ISSN 3060-4567

NARROWBAND INTERNET OF THINGS SECURITY THREATS AND COUNTERMEASURES

Norkuvvat Chunaev

Tashkent University of Information

Technologies named after Muhammad Al-Xorazmiy,

Jakhongirbek Khabibullaev

Tashkent University of Information

Technologies named after Muhammad Al-Xorazmiy

Abstract: *Internet of Things technologies have become an integral part of business and public life. This technology can be seen in almost every major city in Russia. Many leading countries are at a relatively high level of mass implementation of Internet of Things technology. Many areas of activity of the country directly depend on the Internet of Things: "smart home", "smart city", digital agriculture, automation of production, etc. At the same time, it is necessary to take into account that the diversified use of technologies entails a special interest of attackers and an increase in security threats. In this regard, experts have a question of ensuring security. This article discusses the characteristics of Internet of Things devices, the main security threats of narrowband Internet of Things and recommendations for countermeasures.*

Keywords: *Internet of Things, NB-IoT, cybersecurity, security threats, computer security*

The Internet of Things (IoT) is one of the biggest and fastest-growing inventions of the last decade, and the growth of this industry can be measured by the massive number of devices connected to the Internet of Things. In developed countries, devices connected to the Internet of Things have become a part of everyday life in many ways. By the end of 2019, the number of these devices connected to the IoT network exceeded 26.66 billion and continues to grow, with 127 new devices connecting to the Internet every second worldwide [1].

ISSN 3060-4567

What does this ever-increasing number of devices mean? The more devices connected to the IoT network, the more vulnerable it becomes to various security threats and risks. Many of the IoT devices connected to the Internet process data of an extremely sensitive nature, which should only be accessed by authorized personnel. These applications are computer programs that, most of the time, rely on real-time conditions to ensure that tasks are completed successfully. One of the reasons for vulnerability to security risks is that manufacturers of devices connected to IoT networks do not consider privacy or security of the device and data as a priority. Therefore, many users, without knowing it, still buy these devices and connect them to the IoT network, increasing the risk of security breaches, etc. [2].

Characteristics of IoT Devices

We are going to discuss some characteristics of IoT devices that pose a high security risk. By identifying the characteristics that lead to the problem, one can find a solution to the problem. However, even a basic definition of the Internet of Things can give an understanding of what is the root cause of security threats.

The Internet of Things is a collection of billions of devices around the world connected to each other via the Internet. Not only that, these IoT devices are also connected to the cloud through the World Wide Web to exchange data with other IoT devices and thus become vulnerable to hackers around the world. Some of the key characteristics of IoT devices include:

- Real-time data collection to perform their tasks,
- Always using LPWAN cellular network, which is also called Narrowband IoT and LTE-M,
- Measuring physical parameters and the ability to perform physical actions,
- Always connected to the cloud,
- Ability to make decisions independently based on available data [3].

Security Threats of Narrowband IoT

The characteristics discussed above give us an idea of the challenges that the narrowband IoT faces. Now, we are going to discuss these many challenges and the

ISSN 3060-4567

reason why many IoT devices face problems. One of the biggest misunderstandings in the market related to IoT security is that the very concept of security means only enhancing the security of IoT devices, while much more is required [4]. When we say "Internet of Things", we mean the complete system, not just the devices in daily use. This system includes the device itself, the cloud, the mobile application that is used to manage the device, the network interface to which the device is connected, and the software; besides this, the operation of the system, the use of encryption, authentication, and finally the physical security of both the device and all other physical components. Thus, along with the IoT device, all these system components are equally vulnerable to the threats and security issues that we are going to discuss [5]. Let's now delve into these issues one by one.

As the English phrase goes, "A chain is only as strong as its weakest link." The case of IoT systems is very similar. No matter how good the overall security is, if you use a device with poor security, the entire system can be easily hacked [5]. The same goes for application security. Poorly secured applications and end devices make systems vulnerable to cyber attacks. One of the main reasons is that most of the device manufacturers are the same manufacturers who made devices before the advent of IoT, and now they have made their devices smart to connect to IoT, but have not taken into account the security issues because it is an unimportant feature for them. Similarly, the case is with application developers. However, security is an important feature of a device or application in an IoT system [6].

As discussed earlier, all IoT devices require some form of authorization or authentication to protect them from data theft or other security threats. But even to this day, most devices released on the commercial market come with processors so small that they are only designed to perform very simple tasks and cannot handle something like authorization or authentication, which would require a larger processor. You might wonder how much computing power would be required for such a simple task as authentication, but you would be mistaken if you thought most commercial devices were capable of this at all [7].

