**Abstract**

The growth of the Internet of Things (IoT) has transformed everyday life, it offers unprecedented convenience along with efficiency. However, this expansion has introduced significant security challenges due to the lack of clear definitions, standards, and hygiene surrounding IoT devices. Much like the challenges faced by the Cyberspace Solarium Commission in defining digital boundaries, the IoT ecosystem struggles with privacy concerns and vulnerabilities in device design. This paper explores the unique threats that IoT had, including limited resources, physical access risks, and weak default security configurations if at all. It also examines the role of IoT in recent high-profile cyberattacks, like the Mirai Botnet along with the copycats that have come since. In addition, the paper reviews current security frameworks, technologies, and strategies to assist with mitigation of IoT risks looking at both consumer and industrial IoT. Lastly, the paper argues that a universally accepted definition of IoT is essential for creating comprehensive cybersecurity policies that can effectively protect the devices that are increasingly becoming integral to modern life.

**Introduction to IoT Security**

What is the Internet of Things (IoT)? Similar to the broader struggles that the Cyberspace Solarium Commission has had, the problems with securing the internet against attack is because of arguments of privacy (amongst other things). Without an official, internationally accepted definition of what is, in a sense, a person’s digital boundary, like their home or what the digital walls of the company are. What is private? Where does a person/entity have a reasonable expectation of privacy? The IoT does not have a single definition of what it is either. National Institute of Standards and Technology (NIST) defines it as: “devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g. Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world” [1]. Britannica focuses on the technical foundation of what is IoT, ““smart,” computer-like devices so commonplace today, which can connect with the internet or interact via wireless networks” [2]. Wikipedia takes these definitions one step further by adding that the IoT needs to be individually addressable.

The appeal of convenience is one of the reasons that the IoT has exploded. In 2021, it was calculated that there were 7,620 new IoT devices connected to the internet every minute [3]. According to Christo, this year (2025) it will reach 152,000/min [3]. For companies, it is data and analytics. The massive data collection capabilities of IoT’s provide companies with valuable insights, enabling predictive analytics. However, this data can often be harvested and sold for marketing purposes, highlighting the vulnerabilities in IoT.

In 2022 alone, the IoT market was valued at $742 billion [3]. It comes at no surprise that the criminal market want’s a “piece of the pie”. Half of all crime now occurs online [4]. The FBI’s Internet Crime Report reported losses exceeding $16 billion, which is a 33% increase from 2023 to 2024 [5]. With weak to no securities on many IoT devices, this becomes a large problem. Sean from Jumpcloud released a statistic that said more than 50% of IoT devices have a critical vulnerability that can be exploited in 2025 [6]. This is because it only takes one open device to allow attackers to get into a system and start moving laterally through the network. HIPPA is just one concern in the healthcare industry, with the use of IoT becoming popular. Ascension Health Care has become an example, their data breach was believed to be from a spear phishing attack however, it illustrates how easy it is for one event to cause a significant problem. By significance, it is reported that financial losses due to the attack include $1.8 billion [7]. Lawsuits are ongoing.

The private sector is also on the menu for attackers. Not always the end goal though. Just a means to an end. One example of this is the Mirai Botnet Attack which targeted unsecured IoT devices. This attack caused widespread outages due to the DDoS attack including some critical services. This was accomplished with a short list of 62 common default usernames and passwords but gave access to hundreds of thousands of devices [8].

**Key Threats and Security Challenges**

The IoT provides some unique security challenges. It is often forgotten by the general public that devices that don’t look like computers still are a computer of sorts. With IoT popularity it is nearly impossible to go somewhere and not run into an IoT device. Three of the security challenges that are important to note with attempting to secure devices are [9]:

* Limited battery life
* IoT devices can have minimal processing power. Often relying on microcontrollers to accomplish their tasks and have only small processing capabilities.
* Use of low bandwidth networks

A device that has limited battery life and is expected to last for a long time is an implanted pacemaker/defibrillator. One might think, why would these be connected to networks? These devices can be connected to a computer (programmer) via something like WiFi but instead a proprietary protocol going over Radio Frequency Telemetry. This is done to interrogate the device to give information to the doctor to aid in treatment of the patient. For now, each manufacturer has their own protocols and algorithms. This makes ICD’s less of a target now. An article in the American Heart Association Journals has stated that there are clinical benefits to standardize protocols and to implement remote interrogation and alert functionality through Bluetooth… [10]. Something less critical but still in the list of IoT are devices like printers, smart home controllers and IP cameras. Alone, these are small low computational powered devices. Yet IP cameras were cited as a major component of the Mirai DDoS botnet [11].

Internet security can also have physical access considerations as a challenge. A rubber ducky is an example of this. The social engineering USB drop is of concern of this. Employees finding a random USB drive in the parking lot can be one of these. When plugged in can be used as a keyboard to input commands faster than any human ever could.

