Current issues in IoT networking

Guanxiong Wang (A paper written under the guidance of Prof. Raj Jain)

Abstract

One of the most popular technical vocabularies in the last decade is the Internet of Things. It was proposed as early as the end of the last century, but it has gradually become popular in the past decade. Now it has penetrated every aspect of life. For example, all smart home devices include smart table lamps, smart curtains, and smart switches. The Internet of Things is also changing our production and lifestyles, making our society smarter, saving costs in the production process, and better monitoring the supply chain and assembly lines. By consulting the relevant literature of the past five years, this article sorts out the main problems facing the Internet of Things and proposes some solutions.

Keywords:

IoT, Internet of Things, sensors, security, privacy, networking, issues, RFID, Radio-frequency identification, IPv4, IPv6.

Table of Contents:

1. Introduction

With the development of the Internet of Things, various smart devices have provided great convenience to our lives. But while enjoying the convenience, there are still many issues waiting to be solved. For example, security issues, privacy issues, compatibility issues, legal issues involved in different jurisdictions, and so on. Failure to solve these problems will affect the further development of the Internet of Things. We have proposed solutions from the aspects of developers, standard formulation, and information security verification.

2. Introduction to IoT

Although the concept of the Internet of Things has become popular in recent years, people have had the idea of the Internet of Everything a long time ago. The Internet of Things is a network based on products with radio frequency identification devices and sensors. Each product can be uniquely identified based on its sensors and systems, which is equivalent to the id of the product. The convenience and progress brought by the Internet of Things are not without cost, and technological advances are also accompanied by the emergence of many new issues.

2.1 The origin of the Internet of Things

As early as 1966, Karl Steinbuch, a German computer science expert predicted that "In a few decades, computers will be interwoven into almost all industrial products" [Postscapes].

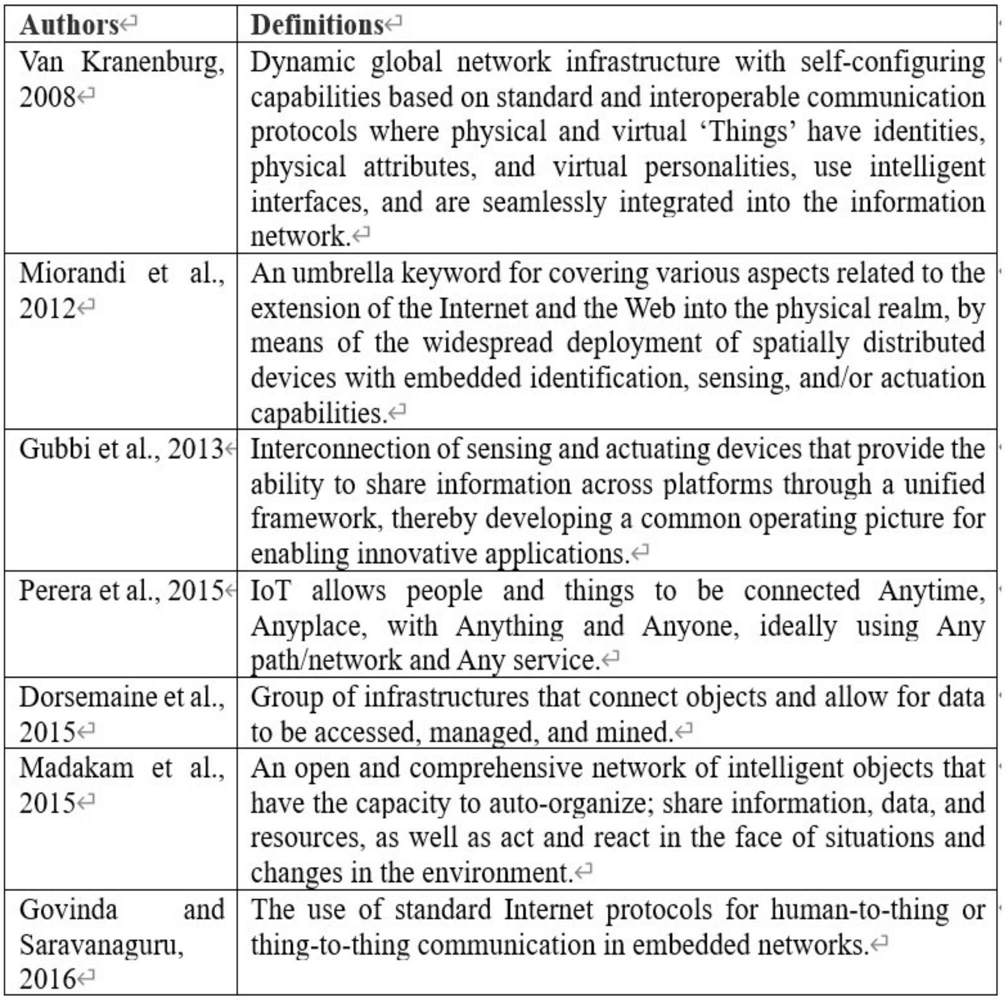
What is happening in our world now proves that his prediction is correct. Later in 1982, David Nichols, a graduate student in the Department of Computer Science at Carnegie Mellon University, improved the Coca-Cola vending machine at the time through cooperation with several students, making it the first device connected to ARPANET and able to report its inventory and whether the Coke is in a cold state, and this is the primary realization of the early smart device network [Wiki].

