Securing IoT Devices Data Utilizing Machine Learning Approach

Project 2

By: Jasmine Roberts

Bowie State University

CTEC 402-001 Software & Operating Systems Security

Dr. Haydar Teymourlouei

March 2nd, 2023

# 

[Introduction 3](#_7d00w0gw6uni)

[Problem Definition 3](#_33eof2p4ecir)

[Research Questions 3](#_ulri76ohbef1)

[Research Purpose 4](#_mzssass2jwah)

[**Methodologies 6**](#_4clv7f1g24ms)

[Method 1: Strong Password Use 6](#_6uj0laeumv9z)

[Method 2: Two-Factor Authentication 6](#_peeg7genxm07)

[Method 3: Blockchain Technology 8](#_kvnh9rwxoier)

[Method 4: Q - Learning 9](#_rq2etlfrhp56)

[Method 5: Extended Detection and Response (XDR) 10](#_6flaqhj63hie)

[Method 6: Update firmware/software and install patches 11](#_gskv377va50c)

[Method 7: VLAN network segmentation 11](#_m81vejo9v1hs)

[Method 8: Azure IoT Hub 12](#_h2w48wmapcjx)

[**Summary 13**](#_qce3hvu8e81a)

[**References 14**](#_6ai36euqw6ad)

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# Introduction

IoT (Internet of Things) devices are often described as physical objects that have sensors, processing abilities and software. When it comes to your IoT devices data security it can be tough because usually in this day and time we use multiple devices on a daily basis and cannot secure all of them at once. (*What Is IoT? - Internet of Things Explained - AWS*, n.d.)IoT devices and its data can be easily vulnerable just because the users aren’t aware of many protection methods. Complications with many IoT devices include the lack of security protection, poor vulnerability testing, weak passwords, and lack of visibility. (*IoT Security Challenges and Problems*, n.d.)

In our research project, we are going to provide information and display credible methods, software, and tools to help secure IoT Devices and its Data .These methods, software, and tools are a way of mentoring your data to keep it secure. We are going to display easy read instructional steps and screenshots to demonstrate how to use and the benefits of the methods that we conducted. These methods will be descriptive enough to where they can be easily accessible for use at any convenience. Throughout our research project, everything that is included is carefully documented, credible, and worth the access.

# Problem Definition

As stated before, securing IoT Devices Data can be difficult. There are so many IoT devices that are in use all around the world. By there being numerous devices in use there is some difficulty with securing itself and its data. One problem is that users aren’t aware of free open-source software and methods to help with security. The second problem is that the users of IoT ignore the fact that their IoT device and its data is highly recommended to have security until a vulnerability happens. In other words, something bad (vulnerability) has to happen to them in order for them to get security. In our research project, the free open-source software, and methods within the IoT will be easy instructional steps and screenshots to demonstrate how to use and the benefits of the methods that we conducted.

# Research Questions

1. What does the IoT entail?
2. What are some challenges of securing IoT devices?
3. Why is it important to secure IoT devices?
4. What are some of the technologies included in the IoT?
5. What are some goals of IoT security?
6. What is some software’s that have been created to ensure that the IoT will be secure?
7. Are some devices harder to secure than others?
8. How can people be made aware of the need to secure IoT devices?
9. How can IoT vulnerabilities affect its users?
10. Where can users find information regarding IoT device security?

# 

# 

# Research Purpose

The purpose of research is for awareness and to supply creditable methods to help secure IoT devices and their data. Many devices such as Cell Phones, Tablets, laptops, Desktops, SMART Watches, SMART TVs, etc., all have a risk of having a vulnerability and they all consist of an IoT device. Conducting research can be a helpful tool to have better security for your IoT device, and you will have credible information. The main reason to have a secure IoT device is to preserve your privacy, and confidentiality, and double ensure the security of its users, and its data**.** As far as awareness is concerned, users aren't aware of the free open-source software that can help with securing your IoT device and its data and promote safe IoT usage.