Because of convenience for people that just want things to work also to limit the need to add to the processor needs, many IoT devices have credentials hardcoded. With this there is no way to secure these devices by changing passwords. One of only a few ways to secure these devices is to separate them on the network and potentially behind something that can intercept communications to these devices. That is not feasible in the general public. Even with some home routers offering auto updates there are many routers that have not had their firmware updated since purchase. According to a survey by Broadband Genie, a striking 89% of respondents in the UK reported having never updated their router’s firmware [12]. This study brings up the next security challenge, default passwords and weak configurations. The survey cited 86% of the respondents never changed their administrator password [12]! Implementing a Zero Trust for IoT is paramount.

**Existing Technologies, Research, and Frameworks**

Existing Technologies to protect the IoT can be as simple or complex as network segmentation or VLANs. OWASP emphasized this by moving vulnerable and outdated components from 9th to 6th place [13].

A diagram of a diagram

AI-generated content may be incorrect.

Picture : https://owasp.org/www-project-top-ten/

Because of the risks NIST has created a framework to help guide companies in development. This list includes [14]:

* Policies and procedures
* Training and awareness
* Providing support to teach users
* Changing setting on tech devices
* Risk management activities
* Disposal practices
* Physical protections
* Vulnerability assessments
* Bug reporting
* Contracts
* Audits
* Contingency plans
* Systems and applications development lifecycles
* Compliance

To help with updating all the IoTs in a company, using an over-the-air update system could be a solution. An example of this is Samsung pushing updates to all devices connected to the wireless network.

**Critical Analysis/Comparison**

When comparing IoT there is two categories that can be broken into. Consumer IoT and Industrial IoT (IIoT). As mentioned above there are many challenges that are in the consumer IoT vs IIoT. Lack of education and willingness to update equipment for consumers poses the biggest challenge. Getting companies to invest in keeping up devices that are not generating any revenue is another challenge. For IIoT it becomes easier, yet still costly to implement changes. Uptime requirements for companies are, many times, needed 24/7.

Network segmentation and VLANs: Attempting to have the public to implement this is challenging because of the lack of desire to learn how to or take time to implement. IoT-specific firewalls and IDS/IPS can be costly but can help to protect companies. Microsoft has announced that starting July 1st, 2025, windows server hotpatching will be subscription only and costing $1.50 per core per month [15]. This doesn’t seem much but can add up very quickly. According to Trenton Systems, older lighter workload servers might have 4 to 8 cores per processor [16], newer processors range from 16 to 64+ cores [16]. High-performance servers can have 200 or more per processor [17]. Many servers in this class can hold multiple of these processors in banks. With companies having multiple servers, this cost can rapidly increase just for the server alone. This type of payment for updates can become too expensive for a company if IoT manufacturers started charging for updating each device. A study by Blythe said that cyberhygiene was absent in user manuals or online materials associated of 90% of IoT devices sampled [18]. This is another possible avenue to raise awareness to work towards securing the IoT. Companies are starting to have to address security concerns when employees want to use their private IoT devices at work. When company owned, control becomes easier, but with employee-owned devices this area becomes grey. Who can control what part?

**Real-World Case Studies**

As mentioned earlier, the Mirai Botnet is a real-world example of how the IoT can be used for evil. Even if this was just proof of concept that went bad the copycats are very real. Variants include IoT Reaper, Okiru, Satori, and Muhstik to name a few. Now that it is understood that just barrowing a little processor power from a large list of devices. It can easily take down large targets. Apple has even used this for what they think is good where their devices, especially Airtags, can borrow a little bit of network bandwidth from any nearby access point unless they opt out. Apple has also made a statement: “AirTag was designed to help people locate their personal belongings, not to track people or another person’s property, and we condemn in the strongest possible terms any malicious use of our products.” [18]. Ruheni points out an important distinction, misuse is “condemned” not “prevented” [18]. So, the problem is there; Just not fixed. The importance of securing IoT devices is shown in the following pictures. The first is alleged iRobot Rumba footage, the second picture is verified, and involves Ring security cameras.

A collage of a person sitting on a couch

AI-generated content may be incorrect.

Picture : <https://strangesounds.org/wp-content/uploads/2022/12/MIT-Confirms-Roomba-Vacumn-Secretely-Took-Photos-Of-Woman-In-Bathroom.jpg>

A room with a ceiling fan and bed

AI-generated content may be incorrect.

Picture : <https://www.popularmechanics.com/technology/security/a30242264/ring-doorbell-hack/>

**Conclusion and Future Trends**

IoT is not going to be going anywhere in the foreseeable future. Therefore, securing these devices needs to be at the forefront of new policies for companies. The key challenge is how to secure devices that haven’t been designed with security in mind. For companies an employee satisfaction driver is getting to use their own IoT. Ultimately with this information. Which side is going to win? Jamie Yap of ZDNet found that 64% of employees reported improved efficiency when using personal devices for work [19]. Michael Lazar of Insight stated that 87% of companies rely on employees using personal devices for business applications [20]. In conclusion, the definition of what an IoT is needs to be cemented into an internationally excepted definition. That way laws and policies can start to be implemented to protect against misuse of this potentially amazing group of technologies. After all it isn’t the tool that is either good or bad. A hammer can be used for good and build a home, it is also on the FBI list of weapons used in murder. The IoT is too important not to protect.