Later in 1999, Kevin Ashton, an expert at P&G, invented the term "Internet of Things". He also believes that all objects in the physical world can be connected to the Internet through sensors driven by RFID (Radio-frequency identification Offsite Link), so that data can be collected and tracked without human participation, which can greatly reduce costs [HistoryofInformation].

2.2 The definition of the Internet of Things

Although the Internet of Things is so popular now, there is no accurate and consensus definition of it. Different organizations have different understandings and definitions [Rose 15].

For readers to have a more comprehensive understanding, here are some main definitions from Andrea Sestino's summary:



Authors	Definitions
Van Kranenburg, 2008	Dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network.
Miorandi et al., 2012	An umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing, and/or actuation capabilities.
Gubbi et al., 2013	Interconnection of sensing and actuating devices that provide the ability to share information across platforms through a unified framework, thereby developing a common operating picture for enabling innovative applications.
Perera et al., 2015	IoT allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service.
Dorsemaine et al., 2015	Group of infrastructures that connect objects and allow for data to be accessed, managed, and mined.
Madakam et al., 2015	An open and comprehensive network of intelligent objects that have the capacity to auto-organize; share information, data, and resources, as well as act and react in the face of situations and changes in the environment.
Govinda and Saravanaguru, 2016	The use of standard Internet protocols for human-to-thing or thing-to-thing communication in embedded networks.

Figure1: Main definitions of Internet of Things [Sestino 20].

I personally think that the more accurate definition comes from the definition of the International Telecommunication Union (ITU) ITU-T Recommendation Y.2060:

"3.2.2 Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

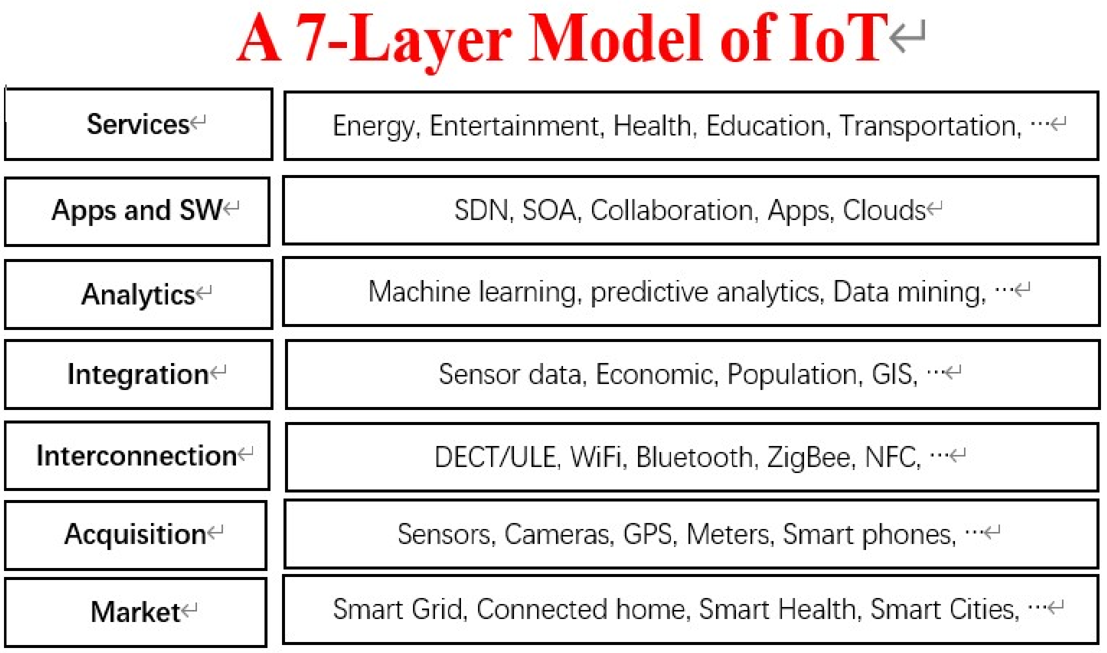
Note 1-Through the exploitation of identification, data capture, processing, and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

