4-1-2023

Cybersecurity of the Cloud and IoT Devices

Caleb Cecil
University of Dayton

Cybersecurity of the

Cloud and IoT Devices

Honors Thesis

Caleb Cecil

Department: Computer Science

Advisor: Luan Nguyen, Ph.D.

May 2023

Cybersecurity of the Cloud and IoT Devices

Honors Thesis

Caleb Cecil

Department: Computer Science

Advisor: Luan Nguyen, Ph.D.

May 2023

Abstract

The next wave of computing is moving to the cloud. The cloud offers reliable, scalable, and cheap ways for companies to upgrade their business. It has revolutionized how we interact with each other today and is becoming an integral part of our everyday lives. However, when companies move to the cloud they need to set up their cloud architecture or data transmission securely. This leads to huge security risks in which sensitive data could be released. This project outlines the different threats and vulnerabilities that the cloud faces and the specifications needed for security. This research intends to evaluate the current security threats and their solutions to create a formal analysis that could be used when building all cloud architectures involving IoT devices to increase their security.

Acknowledgements

I would like to thank Dr. Nguyen and Dr. Phung for their support and guidance on this project. I would also like to thank the Honors Department for assistance in helping me complete this thesis. Lastly I would like to thank all my friends and mentors who encouraged me to embark on this project and inspired me to complete it.

Table of Contents

General Audience

The next wave of computing is moving to the cloud. The cloud offers reliable, scalable, and cheap ways for companies to upgrade their business. It has revolutionized how we interact with each other today and is becoming an integral part of our everyday lives. One of the most popular uses todays is for storage. Along with that many, companies are storing the data of their Internet of Things devices in the cloud. However, when they do this they do not set up their cloud architecture or data transmission to the cloud securely. This leads to huge security risks in which sensitive data could be released and could be catastrophic. This paper outlines the different threats and vulnerabilities that the cloud faces. It also surveys the current solutions to cloud security. Finally, it will create a generalized model and considerations that should be taken into account when creating cloud architecture. This model will be used in a case study to validate the efficacy of this cloud architecture.

Project Description

The research was split into three parts. The first part was creating a basic description of the cloud and the layout of its architecture and its use cases. Then it went in to describing what the Internet of Things (IoT) is and how it relates to the cloud. The cloud is simply an on-demand computing service. It allows people to host applications, and store or process data. Cloud architecture is how you combine these different things that it can do. Cloud architecture today uses a few models: Platform as a Service(PaaS), Software as a Service(SaaS), or Infrastructure as a Service(IaaS)[1]. The cloud allows

IoT devices to store large amounts of data from their sensors and also connect to many different devices.

The second part of the research was a survey of the different vulnerabilities that face the cloud and IoT today. Some Current vulnerabilities include Dos attacks, wrapping attacks, and cloud injection [1][2]. These attacks are just some of the many vulnerabilities that could be exploited. Finally, the project comes to see how we can formally verify security mechanisms for the cloud and IoT devices today.

This research intends to evaluate through formal verification the current security threats and their solutions that could be used in all cloud architectures involving IoT devices to increase their security. Through the course of the research, I was asked to present in a Ted style talk. This then shifted the focus of the paper to the speech. The speech was then adapted to fit the needs of this manuscript.

Honors Thesis Ted Style Talk

We live in a world today where everything is connected. We are connected to the world and can know the local news about small city in Ghana. We are connected with each other to where we can instantly message someone through various social media outlets. We are even connected to our cars through things like Apple car play. A lot of these things we are connected to need the internet to function. We call this the Internet of things or IoT for short. And “thing” can mean anything like a sensor on a machine in a factory or device from your phone to a watch to your headphones to even your fridge. These IoT devices also produce an immense amount of data. Data that you might want to store like your photos from your phone or data that you might want to stream like a

security camera feed. To do these things takes a lot of computing power, which is not cheap. So to do all these things we use the cloud. The cloud is on-demand computing resource. You can think about it like using someone else's computer that is better than yours. The cloud allows us to do things like back up our phones, use analytical tools like chat-gbt, or even stream our favorite shows. The combination of the cloud and IoT devices can enable real-time monitoring, control, and automation of various systems and processes, improving efficiency, productivity, and convenience.

