone, and etc.

Subsequently, [6] also lists some threats that were frequently related with IoT, like:

- Intensified Surface attack.
- Systems of legacy.
- Devices that are undetected, prohibited, and invalidated.
- Unauthorized remote access.
- Extensive exposure to sensitive data.

In addition, [6] additionally claimed that these threats must be addressed separately to be related to each other. That's why the CIA can be implemented in every unit. Also the Ubiquitous defense-in-depth strategy was stated in [6] which summarized in the following figure: which will allow the organization to incorporate and track the device security along with the activities and process for the device. It will also include each layer protection and few more technique that would support to accomplish the objectives and identify the threats. Another literature [7], discussed same threats, but also included others that were not addressed in [6]. This was due to the various techniques of identifying threats. So providing security or not it's not the case with [7] instead trying to secure the system in the network base that was part of the things which [6] has discussed, but [7] clarified why it was very important than trying to protect the device with a work strategy or just device on its own [7] stated that securing the IoT device makes it very helpful and appropriate for having an IoT system, like:

- Network Attacks
- Physical Attacks
- Encryption Attacks
- Software Attacks

Hence, to protect the IoT, these risks should be considered and each of the internal risks related to it, as the case of physical attacks on the basis of [7]:

- Node tempering: Which will physically or partially alters the node sensor so that it can provide consistent and direct system access.
- Interference of RF with RFIDs: Through transmitting radio signals to the IoT RFID devices as the DoS attack for generating noise to the device itself.
- Physical damage: damage to the real IoT system and this form of threat was primarily relevant to the protection of the location or building in which the IoT gadget was located [7]. In the other form of threat that is stated by [7] which was a network attack that was similar compared to [6], it actually varies in the form that the attack could occur and how an attack pattern is rendered. So there are more common threats to be prevented in the implementation of the IoT while dealing with particular network attacks.
- Traffic Analysis Attack: It was sniffling in the selected network and then implementing any analytical method utilizing specialized equipments for that purpose that was aimed at one of the things which claimed in [6], that was confidentiality and considered to be a backbone of security.

- Man in the middle attack: the kind of thing described in [6]. Through securing the network and having security protocols to secure the transmutation. However, [7] explicitly specifies what must be happen in the specified attack, how it could occur in this type of attack, where the man in middle was fixed trying to detect the transmission that was going on from the sender and the receiver side of the IoT device.

3.3. Systems review for risk management

Since the risks and vulnerabilities related to the IoT were identified, the literature on risk management can be reviewed. A special publication on the risk management of information technology systems has been published by the National Institute of Standards and Technology or NIST [1]. This publication describes risk management as a three-stage model. It begins by defining the risk, then evaluation, and in the end, by decreasing risk to the appropriate level. It is further noted that risk management helps IT professionals to accomplish the objectives of the organizations by determining a balance within operating costs, control costs, and incident costs.

Therefore, a well-designed risk management method can help to make decisions on the implementation of effective controls. What does the management execute when the residual was better than risk appetite? Hence, the publication noted that management must replicate the risk management iteration till the residual was below or similar to risk appetite. From this, the risk management was concluded as an ongoing procedure that was changing every time. While this work [1] offered the strong basis for process of risk managements, it was very broad and little out of date for present world. NIST, therefore, released a more detailed publication specifically customized to risk management of information security [2]. This work noted that process of risk management consists of four major elements:

- Assess risk.
- Frame risk.
- Monitor risk ongoing.
- Respond to risk.

The four factors and their association with each other are represented in the fig.2.

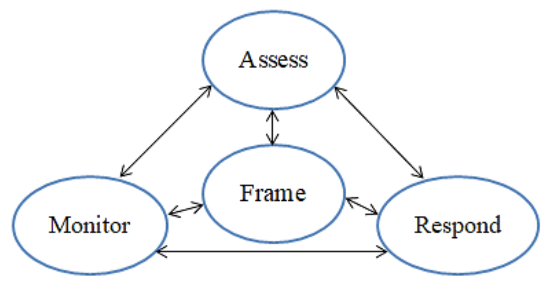

Figure.2. Risk Management Framework

The initial factor of risk management was risk framing. It discusses how organization builds the risk environments. This indicates that an organization must explicitly define a context in where decisions on risk-based are taken. This was not a simple job and involves recognition as following:

- Risk constrains.
- Risk assumptions
- Tolerance to risk.
- Trade-offs and Priorities.