Note 2-From a broader perspective, the IoT can be perceived as a vision with technological and societal implications." [ITU-T 12]

2.3 Some basic concepts in IoT

Current issues in IoT networking

We can divide the Internet of Things into multiple layers, here is a model that is given by Professor Jain. Basically, there are seven layers: Market, Acquisition, Interconnection, Integration, Analytics, Apps and SW, Services. From the second layer to the sixth layer, we will also need to consider the security and management aspects. The Figure below is from Professor Jain's lecture, which also lists some specific examples of each layer.

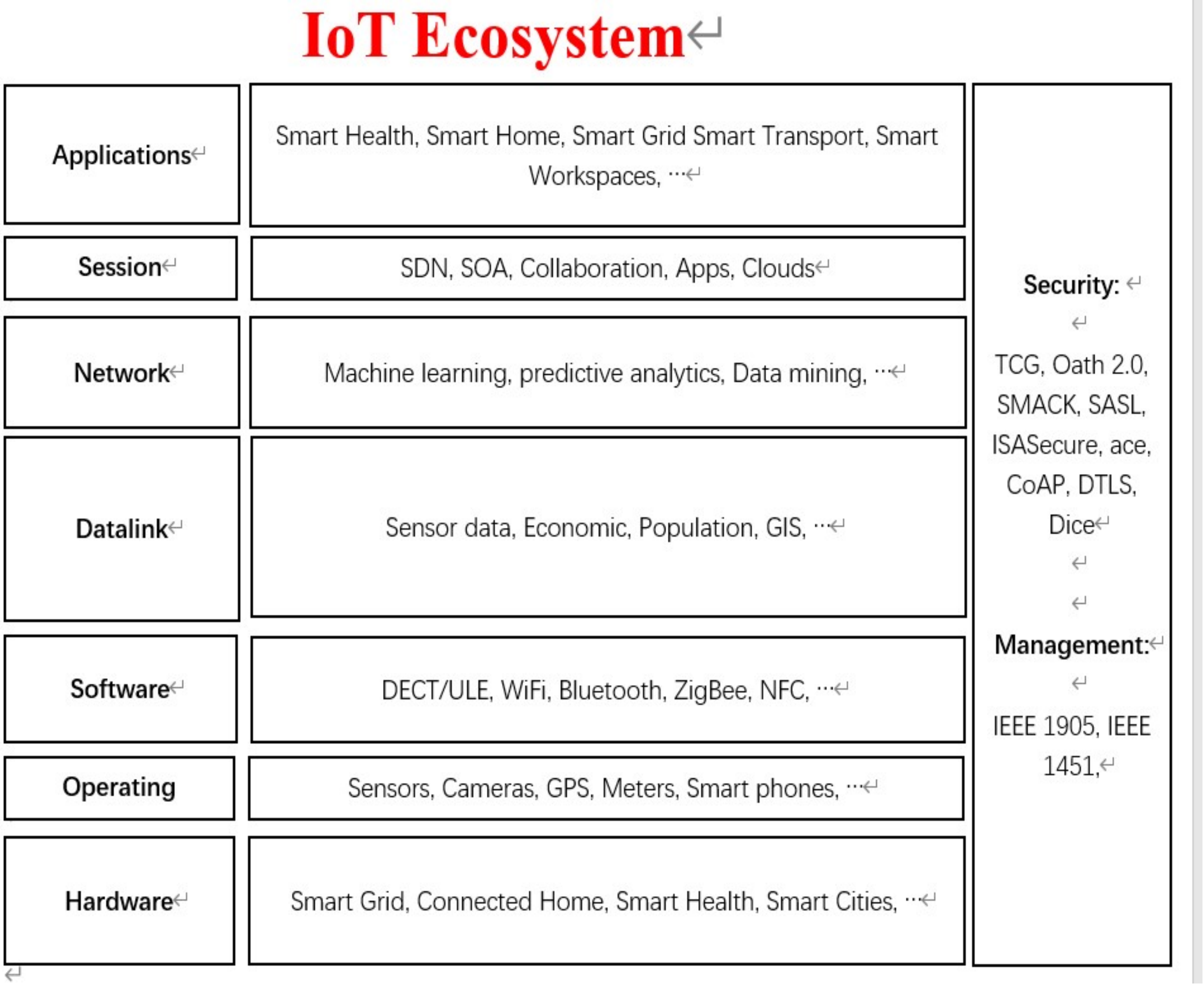


A 7-Layer Model of IoT

Services	Energy, Entertainment, Health, Education, Transportation, ···
Apps and SW	SDN, SOA, Collaboration, Apps, Clouds
Analytics	Machine learning, predictive analytics, Data mining, ···
Integration	Sensor data, Economic, Population, GIS, ···
Interconnection	DECT/ULE, WiFi, Bluetooth, ZigBee, NFC, ···
Acquisition	Sensors, Cameras, GPS, Meters, Smart phones, ···
Market	Smart Grid, Connected home, Smart Health, Smart Cities, ···

Figure2: A 7-Layer Model of IoT [Jain 21].

In addition, Professor Jain also gave a 7-layer diagram of the IoT ecosystem, hoping to enable readers to have a more intuitive understanding of the composition of IoT. Due to limited space, I cannot analyze every aspect or protocol in the figure in detail in this article. Interested readers can consult more information according to their own interests. This article will analyze IoT issues in general.



IoT Ecosystem

Applications	Smart Health, Smart Home, Smart Grid Smart Transport, Smart Workspaces, …	Security: TCG, Oath 2.0, SMACK, SASL, ISASecure, ace, CoAP, DTLS, Dice Management: IEEE 1905, IEEE 1451,
Session	SDN, SOA, Collaboration, Apps, Clouds	
Network	Machine learning, predictive analytics, Data mining, …	
Datalink	Sensor data, Economic, Population, GIS, …	
Software	DECT/ULE, WiFi, Bluetooth, ZigBee, NFC, …	
Operating	Sensors, Cameras, GPS, Meters, Smart phones, …	
Hardware	Smart Grid, Connected Home, Smart Health, Smart Cities, …	