**Case Study**

The specific Internet of Things case study that we decided to research was dealing with Google's Nest Thermostat. The Nest thermostat can boot from a bootable USB stick inserted into its USB port when the hard reset button is pressed, putting it into device firmware update mode. The attackers used this feature to upload their customized images into the ROM of the target device. The first stage bootloader, x-loader, and the second stage bootloader, u-boot; and the ramdisk technique was used to load the file system into memory. The attackers altered U-boot to set up the environment for running the component with the specialized ramdisk. u-boot runs Linux mounts and modifies the Nest device's existing file system using the attacker's ramdisk, granting root access. In order to access the thermostat, the Secure Shell server Dropbear was next installed on the target device. After that, the attacker continued by injecting the Odysseus malware, which allowed it to connect remotely to Achaea, the attacker's server, and avoid network address translation in order to join the home network. Now, the thermostat controls the entire home network by acting as a botnet. Profiling the members of the household, engaging in unauthorized surveillance, and obtaining embarrassing images and videos of the people are all consequences.

Typically, in boot process hijacking, an attacker tries to stop a device from starting normally by taking advantage of any weakness in its boot path and replacing the boot images with customized boot images. The attacker could take advantage of the thermostat's device firmware update feature to boot from a USB device because no integrity check was performed on the types of images being loaded into ROM. The attacker could then gain remote access to the device, install malicious software on it, and access the home network. If sufficient authentication mechanisms are in place from the very first run of the code, a secure boot based on a chain of trust can be established to counteract this attack. To enable secure boot support, this necessitates replacing the built-in processors with customized hardware. One source of these attacks in IoT devices is the absence of integrity checks on the software images being loaded into the device, as well as insecure software application programming interfaces and hardware interfaces. In order to connect and communicate with application developers and other users, IoT devices may offer insecure APIs, putting them at risk of malicious code injection attacks from untrusted parties. Input validation, IP address filtering, and other well-known best practices for protecting API endpoints can be used to prevent such attacks.



# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

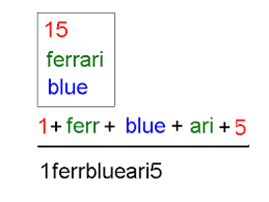
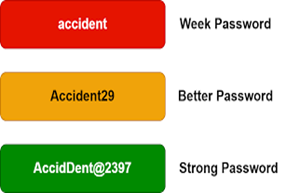
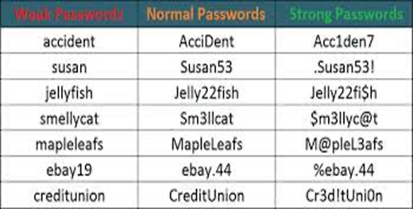
# Methodologies

## *Method 1: Strong Password Use*

***Articles:***

1. ***The Importance of having strong passwords for your organization,DHoof***
2. ***How to Secure IoT Devices and Protect Them from Cyber Attacks, 2022***

To secure IoT Devices and their data, one way is Strong Password use. A strong password consists of being unique, and lengthy for each of your IoT devices to protect itself and its data. It is also recommended to not overuse it, such as using the same password for each device. Using a common and simple password is putting your IoT device at risk and can open a door to vulnerabilities. Having a strong and secure password is the best defense against securing your IoT Devices and their data. A strong password should be at least eight characters long and include a mix of uppercase and lowercase letters, numbers, and symbols. It’s not recommended to use easily guessed words like “password” or easily accessible personal information like your birthdate. We as users mostly pick passwords that are easy to remember but that is also not recommended. (*How to Secure IoT Devices and Protect Them From Cyber Attacks*, 2021) The more complex your password is, the greater the chance your information is protected. A strong password can also increase the protection from Phishing attacks, which means that your password is easy to be preyed on during this attack. (*The Importance of Having Strong Passwords for Your Organization*, 2022)

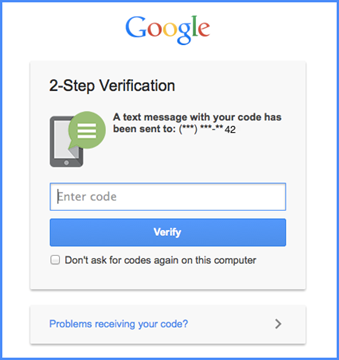
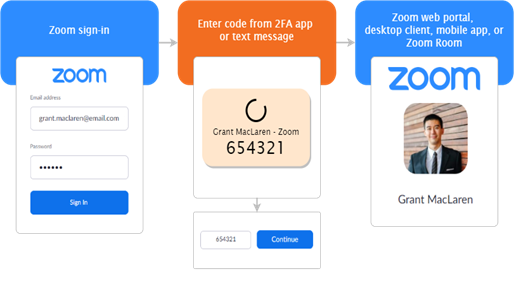
**** *Examples of Weak, Normal, and Strong password use. How to create a strong Password. Examples of Weak, Better and Strong Passwords.*

