# **Modern Age of Internet of Things: How our privacy is impacted**

Feifan Cao, Computer Science; Professor Mentor, CECS Departments

# **Project Objective or Aim**

The goal is to determine different ways our privacy is being invaded by cybercriminals and how our personal data are being sold by the various business models without any major detection or individual’s consent. Furthermore, Consumers like us tend to gain a better understanding on what data is collected and how it is used and what privacy practices related industries have developed so far that match their customers’ expectations.

# **Project Background and Significance**

During the COVID-19 pandemic lockdown, the connected device in the household was growing explosively and exchanging information exponentially daily. On the other hand, 90% of your private data has traveled to the other side of the internet right underneath your nose without triggering a single idea of your suspicion.

As AI and algorithms gather more and more data, cybercriminals, or big head companies, can utilize all these computing data to predict your daily actions even perform attack and plant ransomware infections. Individuals’ private data like daily habits, location information, activities are also secretly being sent to companies’ business model enabling “surveillance capitalism”, Individuals must often accept companies’ privacy policies in connection with purchasing and using IoT devices and services. These documents can authorize companies to use personally identifiable data for their own purposes, and transfer and disclose certain data to third parties.

Furthermore, in 2020, Android devices were the most targeted by malware, researchers found, making up 26.64 percent of all infections. Meanwhile, Windows devices and PCs, which are increasingly connected to mobile networks via USB dongles and Wi-Fi, made up 38.92 percent. All the devices mentioned above are literally less than an inch away from us, and the percentage of these danger zones is quite astonishing. The IoT also worsens the current situation of levels of privacy. The law protects us and the right we have been fighting for since recent years big data peeks into everybody’s life. The growing market dominance and the demands of more computing power brought us a taste of convenience, but we certainly have a way bigger price owed to the “loan shark”.

Moreover, the cyberattack that happened back in 2016 that hacked almost a million IoT things is still refreshing till this day. A massive Distributed Denial of Service (DDoS) broke large portions of the Internet, including Netflix, PayPal, GitHub, Amazon, Reddit, Spotify, and Twitter, causing a significant amount of inaccessibility to the major services and websites. The attack was well planned to come from east coast with over 1 million IP addresses, and it largely consist of easily hacked IoT devices.

Additionally, Manufacturers mainly focus on the accessibility and performance of these devices which are utilized in a way that can’t be secured or encrypted. Mirai is a piece of malware that targets [Internet of Things](https://thehackernews.com/2015/08/hacking-internet-of-things-drone.html) devices such as routers, and security cameras, DVRs, and enslaves vast numbers of these compromised devices into a botnet, which is then used to conduct DDoS attacks. The data also suggested that there were more than 1.2 million Mirai-infected devices, also over 166,000 devices being operative. Mirai-infected IoT is still in a rate of increasing and don’t seem to have any intend of slowing down soon due to customer demands or home intelligence upgrade.

# **Research Methods**

Task 1 (first 2 weeks of May): A qualitative research approach is proposed for the IoT research. Following the phenomenological approach, we seek to understand the percentage among the population that knowledge how privacy is invaded by IoT, or personal data gets collected, unauthorized accesses and data get sold by big head companies. The research data may consist of interview transcripts, field notes from observations, a wide variety of records.

Task 2 (last 2 weeks of May): Data collection from school library and online resource will be conducted on the current influences of IoT, its history and progress. The focus will especially be on the recent IoT ransomware, Botnets, Denial-of-Service attacks, etc. These can approximate the amount of device that’s used by the criminal without any form of data encryption. Additionally, further legal documents will also be viewed to compare to how private data from electronic devices is handled within the legislative loopholes.

Task 3 (first 2 weeks of June): physical test will be conducted by using uPNP, a technology that provides an instant, seamless connection to network-enabled devices. Devices, such as video cameras, use uPNP to talk to your router and accept outside connections. Also experiment will utilize specialized search engines that can go out of the way to locate and index online devices, without any permission from end users.