Figure3: IoT Ecosystem [Jain 21].

2.4 The importance and some issues of IoT [Gillis 21]

Before the emergence of the Internet of Things, people needed to personally collect various data from machines, and then analyze and process the data to use or pass it to other machines for use. This is a tedious and costly process, but everything is different after the advent of the Internet of Things. With the emergence and development of the Internet of Things, enterprises and factories can monitor and obtain the operation status and data of equipment and machines for 24 hours without being on duty, which saves labor costs and improves accuracy, so that enterprises can better optimize their production lines and supply chain.

For individuals, the Internet of Things makes our lives more intelligent and convenient. Our smart devices can connect to each other to achieve a fully automated living environment.

Although the Internet of Things has so many advantages, it comes with some disadvantages that cannot be ignored. Communication between devices all the time gives hackers more opportunities. If someone steals private or confidential information, it may cause bad results.

Excessive data volume may also be a challenge, and companies must filter and optimize the data. In addition, there are reliability issues, such as how to ensure that the data is correct and complete, because a failure of one set may affect the operation of the entire system equipment.

Summary:

Karl Steinbuch predicted the trend of the Internet of Everything in 1966, David Nichols developed the first device connected to ARPANET in 1982, and Kevin Ashton coined the term Internet of Things in 1999. Since then, more and more companies and organizations have promoted the continued development of the Internet of Things and have a new understanding and definition of it. It can be determined that the Internet of Things has played an important role in all aspects of our lives. But if the Internet of Things technology wants to achieve sustained and rapid development and popularization, some of its issues must be resolved.