## *Method 2: Two-Factor Authentication*

***Article:***

1. ***Two Factor Authentication for Apple ID, Apple***

When you are using your IoT device, there’s a strong possibility a hacker will try to crack your protection and steal your credentials and personal information. You can prevent this by using Two-Factor Authentication, for your IoT device, which accounts for where you keep your personal information. Having a Two-Factor Authentication hackers will not be able to get your personal information because they will not have a secret code to log in. Two-Factor Authentication consists of a code that will be sent to you via SMS, to log inside of your information. This means if the hacker doesn’t have your phone/device, they cannot log in or use. This will protect your IoT device and its data. (James, 2021). Using Two-Factor Authentication, it's an extra layer of security, in other words it's making sure that you’re the only one accessing your information. (*Two-Factor Authentication for Apple ID*, 2022)



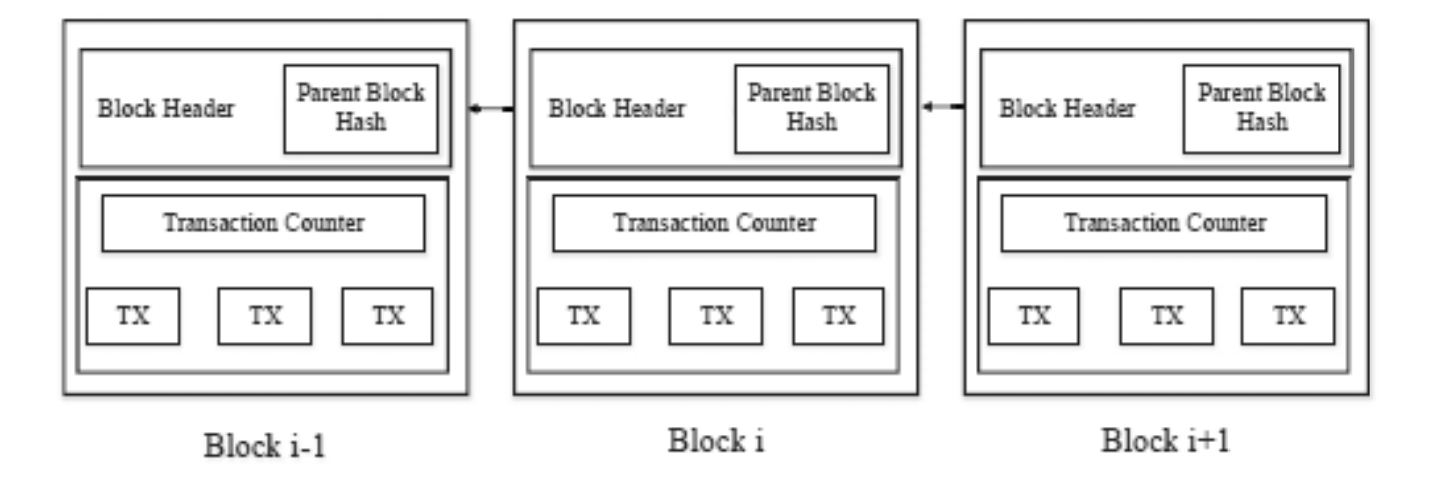
*Two-factor Authentication including Zoom Client, Google Account, Ring Doorbell, and Apple ID Account.*

## *Method 3: Blockchain Technology*

***Article:***

1. ***Secure IoT Communication using Blockchain Technology,D. Fakhri and K. Mutijarsa,***

