Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Security And Privacy Of Iot For Source Location For Future Enhancement

Ms. Naghma Khatoon[1], Mr. Abhishek Kumar Gupta[2]

[1]Assistant Professor Computing And Information Technology Usha Martin University, Ranchi, Jharkhand

[2]Assistant Professor, Computer Science, Mangalayatan University, Beswan, Uttar Pradesh

ABSTRACT

The Internet of Things (IOT) future is already here. Healthcare, energy, and industrial automation are just a few examples of industries where IOT applications have had a significant impact. In the midst of all the benefits that the Internet of Things (IOT) has provided, new dangers have also surfaced. These risks are getting easier to deal with, but there are still a lot of unanswered questions. This study proposes "IOT characteristics" to better identify the core causes of new dangers and issues in current research today. Eight new IOT features were then examined in terms of their impact on security and privacy, including the dangers they pose, the remedies now in place, and the problems that remain to be addressed. Since this study analyses all known research works linked to IOT security from 2013-2017, it shows how IOT characteristics have an influence on the current state of research in this sector.

KEYWORDS: Internet-of-Things (IOT), IOT features, privacy, security, survey.

INTRODUCTION

Our lives will be made easier by the Internet of Things (IOT), a new technology that allows electronic devices and sensors to talk with one another through the internet. The Internet of Things (IOT) uses smart devices and the internet to give innovative solutions to a broad variety of commercial, government, and public/private sector concerns. Our everyday lives are increasingly being transformed by the Internet of Things (IOT), and it can be felt all around us. There are many smart systems, frameworks, and devices that can be connected to the Internet of Things (IOT). Quantum and nanotechnology are also used to attain previously inconceivable levels of storage, detection and processing speed. Quantum and nanotechnology An abundance of online and print

resources highlight the potential of IOT changes via research articles, news pieces, and printed materials. Prior to establishing new and innovative business ideas that take security, assurance, interoperability into consideration, this work might be employed as a preliminary effort.

LITERATURE REVIEW

JYOTINEELI (2021) People and computers will be able to operate billions of connected devices, including actuators, sensors, and other services, thanks to the Internet of Things (IOT) technology. Realizing the Internet of Things as a system will allow the distribution environment to integrate the cyber-world in an unbroken manner and will allow adjustments to be made centrally and human connection with the outside world to be authorized. The security and privacy risks of the Internet of Things (IOT) are examined in this study. With the most promising technologies in mind, we'll take a quick look at some of the existing techniques and analyze the security architecture aspects that can help us keep an eye on their requirements. There are a multitude of standards and stacks for communication assumed in the IOT, thus conventional security countermeasures cannot be immediately used.

RACHIT, SHOBHA BHATT (2021) IOT is a network of embedded devices that have unique identifiers and embedded software required to interact between the transient states. There are numerous IOT security issues that need to be examined in light of current IOT standards and protocols. A comprehensive overview of IOT security issues, new security protocols, and recently proposed security projects is presented in this paper, which focuses on the impending security elements of the IOT. IOT architecture is examined in terms of protocols and standards proposed for the future generation of IOT systems. Protocols, standards, and proposed security models are compared in accordance with IOT security needs.

MOURADE AZROUR (2021) It is possible to link a wide range of devices and objects through the Internet of Things (IOT). Sensing, processing, and transferring data are three of the most important components of the "Internet of Things" (IOT). Healthcare, telecommunications, the environment, industry, construction, water management, and energy are just some of the areas where the "Internet of Things" (IOT) is being used in a broad variety of ways. Internet of Things (IOT) technology depends on embedded devices rather than desktops, laptops, and smartphones. Data produced by sensors and the capacity to merge physical and virtual worlds means that IOT systems need to be more secure than ever before. Additionally, light-weight encryption approaches are required for IoT. For this research, the goal is to identify the best authentication procedures for an IOT service, given the projected security challenges and important concerns.