Task 4 (Last 2 weeks of June): A number of IoT devices rely on cellular connections to function instead of Wi-Fi. But while connecting a device to the internet can open the door to attackers, so we will manipulate a cellular network to intercept any digital signals delivered from multiple set-up endpoints to calculate the time elapsed for the researcher to simulate a successful attack. Furthermore, controlled experiments will be used on how long the IoT devices can defense on the attack based on the controlled variables of secured password, firmware, high-level encryption, etc.

Timeline

Description automatically generated

# **Expected Outcome**

Developers and manufacturers will be encouraged and pushed to come up with new implementations that strengthen the levels of security and encryption of their DNS server and password. On the other hand, research data will be shared with other consumers, and they will be able to identify different types of IoT devices and utilize multiple ways to install them with enhanced security concepts and how to set up better protection fence, like keeping up with device secure integrity update, coming up with stronger password.

Businesses need to ensure their data is safe and isn’t easily accessible by unauthorized users. Though online thieves are trying to use modern technologies to stay ahead of businesses, the IoT can provide a safer environment to store your information through the usage of dedicated networks, specific security protocols or security modules embedded in the IoT engines.

In addition, it allows us to monitor all activities on your equipment in real-time. Through IoT technology, you can notice any unusual activity on your systems and respond to it immediately.

IoT also allows you to use remote surveillance or ID verification. This ensures only legitimate people can access your sites and equipment. In addition, this makes sure your customers’ information is safe and improves their experience, allowing them to continue engaging with your business.

# **Literature Review**

Elsevier B.V., “ Internet of Things (Amsterdam, Netherlands)”, Volume:1, 2018,  <https://ucfflvc.primo.exlibrisgroup.com/discovery/jfulldisplay?context=L&vid=01FALSC_UCF:UCF&tab=jsearch_slot&docid=alma99383232028606596>

Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111 (2019). <https://doi.org/10.1186/s40537-019-0268-2>

Elgazzar K, Khalil H, Alghamdi T, Badr A, Abdelkader G, Elewah A and Buyya R (2022) Revisiting the internet of things: New trends, opportunities and grand challenges. *Front. Internet. Things* 1:1073780. doi: 10.3389/friot.2022.1073780

European Alliance for Innovation, issuing body, “EAI endorsed transactions on internet of things”, Place of publication not identified : EAI, Volume 1, issue 1, 2015, <https://ucf-flvc.primo.exlibrisgroup.com/discovery/jfulldisplay?context=L&vid=01FALSC_UCF:UCF&tab=jsearch_slot&docid=alma99383143914206596>

IEEE, “Internet of Things (GCIoT)”, 2018, <https://ucf-flvc.primo.exlibrisgroup.com/discovery/jfulldisplay?context=L&vid=01FALSC_UCF:UCF&tab=jsearch_slot&docid=alma99383122259306596>

Elsevier, “Internet of Things and Cyber-Physical Systems”, IEEE, 2021,  <https://ucf-flvc.primo.exlibrisgroup.com/permalink/01FALSC_UCF/kngciq/alma99383122259306596>

# **Preliminary Work and Experience**

I have worked on projects relating to assessment of IoT with moderate level of knowledge on user data utilization and manipulation, along with the course Modern Network+, Malware Analysis, and Social Network Analysis. This project would be a culmination of some of my past major work which provided me skills in critically analyzing scientific publications, practicing instruction detection techniques, and working with network security.

Additionally, I have been working on the first and second tasks of this project with the help of my mentor and the funding from the UCF research grant program, and I gained a better understanding on scholarly methods, relevant sources, and the sheer complexity of planning and carrying forward a large-scale research project.

# **IRB/IACUC statement**

According to IRB Approval: human subjects research activities designed to develop or contribute to generalizable knowledge, to ensure compliance with IACUC guidelines before the work begins, completed forms for IRB approval requested if that’s applicable.

# **Budget**

Travel costs to conduct research: travel by car for reimbursement will be given $.7/mile traveled (inclusive of gas and miles on the car)

Supplies or materials needed for the project not currently available on campus: 1 modem and 3 routers that can be used to set up a wireless network, 4 IoT devices

$50/modem, $60/router, $50/IoT device.

Toal: $430