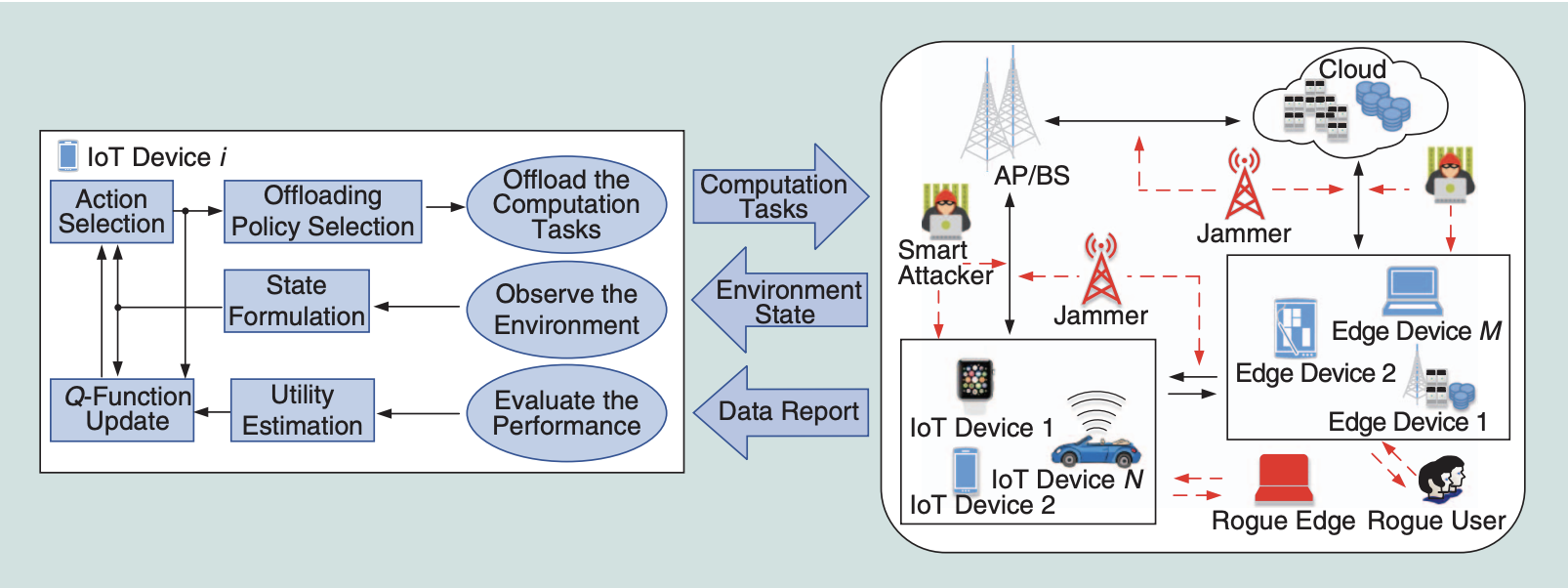
Since Bitcoin made blockchain popular, it has also been developing at a rapid rate. Blockchain technology can be used to address IoT security issues. Creating secure communication between IoT devices is one method of achieving this. Blockchain technology was initially applied to prevent transactional double-spending. Blockchain technology started to be applied to other fields over time, including IoT, healthcare, and transportation. With the aid of embedded systems, sensors, software, and artificial intelligence, the Internet of Things is a device that connects various items in a network to obtain data from the internet for use in a variety of intelligent applications. Each connected device will have a distinct identity of its own. Despite the fact that IoT offers many advantages to humans, it also poses security risks. Hackers are attempting to retrieve sensitive data from these IoT devices.

The phrase "blockchain" is frequently used to describe data structures, networks, and occasionally systems. A blockchain is a list of blocks in a particular order, each containing a transaction. Each block in the blockchain contains a hash from the previous block and is linked to it. As a result, altering or deleting the blockchain's transaction history would require altering the entire blockchain's data. Blockchain is secure from hackers because of this. There are a couple of distinctions to the blockchain. The first is Audibility, which means the previous transaction is referred to in every blockchain transaction. This makes it simple to track and verify each transaction. The second would be Anonymity, which entails using a generated address, each user on the blockchain network can communicate with another user. As a result, during the interaction, the user's true identity is hidden. Next, decentralization, to verify transactions in the blockchain, third parties are not required. On blockchain networks, consistency algorithms are employed to preserve data. Lastly, Persistence blockchain allows for quick transaction validation, and invalid transactions are not picked up by miners. Therefore, transactions that have already happened cannot be deleted.