3. Current issues in IoT

Although the Internet of Things is so important and popular, its shortcomings cannot be ignored. While it brings convenience to people, it also produces a series of problems, such as security issues, privacy issues, legal issues involved, and so on.

3.1 Security issues

Since the Internet of Things links the physical world together through the Internet and they are transmitting data all the time, more transmission and data will also have more risks. To control development and production costs and make their products cost-effective, manufacturers often only configure necessary functions for the Internet of Things. Most smart Internet devices can only run 8-bit or 16-bit operating systems. In addition, due to low processor computing speed, insufficient storage space, insufficient communication bandwidth, and poor battery life, many traditional security solutions cannot be applied to the smart devices of the Internet of Things, which directly leads to the hidden security risks of many smart devices of the Internet of Things [Sha 18]. Poorly designed equipment or protocols may lead to the theft of user data and lead to abuse. [Singhai 21]. But security is also an important part of the Internet of Things, because if users believe that the device is insecure, it may cause their data and information to be stolen, then users will reduce their use of the Internet of Things. This has a negative impact on the innovation and production of IoT devices, leading to a negative cycle [Rose 15].

In addition, most of the IoT devices consumed by users are produced and provided by a small number of leading companies, which leads to a large amount of homogeneity. It can be compared to the automobile industry. A security breach of any vehicle model may lead to a large-scale recall. Any small loophole or insecure protocol does not exist alone, on the contrary, its harm will be magnified by the huge number of the same devices or protocol [Rose 15].

Long-term maintenance of IoT devices is also a challenge. In the fast-paced society at present, you can never predict a company will fail or not. If a company goes bankrupt, but users are still using the equipment it produces, this will cause the update of this equipment to stagnate. It may be safe now, but with the development of security threats, these types of equipment will not be safe. Therefore, the long-term management and maintenance of equipment is also an issue [Rose 15].

3.2 Privacy issues

IoT devices collect and transmit data all the time, which may cause a series of privacy issues. These data may be personal data about the user or may indirectly reflect the personal information of the user. For example, the Internet-enabled lamp captures and collects the user's preference for light intensity is harmless, but if his Internet lamp collects and reports the time, he often uses the lamp, then these data can expose the person's life and rest. This privacy exposure is particularly serious when multiple devices work together. For example, in the above case, your Internet-enabled watch also records and uploads the user's daily itinerary, and the mobile phone records the user's consumption location and habits. This combination of data can be It depicts the daily life of the user, so what data to record and how to use the user's data becomes particularly important. How to protect the user's privacy is an issue [Rose 15].

You may have the following similar experience: You searched for a product on a mobile application, and then you opened your computer browser and found that Google recommended you the product you just saw on the mobile application. You may wonder why Google is so smart, but it is because your data has been misused without your permission. To make matters worse, you only verbally talked about something with your friend, and then you opened the shopping app and found that it pushed the item you just talked about to you, although there is no evidence that the mobile app will monitor and analyze your daily conversations, through my survey of some friends around, they have all had similar experiences. Fortunately, Apple added an option to prohibit apps or websites from tracking personal information in this year's system update. This is an effective protection for user privacy, but other brands of IoT devices also have the same privacy issues.

In addition, IoT devices are widely used in the medical field, which involves more private personal information. These private data include height, weight, sexual ability, HIV infection, genetic information, and so on. Therefore, in the medical field, personal data obtained by IoT devices have serious privacy issues [Ray 20].

For IoT devices, we need to clarify who can collect data, where the data needs to be stored, who can access the data, who is responsible for the security of data transmission, and users know their own data management authority. Thereby reducing the occurrence of privacy issues [Strous 21].

3.3 Scalability issues and Incompatibility issues

With the development of the Internet and smart devices, billions of smart devices are being connected to the interconnected system. IPv4 addresses are 32 bits and most of them are already occupied, so they cannot meet the needs of a larger number of devices in the future. To solve this scalability issue, IPv6 was created. IPv6 uses 128-bit addresses to provide 3.4 * 10^38 different addresses for devices on the Internet, which can theoretically meet the needs of future devices [Singhai 21]. To consider, a large number of deployed devices using IPv4, IPv6 will coexist with IPv4 for a period, but the trend is to gradually transition to IPv6 [Salazar 17].