MIKHAIL ZYMBLER (2019) We've gone from a conventional way of life to a high-tech one thanks to the Internet of Things (IOT). Examples of IOT-induced advancements include smart cities, smart homes, and pollution control. There have been

a number of important studies and investigations into how the Internet of Things can improve technology. In order to properly exploit the IOT, however, a number of impediments and problems must be handled first. In order to handle these issues and possibilities, the Internet of Things (IOT) must be taken into consideration. To provide a thorough analysis from both a technical and social perspective, this article's main goal is to provide an overview. As well as architecture and essential application domains, this article discusses various IOT difficulties and critical problems. This page also displays current literature and shows its contribution to several aspects of the Internet of Things (IoT). The Internet of Things relies heavily on big data and data analysis (IOT). After reading this article, readers and researchers will have a better understanding of IOT and its practical application in the real world.

ZULFIQAR ALI SOLANGI (2018) As smart sensors, cameras, databases, and massive data centres come together to form the Internet of Things (IOT), a global network computing environment that is both invisible and everywhere. Participation in an international network has always been an aspiration. The connection potential of the Internet of Things (IOT) will be retained in all facets of the future smart world, from smart household items like TVs, washing machines, thermostats, and refrigerators to the Industrial Internet of Things (IIOT) and the Internet of Medical Things (IoMT). Maintaining IOT connectivity's advantages, however, is essential to avoid unforeseen security and privacy vulnerabilities that might lead to a broad variety of threats, including ransomware and eavesdropping, among other things. This paper will present and anticipate advanced approaches for end-to-end security and privacy difficulties, including a comprehensive strategy for identifying, authenticating, and controlling IOT devices. Internet of Things privacy and security concerns are only going to develop in the future.

IOT SECURITY RESEARCH ANALYSIS

Security research on the Internet of Things (IoT) has been examined from more than 200 research publications published in top journals and conferences over the last five years. On the basis of this research, we'll show how IOT security research has evolved and discuss the driving forces behind it. In addition, we provide researchers with analysis-based ideas and assistance in keeping abreast of the most recent IOT security research status and research goals.

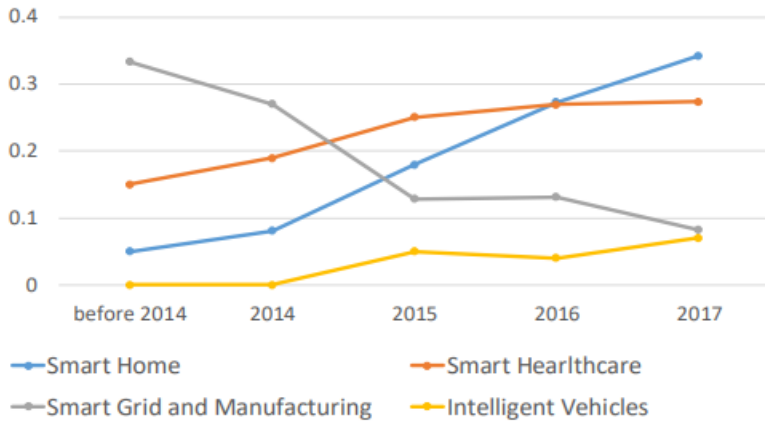
A. Research Collection and Label

IOT research papers will be discussed in the next part using statistical analysis and classification. We begin this part by describing how we searched and filtered existing research publications, and then explain how we labeled each paper.

To begin, we gathered papers from prestigious computer security journals and conferences (concrete catalogue see the Get Hub link in Appendix). Following this method, we decided whether or not the research is relevant to IOT security. To begin,

we selected IOT keywords that encompass a wide range of IOT devices, protocols, and use cases. Using these IOT keywords or abbreviations in the title of a paper, we added it to our list of studies. Or we examined to see whether there are any IOT keywords in the abstract, such as "privacy" or "security." Finally, over 200 research papers were chosen for additional examination (all tags of these papers see the Getup link in Appendix).