*Example of a blockchain structure*

## *Method 4: Q - Learning*

Q-learning is an easy-to-implement reinforcement learning method with minimal computational complexity. IoT devices, for instance, can choose their offloading data rates to protect themselves from jamming and spoofing attacks by using Q-learning-based offloading. Each time slot's Q-values are updated using the iterative Bellman equation in accordance with the current offloading policy, the state of the network, and the jamming protection the IoT device has received. The Internet of Things (IoT) device calculates the utility for this time period by analyzing the signal-to-interference plus noise ratio of the transmitted signal, secrecy capacity, offloading latency, and energy consumption of the offloading process. The IoT device uses the e-greedy algorithm to select an offloading policy, choosing the offloading policy with the maximum Q-value with a high probability while choosing the other policies with a low probability. The Internet of Things device thus chooses between exploration and exploitation. This plan lowers the rate of jamming and spoofing by 8% and 50%, respectively.

A Q-learning-based anti jamming transmission states that an IoT device can use Q-learning to select the radio channel to connect to the cloud or an edge device without being aware of the jamming and interference model in IoT systems. The IoT device formulates the state by observing the center frequency and radio bandwidth of each channel, then selects the best offloading channel based on the Q-function and the current state. The IoT device assesses the utility after receiving the computation report and updates the Q values. Results reveal that when compared to the benchmark random channel selection strategy, this scheme raises the average cumulative reward by 53.8%. In order to avoid interference and jamming from other radio devices, Q-learning also assists IoT devices in obtaining the best subband from the radio spectrum band.

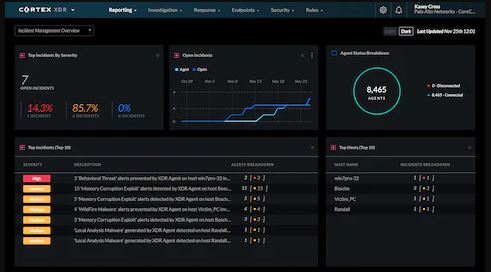
*An illustration of ML-based offloading*

## 

## *Method 5: Extended Detection and Response (XDR)*

Extended Detection and Response or XDR can deliver visibility into data across networks, clouds, endpoints, and applications, at the same time applying analytics and automation to detect, analyze, hunt, and remediate the incoming present and future threats. Now how does XDR work? Well, it collects and correlates data across email, endpoints, servers, cloud workloads, and networks, this enables visibility and context into threats that are more complicated. The incoming threats can and will be analyzed, prioritized, hunted, and remediated so that they can prevent data loss and have security breaches less likely to happen.

There are three parts to XDR which are telemetry and data analysis, detection, and response. Telemetry and data analysis have XDR monitors and it collects data across multiple security layers. It uses data analysis that does data analysis that correlates context from different alerts. Detection is why XDR has superior visibility which allows it to sift through alerts and then report on the ones that need a response. This strong visibility allows it to make baselines of normal behavior inside of an environment which then enables the detection of threats that leverage software, ports, and protocols. Detection will investigate the origin of the threat and stop it from affecting the system. The response is the last part; it has the capability to contain and remove threats it detects and it also updates security policies that prevent similar breaches from happening again. The response goes beyond endpoint protection, it responds to threats across all the security control points it touches, from container security to networks and servers.



*XDR in use demonstration*

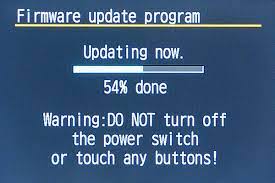
## 

## 

## *Method 6: Update firmware/software and install patches*

Software updates and patches for an OS help because the vendor will release a new software that fixes performance bugs, as well as to provide enhanced security features. Software updates and patches become available by the Vendors when they put them on their website for users to download or it can show up as an alert. Attackers may still target vulnerabilities for months or even years after updates are available. Some software updates give the user an option to make the update and some updates are done automatically.

Make sure the website is the official website, Don’t trust a link in an email message. attackers have used email messages to direct users to websites hosting malicious files disguised as legitimate updates. Also be cautious when an email message may read that the software update files are attached, those are most likely containing malware. If automatic options are available, the Cybersecurity and Infrastructure Security Agency (CISA) recommends that you take advantage of them. If they are not available, periodically check your vendor’s websites for updates.



*A device that’s uploading firmware.*

## *Method 7: VLAN network segmentation*

“VLAN network segmentation can create a collection of isolated networks within the data center. Each network is a separate broadcast domain. When properly configured, VLAN segmentation severely hinders access to system attack surfaces. It reduces packet-sniffing capabilities and increases threat agent effort. Finally, authorized users only “see” the servers and other devices necessary to perform their daily tasks” *(Olzak, 2021).* Authorized users can only see the servers and other devices that are needed to do daily tasks. VLAN network segmentation can do protocol separation.