The next factor was assessing risk. It discusses how organizations assess risk between the risk system boundaries. This factor was certainly the significant, and its purpose was to define the followings:

- Risks to the organizations.
- Internal as well as external susceptibilities.
- The risk effect that exploit the vulnerabilities.
- Probability of the attack.

Though, to achieve these objectives, the organizations must define the followings:

- Risk management methods, strategies, and methodology.
- Risk based assumptions.
- Responsibilities and Roles.
- How information on the risk assessment is stored, analyzed, and shared.
- How the risk assessment was carried out.
- Frequency of risk assessments.
- How to obtain information on the threat.

Risk response is the third factor of risk management. How organizations respond to risk after the risk has been defined through a risk assessment was addressed. The purpose of this aspect was to offer a coherent and holistic risk response in accordance with frame of risk. However, this objective could not be accomplished without the followings:

- Develop the alternate risk response protocol.
- Evaluation of the alternative process.
- Determination of the acceptable risk protocol among the sense of risk tolerances.
- Implement the risk responses on the basis of procedures determined.

The final factor of the risk management was continuous monitoring of risk, which discusses how organizations track threats eventually. The purpose of this part was to:

- Assure that the risk responses prepared was well implemented.
- Determining the continued efficacy of risk responses initiatives.
- Detect changes that affect risk.

This work was clearly comprehensive and allows for integrated method to risk management. The International Organization for Standardization or ISO has also published a standard on risk management in the field of data security [10]. When this principle was agreed upon among the network, it lacked a functional feature and did not offer for any deployment, as discussed in [8 & 9]. Nor does it describe an overview of controls presently in effect, as discussed in [11].

TABLE.1. COMPARISON OF RISK MANAGEMENT FRAMEWORKS

Attribute/Framework	NIST SP 800-30	ISO 27005
Method	Tactical	Higher level
Human resource	Not addressed	Explicitly addressed
Information gathering	Interview, Questioner, and document.	Questioner, Interview, and document.
Access	Free access	Paid access

III. ANALYSIS AND DISCUSSION

In the literature review, numerous flaws and problems associated with IoT systems were discussed and various risk assessment systems and their elements were addressed. The discrepancies and similarities among these systems were analyzed. On the basis of the analysis, that NIST 800-30 was essentially a management framework that blends into a technology-related context and was therefore more technical. Hence, ISO 27005 was better suited to management of higher-level activities, as it encompasses systems, people and technologies. However, these two systems were applicable to several organization that means that they were very generic for anything like an IoT unit.

IV. PROPOSED SOLUTION

After evaluating the various existing risk management systems and analyzing the findings, the following are proposed, rather implementing the common risk management system to every current IoT devices.

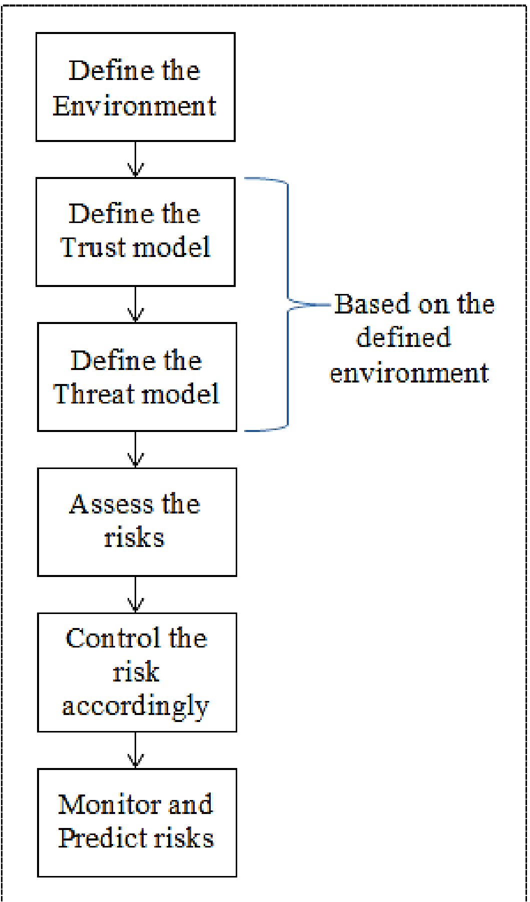
Define the Environment
Define the Trust model
Define the Threat model
Based on the defined environment
Assess the risks
Control the risk accordingly
Monitor and Predict risks