# References

|  |  |
| --- | --- |
| [1] | National Institute of Standards and Technology, "Glossary," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/iot\_device. |
| [2] | Britannica, "Internet of Things," Britannica, [Online]. Available: https://www.britannica.com/technology/artificial-intelligence. |
| [3] | C. Petrov, "26 Insightful Internet of Things Statistics 2024," Techjury, 3 January 2024. [Online]. Available: https://techjury.net/blog/internet-of-things-statistics/. |
| [4] | J. M. Blythe and S. D. Johnson, "A systematic review of crime facilitated by the consumer Internet of Things," *Security Journal,* pp. 97-125, March 2021. |
| [5] | Federal Bureau of Investigation Internet Crime Complaint Center, "IC3 Annual Report," FBI, 2024. |
| [6] | S. Blanton, "IoT Security Risks: Stats and Trends to Know in 2025," Jumpcloud, 10 January 2025. [Online]. Available: https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025. |
| [7] | S. Jain, "Ascension’s Financial Comeback Stalled by Costly Cyberattack, Resulting in $1.8 Billion Loss," The Cyber Exress, 20 September 2024. [Online]. Available: https://thecyberexpress.com/ascension-cyberattack-cost-billion-loss/. |
| [8] | Cybersecurity & Infrastructure Security Agency, "Heightened DDoS Threat Posed by Mirai and Other Botnets," CISA, 17 October 2017. [Online]. Available: https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets. |
| [9] | J. Rosende, "IoT security issues and solutions for low-power devices," Onomondo, 22 January 2025. [Online]. Available: https://onomondo.com/blog/iot-security-issues-and-solutions-low-power-devices/#:~:text=As%20battery%20levels%20decrease%2C%20devices,encryption%20strength%20during%20low%2Dpower. |
| [10] | M. M. N. V. M. a. D. B. K. M. M. Jamie Diamond, "Making the Most of Cardiac Device Remote Management: Towards an Actionable Care Model," *Circluation: Arrhythmia and Electrophysiology,* vol. 14, no. 3, 2021. |
| [11] | M. Heinemeyer, "Mirai Malware: Impact on CCTV Cameras," Darktrace, [Online]. Available: https://www.darktrace.com/blog/mirai-malware-infects-cctv-camera. [Accessed 4 May 2025]. |
| [12] | M. Jackson, "Survey Claims UK Internet Users Leave Broadband Routers Open to Hackers," ISPreview, 30 September 2024. [Online]. Available: https://www.ispreview.co.uk/index.php/2024/09/survey-claims-uk-internet-users-leave-broadband-routers-open-to-hackers.html. |
| [13] | OWASP, "OWASP Top Ten 2025," OWASP, 2025. [Online]. Available: https://owasp.org/www-project-top-ten/. |
| [14] | National Institute of Standards and Technology, "NIST Cybersecurity for IoT:," 4 March 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/nist-cybersecurity-for-iot-update/images-media/NIST%20%20Cybersecurity%20for%20IOT%20Update%20Megas.pdf. |
| [15] | D. Winder, "Microsoft Confirms $1.50 Windows Security Update Hotpatch Fee Starts July 1," Forbes, 30 April 2025. [Online]. Available: https://www.forbes.com/sites/daveywinder/2025/04/30/microsoft-confirms-150-windows-security-update-fee-starts-july-1/. |
| [16] | C. Trick, "How Many Cores are Enough?," Trenton Systems, 18 July 2022. [Online]. Available: https://www.trentonsystems.com/en-us/resource-hub/blog/how-many-cores-are-enough. |
| [17] | H. Mujtaba, "AMD Zen 6 Architecture Rumored To Power EPYC Venice Server CPUs: Over 200 Cores, Completely Redesigned L2/L3 Cache & HBM SKUs," WWCF Tech, 29 April 2022. [Online]. Available: https://wccftech.com/amd-epyc-venice-server-cpus-zen-6-architecture-384-cores-hbm-skus-new-l2-l3-cache-rumor/. |
| [18] | J. lythe, N. Sombatruang and S. Johnson, "What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?," *Journal of Cybersecurity,* no. 10.1093, pp. 1-10, 2019. |
| [19] | R. Mathenge, "The Apple AirTag: What is It, and Why is It so Dangerous?," PrivacySavvy, 23 August 2024. [Online]. Available: https://privacysavvy.com/security/spying/apple-airtag-dangerous-privacy-concerns/. |
| [20] | J. Yap, "BYOD boosts staff's productivity, job satisfaction," ZDNet, 21 March 2012. [Online]. Available: https://www.zdnet.com/article/byod-boosts-staffs-productivity-job-satisfaction/. |
| [21] | M. Lazar, "BYOD Statistics Provide Snapshot of Future," Insight, 16 Nov 2017. [Online]. Available: https://www.insight.com/en\_US/content-and-resources/2017/01182017-byod-statistics-provide-snapshot-of-future.html. |