Each publication was also tagged with three tags (layers, application scenarios, and threats) in order to categorise these papers according to SOA IOT layering or application scenarios for further statistical analysis and to find out what issue research is most worried about at this time. Based on the paper's subject, it is simple to tell which layer and application it belongs to. Despite the fact that these articles offer diverse answers, some of the challenges they are attempting to address are similar. As a result, we label each paper's "threat" tag based on these prevalent issues. Using the OWASP IOT Top Ten security vulnerabilities as a starting point, we discuss these challenges in a more broad way.



The Fig. 1 “illustrates the change of the proportion of the number”

Figure 1 depicts the shift in recent years in the relative quantity of articles in various application situations. Research on IOT security can be shown to be closely tied to the growth of IOT applications. Since smart grids and smart manufacturing become more widely used in the early 2010s, security research in these domains has increased. Smart home and healthcare technology's rapid development in recent years has drawn the attention of security researchers; Interest in the smart grid and smart manufacturing has diminished at the same time.

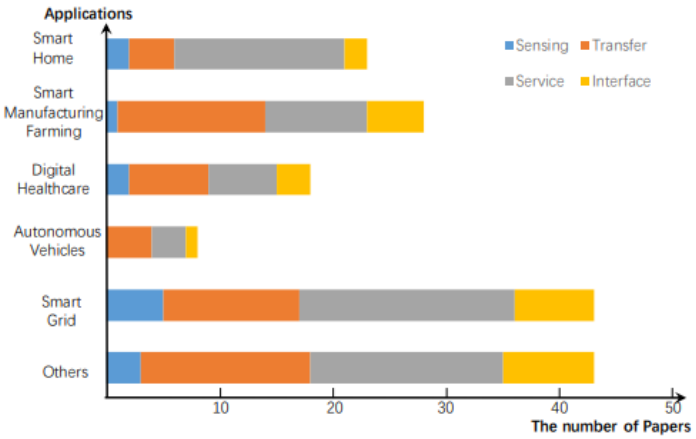


Fig. 2 "The Number of Papers of Each Layer in Different IOT Application Scenarios"

On the IOT application stack's various layers, the number of papers published may be seen in Figure 2. The image shows how the distribution of different layers in security investigations varies depending on the application context. For example, in smart manufacturing, more research is being done on transfer layers than on application levels, whereas in smart homes, the converse is true. All sensors in industrial and agricultural settings rely on WSNs to interact with one other and the remote control system. WSNs are essential. Others will be more at risk as a result of the WSN security issues. Smart home devices, on the other hand, are operated via mobile or online applications. Research on smart home security and secure manufacturing transfers has increased as a result of this. A further illustration of this idea may be seen in Figure 3.

According to Fig. 3, each "threat" tag counted in all potential application situations. The bulk of research has been focused on issues related to data migration, privacy, and network or protocol security. Just because of the traits we've already highlighted, such as intimacy, multiplicity, and diversity. IOT technologies, such as smart home and healthcare devices, collect, transfer, and use more sensitive information, which raises privacy concerns. Cyber-attacks are easier to conduct because of the large number of "Internet of Things" (IOT) devices. Many new technologies and protocols have flaws that necessitate more research and development. As previously stated, a lack of understanding is a major contributor to the vulnerability of cloud and web services due to improperly configured security settings. In addition, the "restricted" and "interdependence" IOT features will lead to greater attacks on IOT systems and mobile applications, despite a decrease in research on IOT systems and mobile applications in the past several years. These fields need more research.