Current issues in IoT networking

A major problem with IoT devices is that they may come from different companies, use different protocols, and the sensors and processors may be different. Each individual device may have a good user experience, but it is difficult for a user to use a single application to control multiple devices to work together and synchronize data, which makes the user's sense of experience degraded and it is troublesome to manage and use. In other words, our IoT smart devices are not smart enough. For example, you need an application to control Alex to turn off the lights, and you also need another application to control the temperature of the air conditioner. This fragmented experience is not the Internet of Things and smart home we are after. Therefore, scalability and incompatibility are also current issues in IoT [Srivastava].

In addition to technical reasons, competition among enterprises is also one of the main reasons leading to the lack of compatibility of IoT smart devices. To maintain their own high profits and build an ecosystem with high user stickiness, some smart device manufacturers will manufacture smart devices compatible only with their own brands to achieve the purpose of locking in consumers. For example, in the smart home market, a smart humidifier from one smart device supplier may not work with another brand's smart switch, which limits your future device choices. For users who like DIY (such as Android users), such an approach undoubtedly hinders innovation and healthy competition. By increasing the barriers between products, users will have limited choices and a broken product experience. Such product barriers will also indirectly lead to agreement barriers. For example, some interactive functions of Apple smart devices cannot be used with Android devices. If you want to experience the complete Apple service, you need to be forced to increase the number of your Apple smart devices.

Compatibility issues are also reflected in the data management aspects of IoT services. Based on the popularity of cloud computing and fog computing, the data collected by many IoT smart devices are transmitted to cloud servers for storage and processing. If the format of these data is proprietary and cannot be modified, it seems that the person who actually controls the data is not the user himself. Because they cannot migrate the same service to other service providers, only when the data is provided to the user in an open-source format or in a recognized standard format, the personal data is useful to the user and can be controlled by the user that what to do with these data [Rose 15].

3.4 Other issues

In addition to some of the main issues above, there are also some minor issues that cannot be ignored. For example, how to evaluate the performance of a smart IoT device or service. First, it is composed of many components, and its performance may be affected by many components. Such as data collection speed, data processing speed, data transmission speed, and so on. In addition, the development of the underlying technology will also affect the performance of the IoT system. Therefore, the performance evaluation of IoT devices and systems is a multi-dimensional evaluation [Salazar 17].

In terms of management, as billions of IoT devices are connected to the Internet, the maintenance and management of the devices have also become a huge problem. Obviously, manual management is unrealistic because the number of devices and their working hours far exceeds that of humans. Therefore, the development of new lightweight management protocols has become a new requirement [Salazar 17].

The data transmission activities of IoT devices may also involve complex legal issues. Different countries and even different states will have different definitions and interpretations of privacy and personal data protection, but IoT devices do not seem to be bound by laws in different regions. For example, an IoT device can legally collect and use certain data in one jurisdiction, but there seems to be no restriction to prevent it from transmitting the data to another jurisdiction, regardless of whether the data is legal in another area. The cross-border flow of these data may cause a series of legal issues, but there is no clear boundary. In this case, who should be responsible for the resulting legal disputes? Because the user may be unknowing, but their device is illegal. This is a complex challenge, and perhaps more stringent laws can be used to limit this situation, and perhaps various jurisdictions can negotiate and unify the laws of IoT data transmission [Rose 15].

Summary:

The Internet of Things also has security issues, privacy issues, scalability issues, incompatibility issues, data management issues, legal issues, etc. If these issues cannot be dealt with in a timely manner, this will cast doubt on people's decision to continue using IoT smart devices, which will also hinder the continued development of the IoT.