The Network architects can limit certain protocols to certain segments of the enterprise. So, for example if the AppleTalk system exists on your wire, they can have their own VLAN in which to operate. This limits traffic in each VLAN to relevant packets. The VLAN allows secure and flexible user mobility. For example, a user that is assigned a specific VLAN can connect to the VLAN no matter where they are. You configure VLANs using layer two technology built into switches.

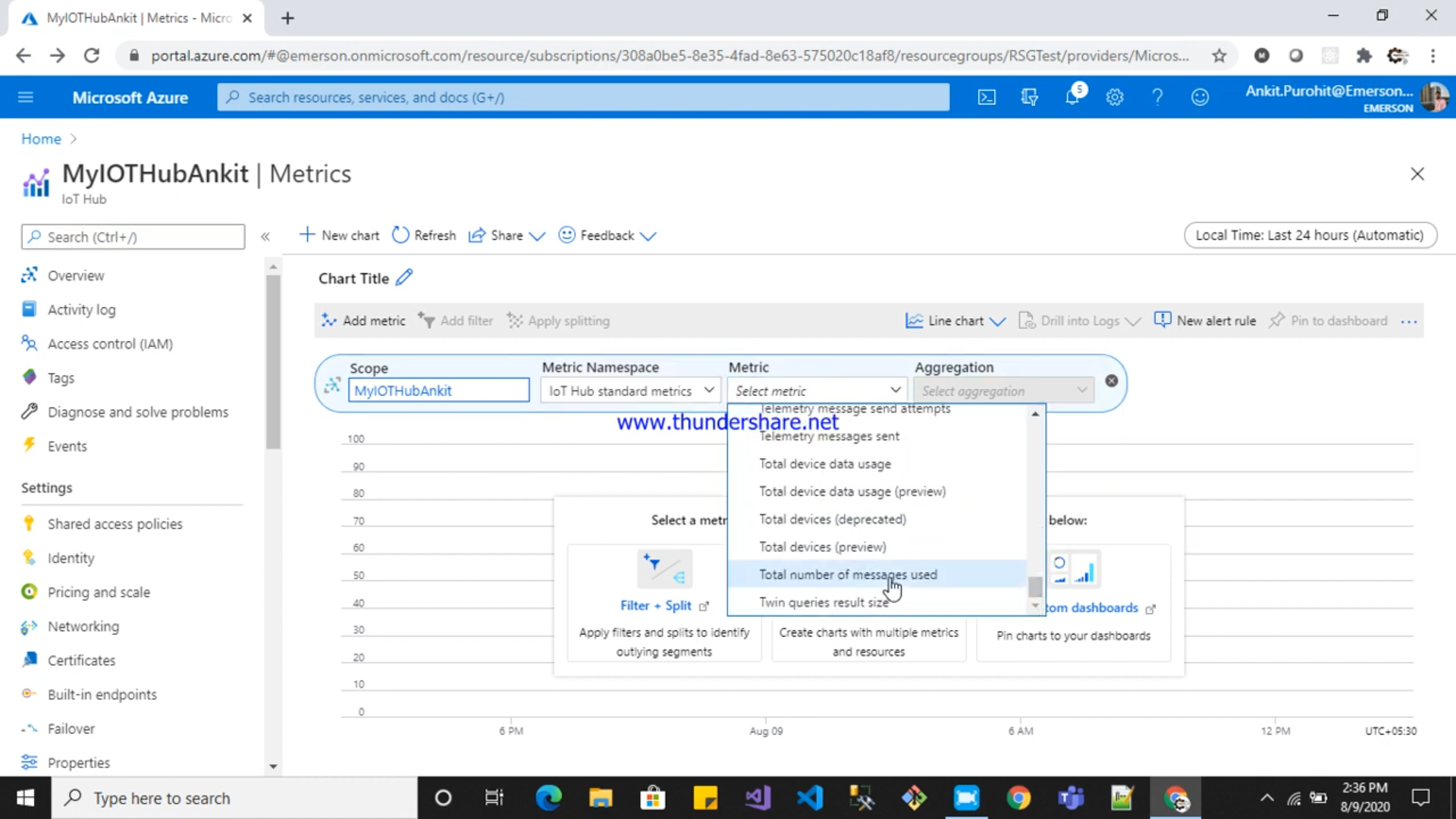
## 

*Schematic of the VLAN configuration.*

## *Method 8: Azure IoT Hub*

“Azure IoT Hub is a managed service hosted in the cloud that acts as a central message hub for communication between an IoT application and its attached devices. You can connect millions of devices and their backend solutions reliably and securely. Almost any device can be connected to an IoT hub”(kgremban, KennedyDMSFT, Ushe-Rathnavel, paweenatongbai, dominicbetts, v-gpettibone, 2022). Different messaging patterns are supported which includes device-to-cloud telemetry, uploading files from devices, and request-reply methods to control your devices from the cloud. The hub can support monitoring that helps you track device creation, connection and failure.

You can add more services to the azure IoT hub which are “Azure Event Grid to enable your business to react quickly to critical events in a reliable, scalable, and secure manner, Azure Logic Apps to automate business processes, Azure Machine Learning to add machine learning and AI models to your solution, Azure Stream Analytics to run real-time analytic computations on the data streaming from your devices” (kgremban, KennedyDMSFT, Ushe-Rathnavel, paweenatongbai, dominicbetts, v-gpettibone, 2022). You add more service to Azure IoT hub by scaling which allows millions of simultaneously connected devices and millions of events per second to support your IoT workloads.



*Azure IoT Hub UI.*

## Summary

Technology is amazing because it changes all the time. An enhanced security system is required as technology becomes more pervasive worldwide. Each organization has room for growth when it comes to maintaining the most recent hardware, software, and security protocols. IoT devices for consumers are typically not created with security in mind. The risks posed by these devices that are used in society are highlighted by the case study used in this essay. We provide a summary