Figure.3. Proposed Model

The process of risk management should be incorporated into the life-cycle production of IoT devices itself. The IoT gadget manufacturer must incorporate an acceptable risk assessment process depending on the design of IoT devices. In this manner, the execution of risk managements can be judged on basis of the device's performance. i.e., the application of risk managements for the surveillance cameras can be done else as relative to the smart refrigerator. That was precisely why the existing risk management systems could not be applied on every IoT applications, because the present risk management framework seem to take the overview of and thus over-generalize risk management. It is comprehended that the IoT system is highly varied. It is also not necessary to implement the similar risk managements system for a microcontroller and the smart lock that was liable for protecting the entire buildings. Generally, trust and threat model vary considerably within IoT device, and thus, the standard risk managements system for each of them cannot be implemented. The risk managements process must be managed during the construction stage of the IoT facility for achieving the most successful and reliable process of risk management feasible. In the figure.3, the model that functions as a module must be incorporated into the life cycle of the IoT system.The initial step in the developed framework was to define the framework or environment in which the IoT interface is supposed to function. Further, an anticipated outcome of this process was a good description of the functionality and shortcomings of the system. In addition, the extrinsic and intrinsic values of the device must also be specified. The purpose of this step was to setup the way for the further steps.

The next step was the concept of the trust model. The specified model must comprise the hardware, software, and information on which a security of the device depends in relation to the defined context. The purpose of this step was to identify which components can be trusted by the IoT system and, thus, to identify what the components of untrusted are, which was important for the following step.

The next step was the concept of a threat model. The identified threat model was intended to recognize vulnerabilities related to the IoT system. It should also classify main threats which might target these vulnerabilities. In addition, the threat model should describe the possible collection of steps that an attacker could take to breach the device. Eventually, the threat model must recognize the effect as soon as the identified threat exploits the vulnerability. All of this must be performed in the sense of the given context. The purpose of this process was to collect the details required for the risk assessments to be carried out in the next step.

The next step, and also the significant one, was to evaluate the risk in line with the performance of the last steps. Risks assessment was a two-step method of risk recognition and risk assessments. The outcome from the past phase to define the possible risk associated in IoT device will be used. Then, after the risk has been established, it will reflect it in a qualitative or quantitative manner depending on the likelihood of occurrence and its effect after it has occurred. The purpose of this process was to direct the decision-making process for reacting to these threats, which would occur in the following step.

The following step was entirely about the use of controls to minimize risks to the optimal level. Though, it was important than a feasibility analysis in advance, particularly in the context of IoT was performed, since the lot of IoT gadgets were inexpensive. The implementation costs and the cost of the effect should be covered by the safeguards applied. The output of this step was an IoT system that was already handled in relation to vulnerabilities and risks and was able to be implemented without further risk control from user. This could be the last process in few situations where it was not possible to install patches and manage IoT systems.

The last step in model was to monitor existing threats and predict potential risks. Residual risks left out of the previous phase should be tracked to assure that the risk appetite was still smaller. Still need to predict potential threats, since technology was constantly changing and new vulnerabilities were developing day-by-day. IoT systems must also be maintained update in order to ensure an acceptable security level. This may be achieved by a range of means, such as patches for security and upgrades. Though, it was important to comprehend that this process will not be possible for few IoT gadgets, hence the expense of this process might be much higher than benefit of an IoT product. In the light of the knowledge given in the earlier steps, the feasibility review may determine either or not it could be necessary to implement this process. Unlike earlier steps, this process was an on-going one.