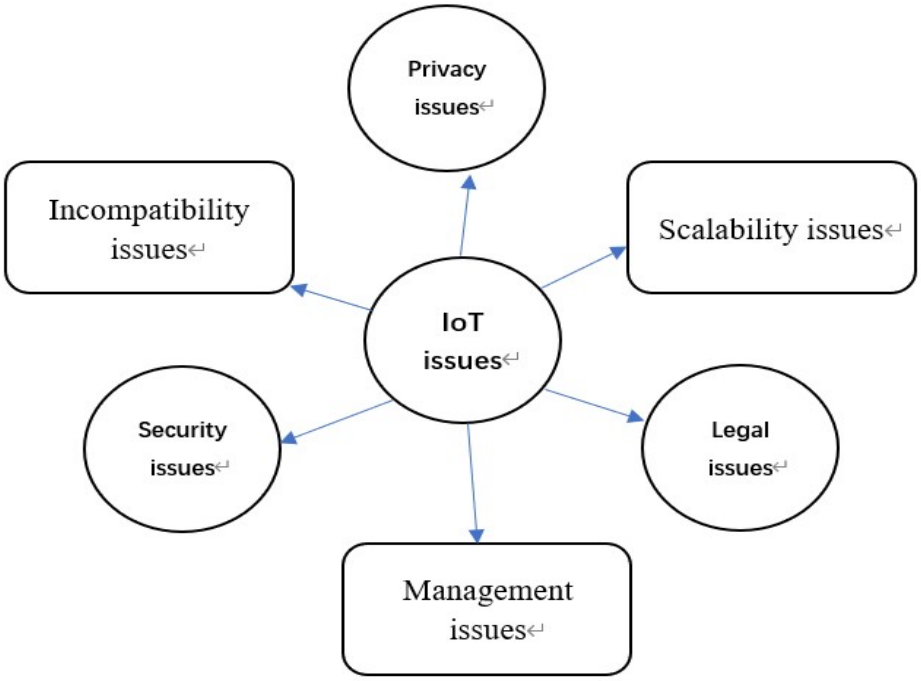


Figure4: Issues in Internet of Things.

4. Solution to some issues

Although there are many problems with the Internet of Things, it cannot deny its importance. We will propose a series of solutions in this chapter to deal with the above problems.

4.1 Solution to security issues

Security is essentially a technique to ensure that protecting consumer development and implementation is a key goal. In terms of protecting user data and information security, we can start from the following directions: data credibility, data integrity, and information accessibility [Rekha 21].

Since many Internet of Things equipment is incomplete in safety prevention during production, a large amount of research has been invested in the equipment maintenance stage. Rather than assume security responsibilities in the later stage, it is better to consider security as an important component in the production and development stage, and consider all aspects of security issues, thereby making future attacks more difficult and predictable [Rekha 21].

Secondly, we must cultivate a good security awareness. As a developer, although excessive investment in security will increase the cost, it is not much compared with the loss caused by hacker attacks. Therefore, as a developer, you need to always pay enough attention to relevant security factors. In the design and development process, you must establish the correct security awareness. At the same time, in the recruitment and cooperation process, whether the candidate has sufficient security awareness should also be an important consideration [Rekha 21].

An important means for smart IoT systems to enhance protection is to implement authorization functions and verification functions. Some sensors should verify whether their recipients or applications are legitimate before publishing their information. This can effectively prevent illegal programs or unauthorized programs from obtaining personal information or disrupting the operation of the program. By creating authorization certificates and end-to-end verification, users' data security can be effectively protected [Rekha 21].

4.2 Solution to privacy issues

The increase of IoT devices has also increased the risk of privacy leakage. The increasing number of devices that collect personal data has also made it increasingly difficult for people to prevent privacy leakage.

In terms of preventing privacy leakage, the first thing that should be done is program developers. They should have clear terms to inform users of the data they want to collect, and a clear interface to show their definition of private data. Secondly, the following principles should be observed: First, the system should not be able to self-adjust to node failures due to a single point of failure. Second, the communication address must match the verification information. Third, the information publisher must provide security management for all information [Weber 15].

4.3 Other solutions

For other challenges, we also give some suggestions. For example, blockchain technology can be used to provide transparent, safe, and reliable lightweight solutions. Develop relevant international standards to eliminate incompatibility issues. Manage different risk levels by layering different IoT devices, etc [Alfrhan 21].

Summary:

We can prevent security issues during equipment design and development and use more complete protocols to ensure data security after equipment deployment. At the same time, formulating international standards is also a way to solve compatibility and legal issues.

5. Summary

The Internet of Things has developed rapidly in the past decade, which is inseparable from the efforts of early scientists, scholars, and professors. The Internet of Things is now playing a huge role in Energy, Entertainment, Health, Education, Transportation, etc., making a lot of things smart, such as Smart Grid, Connected Home, Smart Health, Smart Cities.

At the same time, some problems were exposed. For example, security issues, privacy issues, scalability issues, incompatibility issues, data management issues, legal issues, etc. Whether these problems can be correctly solved will affect the development of the Internet of Things.