of these typical attacks, device vulnerabilities, and potential defenses. As our society becomes more dependent on IoT devices, security, and privacy considerations shouldn't be put off. Attacks like those described in this paper could have grave repercussions. Standards, mitigation techniques, ongoing testing and patching, and cross-sector partnerships are therefore urgently required to address both current and emerging security threats.

# 

# 

# 

# References

*How to Secure IoT Devices and Protect Them From Cyber Attacks*. (2021, June 08). Tech Target: IoT Agenda. Retrieved March 1, 2023, from https://www.techtarget.com/iotagenda/post/How-to-secure-IoT-devices-and-protect-them-from-cyber-attacks - :~:text=Pick a strong password and do not overuse it&text=Make sure to use a, essential to secure IoT devices.

*IoT Security Challenges and Problems*. (n.d.). Balbix. Retrieved March 1, 2023, from https://www.balbix.com/insights/addressing-iot-security-challenges/

James, M. (2021, November 17). *Ways To Secure IoT Devices from Cyber Attacks*. SmartData Collective. Retrieved March 1, 2023, from https://www.smartdatacollective.com/ways-to-secure-iot-devices-from-cyber-attacks/

*What is IoT? - Internet of Things Explained - AWS*. (n.d.). Amazon AWS. Retrieved March 1, 2023, from <https://aws.amazon.com/what-is/iot/>

30, J., 20, S., 14, S., & 15, J. (2021, June 2). VLAN network segmentation and security- chapter five [updated 2021]. Infosec Resources. Retrieved March 2, 2023, from https://resources.infosecinstitute.com/topic/vlan-network-chapter-5/

Kgremban. (n.d.). IOT concepts and Azure Iot Hub. Microsoft Learn. Retrieved March 2, 2023, from https://learn.microsoft.com/en-us/azure/iot-hub/iot-concepts-and-iot-hub

Understanding patches and software updates. TechWeb RSS. (n.d.). Retrieved March 2, 2023, from https://www.bu.edu/tech/support/information-security/security-for-everyone/understanding-patches-and-software-updates/#:~:text=Patches%20are%20software%20and%20operating,to%20provide%20enhanced%20security%20features.

*D. Fakhri and K. Mutijarsa, "Secure IoT Communication using Blockchain Technology," 2018 International Symposium on Electronics and Smart Devices (ISESD), Bandung, Indonesia, 2018, pp. 1-6, doi: 10.1109/ISESD.2018.8605485.*

*L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," in IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41-49, Sept. 2018, doi: 10.1109/MSP.2018.2825478.*