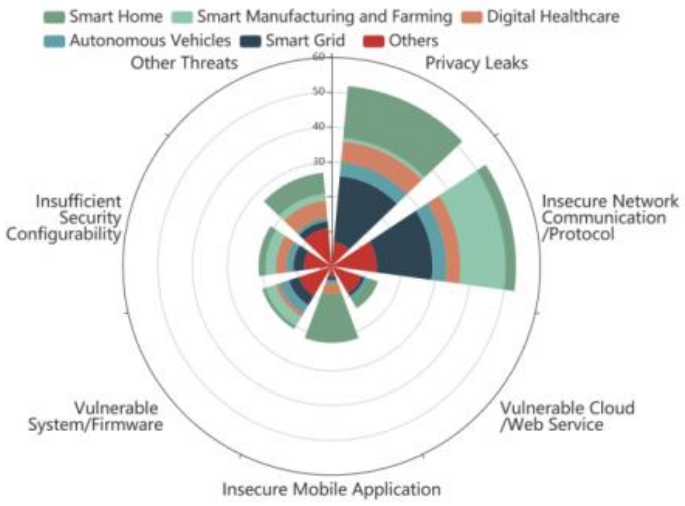


Fig. 3 "The Number of Papers of Different Threat Tags in Different Application Scenarios"

THE EFFECT OF IOT FEATURES ON SECURITY AND PRIVACY

This section will cover every aspect of the Internet of Things, including threats, difficulties, solutions, and possibilities.

1). in this section, we describe the features and distinctions between traditional devices, networks, and apps.

2). Here, we highlight the potential dangers posed by this functionality, along with their possible effects on our users' safety. Diagrams and illustrations of some hazards are also provided, making it easier to understand.

3). In this section, we discuss the difficulties that the qualities in question provide for researchers.

4). Existing solutions to the problems we face, as well as the shortcomings of those solutions, are presented in this section. In addition, we provide several novel security methodologies and ideas that could also assist in the transformation of difficulties and risks into opportunities in this context.

CONCLUSION

Internet of Things (IoT) data security and privacy concerns are explored in this article. These qualities have a number of dangers and research concerns, which we discussed first. There were also existing solutions for these difficulties that we examined and pointed out what new technology was needed. For the final part of our presentation, we explained the current trend in IOT security research and the reasons behind it. We can only have a better understanding of future research hotspots and IOT security development by thoroughly examining these new elements behind the Internet of Things.

REFERENCE

1. Jyoti Neeli(2021),” Insight to security paradigm , research trend & statistics in internet of things(IOT),” Global Transitions Proceedings Volume 2, Issue 1, June 2021, Pages 84-90

2. Rachit, Shobha Bhatt (2021),” Security trends in Internet of Things: a survey,” Published: 12 January 2021

3. Mourade Azrour (2021),” Internet of Things Security: Challenges and Key Issues,” Volume 2021 |Article ID 5533843

4. Mikhail Zymbler (2019),” Internet of Things is a revolutionary approach for future technology enhancement: a review,” Article number: 111 (2019)

5. Zulfiqar Ali Solangi (2018),” The future of data privacy and security concerns in Internet of Things,” May 2018

6. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (IOT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, 2013.

7. D. Bandyopadhyay and J. Sen, “Internet of things: Applications and challenges in technology and standardization,” ” Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.

8. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

9. O. Vermesan and P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers, 2013.

10. O. Mazhelis, H. Warma, S. Leminen, P. Ahokangas, P. Pussinen, M. Rajahonka, R. Siuruainen, H. Okkonen, A. Shveykovskiy, and J. Myllykoski, “Internet-of-things market, value networks, and business models : State of the art report,” 2013.

11. M. Covington and R. Carskadden, “Threat implications of the internet of things,” in Cyber Conflict (CyCon), 2013 5th International Conference on, 2013, pp. 1–12.

12. R. Roman, P. Najera, and J. Lopez, “Securing the internet of things,” Computer, vol. 44, no. 9, pp. 51–58, 2011.

13. H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651.

14. J. Pan, S. Paul, and R. Jain, "A survey of the research on future internet architectures," Communications Magazine, IEEE, vol. 49, no. 7, pp. 26– 36, 2011.

15. O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer et al., "Internet of things strategic research roadmap," O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends, pp. 9–52, 2011.