Reference List

[Postscapes] Internet of Things (IoT) History, https://www.postscapes.com/iot-history/

[Wiki] Wikipedia, https://en.wikipedia.org/wiki/Internet_of_things

[HistoryofInformation] Kevin Ashton Invents the Term "The Internet of Things", https://www.historyofinformation.com/detail.php?id=3411

[Kranenburg 11] Rob Van Kranenburg, "The Internet Of Things: RADICAL TRANSPARENCY WITHIN THE REACH OF ALL", JSTOR, 2011, https://www-jstor-org.libproxy.wustl.edu/stable/48505085?seq=1#metadata_info_tab_contents

[Sestino 20] Andrea Sestino, Maria Irene Prete, Luigi Piper, Gianluigi Guido, "Internet of Things and Big Data as enablers for business digitalization strategies", Science Direct, 2020, https://doi.org/10.1016/j.technovation.2020.102173

[Salazar 17] Jordi Salazar, Santiago Silvestre, "Internet of things", Czech Technical University of Prague Faculty of electrical engineering, 2017, 9788001062326

[Rose 15] Karen Rose, Scott Eldridge, Lyman Chapin, "The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World", https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

[ITU-T 12] TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, "Overview of the Internet of things", 2012, Recommendation ITU-T Y.2060, https://www.itu.int/rec/T-REC-Y.2060-201206-I

[Gillis 21] Alexander S. Gillis, "What is internet of things (IoT)?", https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[Singhai 21] Richa Singhai, Rama Sushil, "An investigation of various security and privacy issues in Internet of Things", Science Direct, 2021, https://doi.org/10.1016/j.matpr.2021.07.259

[Rekha 21] Shashi Rekha, Lingala Thirupathi, Srikanth Renikunta, Rekha Gangula, "Study of security issues and solutions in Internet of Things (IoT)", Science Direct, 2021, https://doi.org/10.1016/j.matpr.2021.07.295

[Srivastava 20] Neha Srivastava, "Compatibility of Internet of Things (IoT) and User Experience (UX)", 2020, https://www.uxness.in/2020/03/compatibility-of-internet-of-things-iot.html

[Ray 20] Partha Pratim Ray, Dinesh Dash, Neeraj Kumar, "Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions", Science Direct, 2020, https://doi.org/10.1016/j.comcom.2020.05.029

[Strous 21] Leon Strous, Sune von Solms, Andre Zuquete, "Security and privacy of the Internet of Things", Science Direct, 2021, https://doi.org/10.1016/j.cose.2020.102148

[Allhoff 18] Fritz Allhoff, Adam Henschke, "The Internet of Things: Foundational ethical issues", Science Direct, 2018, https://doi.org/10.1016/j.cose.2020.102148

[Sha 18] Kewei Sha, Wei Wei, T. Andrew Yang, Zhiwei Wang, Weisong Shi, "On security challenges and open issues in Internet of Things", Science Direct, 2018, https://doi.org/10.1016/j.future.2018.01.059

[Weber 15] Rolf H. Weber, "Internet of things: Privacy issues revisited", Science Direct, 2015, https://doi.org/10.1016/j.clsr.2015.07.002

[Alfrhan 21]	Aishah Alfrhan, Tarek Moulahi, Abdulatif Alabdulatif, "Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT)", Science Direct, 2021, https://doi.org/10.1016/j.bcra.2021.100036
[Jain 21]	Raj Jain, "Introduction to Internet of Things", 2021, https://www.cse.wustl.edu/~jain/cse570-21/ftp/m_10iot.pdf

List of Acronyms

IoT	Internet of Things
ITU	International Telecommunication Union
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ARPANET	Advanced Research Projects Agency Network
RFID	Radio-frequency identification Offsite Link
SDN	Software Defined Networking
SOA	Service Oriented Architecture
DECT	Digital Enhanced Cordless Communication
ULE	Ultra Low Energy
WiFi	Wireless Fidelity
NFC	Near field communication
CoAP	Constrained Application Protocol
IEEE	Institute for Electrical and Electronic Engineers

Last modified on December 15, 2021
This and other papers on recent advances in networking are available online at
http://www.cse.wustl.edu/~jain/cse570-21/index.html
Back to Raj Jain's Home Page