A Study of the Advances in IoT Security

Mr. Sanjay Kumar Sarangi , Mr. Sandip Kumar Bala

Department of Master in Computer Application, College Of Engineering Bhubaneswar, Odisha, INDIA.

ABSTRACT

The Internet of Things (IoT) improves the efficiency of common objects and eliminates tedious jobs, which brings many advantages to our lives. You may not be aware of the extent to which transferring your data over the internet puts your privacy at danger, but you are entrusting the manufacturers with power over your device and personal information. When gadgets are limited by numerous factors that hackers can use to access your data, the internet of things might not be as safe as you believe. Since the internet of things is all about linking devices together, one weak point can affect any device and anything they are connected to be sufficient to obtain complete access.

Key Words: Internet of Things, SaaS, PaaS, Asas, Service Oriented

1. INTRODUCTION

The internet-of-things, which consists of billions of physical objects that communicate wirelessly, is the means by which physical objects are connected to one another. With an anticipated 8.4 billion linked devices in 2017, the Internet of Things is expanding quickly. By 2018, this number is expected to have increased by 31%.IoT functions by using sensors, processors, and communication technology to gather data from the physical environment and then acting upon it. These gadgets, which are frequently referred to as "smart" gadgets, can communicate with one another via communication protocols. After that, use the data that was obtained. The internet-of-things is a very broad concept that encompasses many different sectors, each with its own unique architecture depending on its requirements.

IOT ARCHUTECTURE

A. Layers

Three fundamental layers make up the IoT architecture, albeit they may vary depending on the use case and the need for additional levels in certain industry solutions.

B. Preception

The physical components of the perception layer include your sensors and actuators, which communicate wirelessly with other devices and the outside environment to deliver and receive data. The goal of this layer is to gather as much data as possible from its actuators and sensors which the network layer can receive.

C. Network

In addition to handling data transmitted between servers and smart devices, the network layer can also be used to send and transform perception layer data into a format that is usable by the recipient device.

Some claim that this is where the Internet of Things takes place because it connects the physical and digital realms and permits them to communicate with one another. This layer processes and routes data using a variety of technologies (such as switches, routers, and cloud computing) before sending it to the appropriate application layer so that it can be read.

Application

The network layer converts the data from the sensors and actuators into a readable format before sending it to the application layer, also known as the business layer, which provides the users with certain services. After that, the application layer can use this data to deliver services or carry out tasks dependent on the information it has received. In order to make predictions or identify trends, this layer can analyze and retain the data it receives.

ENABLING TECHNOLOGIES

A. Hardware Platforms

IoT development kits and hardware platforms are widely accessible. For solutions with simpler duties that would demand less power, the devices with lower specifications would be perfect processing power and will be more affordable, making them more cost-effective than utilizing a device with high specs.

B. Communication

For IOT to function, data must be able to be transmitted between devices in order for them to collect the necessary data and to receive instructions based on the data that has been sent. There are both short- and long-range standards, and the device may use a variety of communication technologies depending on how it is deployed.

C. Cloud solutions

The internet-of-things depends heavily on cloud solutions because they provide universal access to a common resource pool. Through the network layer, all devices in the perception layer can transmit data for analysis and access by the application layer. Different cloud computing technologies are suitable for different kinds of solutions. Some of the most used providers as well as their features.

1) IaaS

Infrastructure as a Service is a business model in which an entity rents out specific services on a "pay as you go" basis that are required for their solution. In contrast to other services where you rent all of their services for a set sum even if you don't use any, you will only pay for what you use with this one.

2) PaaS

The goal of platform as a service is to expedite the development process by giving pre-configured components, such as databases, application servers, and programming languages, to enterprises and organizations and handing over system maintenance to the provider.

3) SaaS

Software as a service, or SaaS, is a type of cloud computing service that provides software on demand that is hosted and maintained by the provider. SaaS often requires a membership and can enhance teamwork and communication.

2. IOT DEVICE CONSTRAINTS

A. Power Consumption

Devices are made with a purpose in mind and are designed with that function in mind. Furthermore, a device's power consumption will increase the more tasks it needs to complete, such storing and gathering data. A device's power requirements will increase when it has additional security added to it.

Processing

The necessity for processing on a device to carry out both the intended function and additional security, which may need the installation of more gates, transistors, and modules, is another barrier to implementing greater security.

B. Design

A device's design is also limited because its size may need the addition of additional modules or transistors, which will increase the complexity and size of the design. Cost and effectiveness considerations during implementation could make the method unfeasible for widespread use. Simulators can be used to test and optimize designs prior to construction, which lowers costs and improves device efficiency.

IOT DEVICE EFFICIANTCY

One advantage of increasing a device's efficiency is that it will require less energy or resources to do the same function, which will save money.

A. Code compression

When combined with encryption and integrity checking to secure processor memory transactions, code compression can be used to increase a device's performance and power consumption. It can also lower the memory footprint and provide more information per memory access.