Imagine you have a smart house. Your fridge, thermostat, voice assistant, and security cameras are all connected to the cloud. You are coming home from work and your fridge tells you that you are low on eggs. So you run to the store to grab some more and you get an alert that there was movement at your front door. You check the real-time footage and see that its just a package getting delivered. On the way home you feel a bit cold so you crank up the thermostat a little bit so that the house will be warm when you get there. When you get home, you tell your voice assistant to check your blood sugar from your insulin pump. Life is swell, or so you might think. A lot of these devices that are connected don’t have any security in them. What if a malicious person was able to “evesdrop” on your security feed? Now they know when you leave the house and what time you come back. Or they turned off the heating in your house in the wintertime while you were asleep. Not only would you be freezing cold when you wake up but your pipes might burst. Even the conversation you have in your own home can be monitored by the voice assistant. Even your insulin pump could be sending faulty data do your app not realizing you need insulin at a certain time.

This hypothetical may sound like a dystopian universe, but it is based on real attacks. The security feed being taped into happened during the Verkada hack in 2021 where hackers were able to access over 150,000 cameras [3]. In 2016 there was an attack that turned off the heating to two buildings in Finland [4]. The FDA had stepped in and have Medtronic recall their insulin pumps because they were exposed to hackers [5]. This calls to question what security *do* these things have. Evaluating the effectiveness of cyber security in IoT devices is essential for our safety because if not we are vulnerable in the most sensitive areas of our life.

One way to evaluate it would be formal analysis. It is a technique that is used to verify certain software. This can also be used to verify security systems as well. One major way we do this is by using temporal logic. Temporal logic is a way to specify properties over time. Take a light bulb for example. A light bulb can be in two states on or off and a light switch can turn on or off the lightbulb. We can specify what its behavior should be over time. Say if the light switch is turned on then the light bulb should be turned on within 3 seconds. This could be modeled by the equation $G(P \rightarrow F(Q))$ which says globally/always P, the light switch being on, will imply that in the future/eventually q, the lightbulb, will turn on. And we verify this over time, so after 1 second is it turned off after two, after 3. We test to see if our statement is what happens using verification software.

This same logic can be applied to cybersecurity. There are a few specifications we can focus on to ensure our devices are secure. One specification property is mutual authentication. That is both devices should authenticate each other to know who is accessing the data. This might look like your insulin pump authenticating the cloud

before sending the data to it and the cloud making sure it is not a rogue device. Protocols like Datagram transport layer security can be used. Datagram transport layer security works by sending digital certificates and authenticating those certificates. To formally verify this protocol, we would first define its transition states like when it should send a its certificate. And then we define what mutual authentication looks like. And then run an analysis on it. Another specification is Integrity. This is the assurance that the data has not been tampered with or modified in any way. An example of a system that does not have integrity is your fridge telling you only need one carton of eggs when you actually need two. To achieve this, we could use a protocol like Secure Hash Algorithm. We can formally verify the Secure Hash Algorithm by defining its different features such as sponge construction and Keccak permutations and then analyze it against our specification of integrity. Lastly, we could look at confidentiality or privacy. This is where information is only accessible to authorized parties. When accessing your home security feed, the stream should be encrypted. That way only you will be able to decrypt it and if intercepted it will be useless data. A policy that is currently implemented is a virtual private network. A virtual private network works by providing end to end encryption. Meaning your data made unreadable without a special key to decrypt it. We can verify VPNs formally by developing a model that considers its properties like the encryption algorithm and its input output behavior. Then define what confidentiality is and plug it into verification software that will test all possibilities of the system.

The cybersecurity of IoT devices is crucial because they touch every aspect of our life. It is important to ensure that IoT devices are designed and implemented with security

in mind to protect against cyber-attacks and safeguard our privacy and safety for ourselves.

References

[1] A. Khaldi, K. Karoui, N. Tanabène and H. B. Ghzala, "A Secure Cloud Computing Architecture Design," 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2014, pp. 289-294, doi: 10.1109/MobileCloud.2014.44.

[2] Y. Lu and L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103-2115, April 2019, doi: 10.1109/JIOT.2018.2869847.

[3] Weaver, Aaron. "More than 150,000 Cameras Hacked in Verkada Breach." *Hacked.com,* 23 Mar. 2021, https://hacked.com/cameras-hacked-in-verkada-breach/.

[4] Cimpanu, Catalin. "DDoS Attacks Bring down Heating System for Two Buildings in Small Finnish Town." *BleepingComputer*, BleepingComputer, 8 Nov. 2016, https://www.bleepingcomputer.com/news/security/ddos-attacks-bring-down-heating-system-for-two-buildings-in-small-finnish-town/.

[5] Wetsman, Nicole. "Medtronic Issues 'Urgent' Recall of Insulin Pump Controller Vulnerable to Hacks." *The Verge*, The Verge, 6 Oct. 2021, https://www.theverge.com/2021/10/6/22712808/medtronic-recall-insulin-pump-controller-cybersecurity-hack.