ISSN 3060-4567

The whole idea of the Internet of Things is to create modern and smart cities, where every device in every home communicates and exchanges data with the system to manage the system intelligently. This means that most of the IoT devices are in urban areas and are accessible to the public. Moreover, the urban infrastructure can sometimes be very complex and dense to the point that it is impossible to ensure the physical security of the system. This increases the risk of a physical attack. We do not mean that some criminal can literally damage the system, but hackers can easily access the IoT system, which is in the public domain, in order to steal data and disrupt the operation of devices [8].

A smart device is a device that has some basic built-in features such as a microphone, camera, night vision, etc. that are necessary to receive, transmit data, and interact with the user. These features act as the eyes and ears of the device and continuously record terabytes of data, sometimes without the knowledge of the user using the device. Such data can be very sensitive and if it falls into the wrong hands, it can violate the user's privacy and become a serious security threat. This is one of the main reasons why people cannot trust the IoT systems, and there have been hundreds of reported cases of data collectors abusing the information and violating many data privacy laws [9].

When you buy a new IoT device or any other device, it usually comes with a default username and default password that you use to log in to the device for the first time. This default username and password are called default credentials and can pose a huge security risk. Some of the IoT devices even to this day come with hard-coded passwords and usernames, which means that these credentials can never be changed and are sometimes imprinted on the device. This makes the device vulnerable not only to cyber attacks but also to physical attacks where someone can gain access to the default username or password. Some users do not change these credentials at all, making their devices even less secure. Hackers always try to gain access to devices using the default username and password [10].

Countermeasures to Narrowband IoT Security Threats

ISSN 3060-4567

There are a number of countermeasures that can be taken to ensure the security of IoT systems. These countermeasures involve everyone from the user to the manufacturers and app developers, etc. Here are some of the steps that each of us should take before switching to IoT-connected smart devices.

The first and most important step that manufacturers and app developers need to take is to understand the importance of security in IoT devices and start considering it as a priority rather than a feature. All new IoT devices that are manufactured and all IoT applications that are developed must be secured from end to end and prevent data leakage. As a user, we can do the following to ensure the security of the applications and endpoint: When purchasing devices or installing an application, we must ensure that it is from a trusted manufacturer or developer. Most of the brands in the market are reliable in terms of safety, the problem arises only when manufacturers from local markets try to promote their product without paying attention to safety [11].

The second most important step to take is the need for authentication and authorization when using smart devices connected to the Internet of Things. Manufacturers and developers must ensure that their devices and applications support secure authorization and authentication.

Users must also ensure that the device they buy has this feature built-in. For devices that are already working but do not support even basic features such as authentication and authorization, secondary applications and devices can be used that provide additional security in the form of authentication or authorization. The user must also ensure that they do not purchase devices with hard-coded default credentials so that they can change their logins and passwords as soon as they receive the device.

From a data perspective, user data is one of the main components that increases risk and must be transferred in a secure manner. Data collectors and providers must make data security their top priority and ensure that data is transferred securely from one device to another. Governments around the world have a huge role to play at this stage and they need to make sure that data providers, app developers,

ISSN 3060-4567

etc. do not misuse user data. Specific laws and regulations need to be created to prevent these people from misusing publicly available data [12].,

Another important step that needs to be taken is to ensure that there is a monitoring system that monitors the entire system from the device endpoint to network security. In case of an excess, it will always find the weakest link in the chain and take action to prevent the situation from happening again. The application used in IoT systems should have built-in functions to record data deviations and then report them so that the user can take appropriate action. Last but not least, it is necessary to create a multi-layered system to protect the IoT system, which in itself is a complex interconnected system. These multiple layers should include administrative, technical and physical controls that are always in place to protect the IoT network from any adverse factors and are always ready to take action. Without a sufficient level of security and data protection, the Internet of Things cannot and will not remain successful in the long run and will inevitably fail. Therefore, management, manufacturers, developers and users themselves must make security the number one priority when working with devices connected to the Internet of Things.

LITERATURE

1. Maayan G.D. The IoT Rundown For 2020: Stats, Risks, and Solutions. Security Today. 2020. pp. 1-4. URL: securitytoday.com/Articles/2020/01/13/TheIoT-Rundown-for-2020.aspx

2. Malan J., Eager J., Lale-Demoz E., Ranghieri C.G. and Brady M. Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape. Centre for Strategy & Evaluation Services LLP. 2020. pp. 1-102.

3. Ugwuanyi S., Paul G. and Irvine J. Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks. Electronics. 2021, №10(2224). pp. 1-30.

4. Langkemper S. The Most Important Security Problems with IoT Devices. Eurofins Cyber Security. 2020. URL: eurofins-cybersecurity.com/news/securityproblems-iot-devices/.

ISSN 3060-4567

5. Heubl B. How to hack an IoT device. Engineering and Technology. 2019. URL: eandt.theiet.org/content/articles/2019/06/how-to-hack-an-iot-device/.