The proposed approach has many benefits over the existing risk management systems, few of them are:

- Appropriate for all IoT devices: Since the proposed approach is incorporated into the product development of all IoT devices, every system will have its own risk management system if required.
- Minimum charges from the User: The model required that risk management would be completely managed by the manufacturer. Therefore, no extra risk assessment can be added to the system by the end user.
- Very effective: Because the device manufacturer knows the best about the device, it could be ensured that the risk management frameworks offered by the manufacturer was very efficient.

V. CONCLUSION AND FUTURE WORK

IoT devices have been a critical part of our lives. However, due to their design, certain IoT devices are vulnerable to different forms of threats, which make it much more difficult to protect them. The importance of handling these vulnerabilities correctly and its built-in threats is thus greatly emphasized. Hence, a new approach to risk management, which is more suitable, because it is uniquely customized to each IoT system, needs minimum overhead from the user and is typically more efficient. In future, the problems of added cost of development will be addressed and also an effort to reduce it.

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable.

HUMAN AND ANIMAL RIGHTS

No animals/humans were used for studies that are basis of this research.

CONSENT FOR PUBLICATION

Not applicable.

AVAILABILITY OF DATA AND MATERIALS

The authors confirm that the data supporting the findings of this research are available within the article.

FUNDING

Full Degree Study, Stipendium Hungaricum Scholarship, Reference Number: SHE-19575-004/2020, Dated: 29.07.2020.

CONFLICT OF INTEREST

The authors declare no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENTS

The author would like to thank Faculty of Informatics, Eötvös Loránd University for providing support while carrying out this work.

REFERENCES

[1] A. Feringa, A. Y. Goguen, and G. Stoneburner, (2002). Risk management guide for information technology systems. Special Publication-800-30.

[2] R. S. Ross. 2011. Managing Information Security Risk: Organization, Mission, and Information System View (No. Special Publication (NIST SP-800-39).I. S. Jacobs and C. P. Bean. Fine particles, thin films and exchange anisotropy. in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic.

[3] Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. CISCO white paper.

[4] R. Shapaval, and R. Matulevičius. (2018). Towards the Reference Model for Security Risk Management in Internet of Things. International Baltic Conference on Databases and Information Systems.

[5] J. Tong, W. Sun and L. Wang. (2013). An information flow security model for home area network of smart grid. IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems.

[6] A. Jha, and M. C. Sunil. (2014). Security considerations for Internet of Things. L&T Technology Services.

[7] I. Andrea, C. Chrysostomou and G. Hadjichristofi. (2015). Internet of Things: Security vulnerabilities and challenges. IEEE Symposium on Computers and Communication (ISCC), Larnaca.

[8] A. Asosheh, B. Dehmoubed, and A. Khani. (2009). A new quantitative approach for information security risk assessment. 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT).

[9] A. Ekelhart, S. Fenz, and T. Neubauer. (2009). Aurum: A framework for information security risk management. 42nd Hawaii International Conference on System Sciences, HICSS '09.

[10] ISO/IEC. ISO 27005 information technology security techniques information security risk management, 2008.

[11] N. Al-Safwani, S. Hassan, and N. Katuk. (2014). A Multiple Attribute Decision Making for Improving

Information Security Control Assessment. Int. J. Comput. Appl.

[12] G. Soos, D. Kozma, J. Nandor, Ferenc, and P. Varga. (2018). IoT Device Lifecycle – A Generic Model and a Use Case for Cellular Mobile Networks.

[13] L. F. Rahman, T. Ozcelebi, and J. Lukkien. (2018). Understanding IoT systems: a life cycle approach. Procedia Comput. Sci.

[14] G. Ambika, and P. Srivaramangai. (2018). Review On Security In The Internet Of Things. Int. J. Adv. Res. Comput. Sci., Vol.9, No.1.

[15] M. A. Razzaq, S. H. Gill, M. A. Qureshi, S. Ullah. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. Int. J. Adv. Res. Comput. Sci. Appl., Vol. 8, No. 6.

Cite this article as: Mugesh Ravi. A Survey on Security Risks in Internet of Things (IoT) Environment. J. Comput. Sci. Intell. Technol. 2020; 1(2): 01–08. ©JCSIT, MNAA PUB WORLD, 2020.