IOT DEVICE SECURITY

The proliferation of IoT devices has many benefits for organizations and consumers alike, streamlining several procedures, but there are drawbacks as well. One of these drawbacks is security and privacy; when our private information, such as financial details, location, and activity, is shared among devices, we run the danger of losing a great deal of privacy.

Authentication

1. ***Noise Insertion***

The goal of noise cancellation is to safeguard raw data while its inside the CPU to prevent data retrieval through side-channel assaults by an adversary. While this approach isn't as safe as encryption, it has the advantage of being quite lightweight. It functions by introducing noise using a key for sensitive data. You may keep the data safe within the device and cut out needless overhead by choosing crucial spots where the data noise is canceled out, making it easy to read.

2. ***Logic Locking***

A relatively new technique called logic locking involves including additional gates in the design to lock "Key gates," which would alter the output and effectively lock the gates' proper operation.

A. Detection & prevention

1. ***Security Auditing Mode***

The security auditing module, when included in a security architecture, is meant to monitor both external and internal activities in order to assess the stability of the device, thereby preventing damage to the device, alerting the network to any critical issues with the device, and identifying security threats.

2. ***Attack Detection Unit***

The attack prevention unit's job is to identify when a device is being attacked and notify the device of the attack so that it can avoid being hacked or damaged.

This is accomplished by keeping an eye on the communication controller's electrical signals, which are used to identify any anomalies in the physical properties of the bus communication between the central module and the main device. This is separate from the main device, so it won't affect its processing speed, and it can be used with a communication controller on a variety of devices.

3. ***Random Canaries Repository***

RSR attempts to defend against stack smash attacks, which take use of buffer overflow flaws to take over a program. By generating a repository of random canary values, which are used when

the application detects an attack, RCR improves Stack Smash Protector by making the attack more difficult.

B. Isolation

1. Secure sensing

Hardware isolation has led to the suggestion of a sensor architecture that will shield a device's sensors from hacked applications. ARM processors' hardware isolation capability and the deployment of a sensor IP into the isolated area—which is shielded from hacked applications—are used to accomplish this.

We are able to share sensor data as needed by implementing shared memory in the regular world that is accessible to the secure world.

Secpage

Secpage is a lightweight hardware and software architecture designed to safeguard sensitive code and data by creating an isolated memory environment within the device. This security technique lowers the overhead of the architecture implementation by giving compromised systems software access to pages that don't need to be secure while also providing a safe, isolated, and trusted environment to prevent data and code access by unauthorized users.

3. COCLUSION

As we can see, security is a major concern with IoT, and as it spreads to many different sectors and services, like healthcare and business, security will become even more crucial to safeguarding private information and gadgets from harm. The perception layer is by far the most vulnerable because it is used in real-world applications, is typically embedded into products that can be disassembled and tampered with, and is typically connected to other devices via the network layer, which can be used to transmit or steal malicious data.

Since devices are typically limited by factors like cost, design, and efficiency, we are unable to add the highest level of security without incurring additional costs or making the deployment impractical. Instead, we must invest in more affordable, lightweight security measures that are unable to thwart attacks. IOT offers a lot of advantages, but it's expanding quickly.

4. REFERENCES

1 J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol.4, no. 5, pp. 1125-1142, Oct. 2017. doi: 10.1109/JIOT.2017.2683200

2.D. A. H. Shehab and O. A. Batarfi, "RCR for preventing stack smashing attacks bypass stack canaries," 2017 Computing Conference, London, United Kingdom, 2017, pp. 795-800. doi: 1109/SAI.2017.8252186

3. E. W. Netto, R. Vaslin, G. Gogniat and J. P. Diguet, "A Code Compression Method to Cope with Security Hardware Overheads," Computer Architecture and High Performance Computing, 2007. SBAC- PAD 2007. 19th International Symposium on, Rio Grande do Sul, 2007, pp. 185-192. doi: 10.1109/SBAC- AD.2007.40

4. F. Ye and Y. Qian, "A Security Architecture for Networked Internet of Things Devices," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6. doi:10.1109/GLOCOM.2017.8254021

5.K. Liang, Y. Feng, J. Wei and W. Guo, "SecPage - A Lightweight Memory Protection Architecture," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016, pp. 1917-1922. doi: 10.1109/TrustCom.2016.0293

6. M. Ye, N. Hu and S. Wei, "Lightweight secure sensing using hardware isolation," 2016 IEEE SENSORS, Orlando, FL, 2016, pp. 1-3. doi: 10.1109/ICSENS.2016.7808904

7. Y. W. Lee and N. A. Touba, "Computing with obfuscated data in arbitrary logic circuits via noise insertion and cancellation," 2017 IEEE Conference on Dependable and Secure Computing, Taipei, 2017, pp. 146-152. doi: 10.1109/DESEC.2017.8073840 R. Jinnai, A. Inomata, I. Arai and K. Fujikawa, "Proposal of hardware device model for IoT endpoint security and its implementation," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, 2017, pp. 91-93. doi:10.1109/PERCOMW.2017.7917533